Copyright

CCIEv5 R&S Advanced Configuration & Troubleshooting Lab Workbook
by Tom Mark Giembicki & Sean Paul Draper

Copyright® 2015, CCIE4ALL All Right Reserved

Produced in the United Kingdom

This book contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without express written permission from the author / publisher.

CCIE R&S Advanced Configuration and Troubleshooting Lab Workbook may be purchased for educational, business or sales promotional use. For more information, contact us – tom.giembicki@gmail.com or sean.draper@gmail.com

Acknowledgments

Tom Mark Giembicki – Tom is in the productivity business. At some level, we all are. We’d like to think that whatever solution we’re selling or service we’re providing will offer a benefit or make life better in some way.

So long as we’re in an organization with limited finances (which probably includes most for-profit and not-for-profit organizations these days) we need to measure “better” in two ways. One way of making things “better” means better for the organization itself, so it can do a better job of achieving its mission for its customers. The other way makes things better for the people who work in the organization. The tendency generally seems to be to focus on making things better for the organization (and therefore the bottom line), but unfortunately, as organizations go about making these types of “improvements”, it is easy to forget that “better for the people” often has a direct impact on “better for the organization”, i.e. making tasks easier and faster for the individuals in a company generally leads to increasing the overall productivity of the company. I would like to thank my family for absolutely everything I have achieved so far in my life and also Insight Team for helping me manage client’s appointments and business trips while working on this book.

Sean Paul Draper – There are too many friends to list here you all know who you are, I would also like to give thank to my family, especially my mother.
# Table of Contents

COPYRIGHT .................................................................................................................. 0
ACKNOWLEDGMENTS .................................................................................................... 0
FOREWORD ...................................................................................................................... 8
TROUBLESHOOTING SECTION .................................................................................... 9
DIAGNOSTICS SECTION ............................................................................................... 10
CONFIGURATION SECTION ............................................................................................ 11
OBJECTIVES AND AUDIENCE .................................................................................... 12
WARNING AND DISCLAIMER ...................................................................................... 13
LICENSE AGREEMENT .................................................................................................. 13
TERM AND TERMINATION OF LICENSE AGREEMENT ........................................... 14
WARRANTY ..................................................................................................................... 14
CCIE EXAM IOS & CATEGORY CHANGES .................................................................. 15
CCIE EXAM GUIDELINES UPDATE ........................................................................... 16
LAB EXAM GUIDELINES ............................................................................................... 17
LAB#1 .............................................................................................................................. 20

**SAN FRANCISCO GROUP HQ** .................................................................................. 20
  VLAN TRUNK VTP .................................................................................................... 20
  ETHERCHANNEL ......................................................................................................... 23
  SPANNING-TREE MST ............................................................................................... 28
  SPANNING-TREE TUNING ......................................................................................... 32
  LAYER 2 SECURITY .................................................................................................... 34
  CDP ............................................................................................................................ 36

**SERVICE PROVIDER#9** .......................................................................................... 38
  VLAN TRUNK VTP .................................................................................................... 38
  ETHERCHANNEL ......................................................................................................... 43
  SPANNING-TREE RAPID PVST ................................................................................ 49
  SPANNING-TREE TUNING ......................................................................................... 53
  SPANNING-TREE TIMERS ......................................................................................... 54
  SPANNING-TREE UPLINKFAST ............................................................................... 55
  ROUTER ON A STICK .................................................................................................. 56

**SYDNEY BUSINESS MODEL HQ** ........................................................................... 60
  VLAN TRUNK VTP .................................................................................................... 60
  SPANNING-TREE RAPID PVST ................................................................................ 63
  SPANNING-TREE TUNING ......................................................................................... 65
  L2 SECURITY ............................................................................................................... 67

**SAN FRANCISCO GROUP REMOTE SITE** .............................................................. 70
  DHCP MANUAL BINDINGS (7-BYTE) ........................................................................ 70

**SAN FRANCISCO GROUP DATA CENTRE** .............................................................. 73
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP (27-BYTE)</td>
<td>73</td>
</tr>
<tr>
<td>BERLIN HQ HOME</td>
<td>76</td>
</tr>
<tr>
<td>DHCP Exclusion</td>
<td>76</td>
</tr>
<tr>
<td>BERLIN REMOTE OFFICE</td>
<td>78</td>
</tr>
<tr>
<td>DHCP Multiple Subnet Functionality</td>
<td>78</td>
</tr>
<tr>
<td>BERLIN HQ DATA CENTRE</td>
<td>83</td>
</tr>
<tr>
<td>DHCP Exclusion</td>
<td>83</td>
</tr>
<tr>
<td>SYDNEY BUSINESS MODEL HQ</td>
<td>87</td>
</tr>
<tr>
<td>PPPoE</td>
<td>87</td>
</tr>
<tr>
<td>SYDNEY BUSINESS REMOTE OFFICE - SP#7</td>
<td>90</td>
</tr>
<tr>
<td>Multilink PPP</td>
<td>90</td>
</tr>
<tr>
<td>SP#3/SP#4</td>
<td>95</td>
</tr>
<tr>
<td>PPP PAP/CHAP</td>
<td>95</td>
</tr>
<tr>
<td>SP#2/SP#6</td>
<td>97</td>
</tr>
<tr>
<td>PPP EAP</td>
<td>97</td>
</tr>
<tr>
<td>SAN FRANCISCO GROUP REMOTE SITE</td>
<td>102</td>
</tr>
<tr>
<td>EIGRP</td>
<td>102</td>
</tr>
<tr>
<td>SAN FRANCISCO GROUP DATA CENTRE</td>
<td>104</td>
</tr>
<tr>
<td>EIGRP</td>
<td>104</td>
</tr>
<tr>
<td>SAN FRANCISCO GROUP HQ</td>
<td>106</td>
</tr>
<tr>
<td>EIGRP</td>
<td>106</td>
</tr>
<tr>
<td>EIGRP Metric</td>
<td>106</td>
</tr>
<tr>
<td>EIGRP Offset-List</td>
<td>109</td>
</tr>
<tr>
<td>EIGRP Distribute List</td>
<td>112</td>
</tr>
<tr>
<td>EIGRP Route Tag</td>
<td>115</td>
</tr>
<tr>
<td>EIGRP Authentication</td>
<td>119</td>
</tr>
<tr>
<td>EIGRP bfd</td>
<td>123</td>
</tr>
<tr>
<td>BERLIN HQ HOME USER</td>
<td>128</td>
</tr>
<tr>
<td>EIGRP</td>
<td>128</td>
</tr>
<tr>
<td>BERLIN REMOTE OFFICE</td>
<td>129</td>
</tr>
<tr>
<td>EIGRP</td>
<td>129</td>
</tr>
<tr>
<td>SYDNEY BUSINESS MODEL HQ</td>
<td>130</td>
</tr>
<tr>
<td>EIGRP</td>
<td>130</td>
</tr>
<tr>
<td>DHCP</td>
<td>130</td>
</tr>
<tr>
<td>SYDNEY BUSINESS REMOTE OFFICE(1)</td>
<td>132</td>
</tr>
<tr>
<td>EIGRP</td>
<td>134</td>
</tr>
<tr>
<td>SYDNEY BUSINESS REMOTE OFFICE(2)</td>
<td>134</td>
</tr>
<tr>
<td>EIGRP</td>
<td>135</td>
</tr>
<tr>
<td>SERVICE PROVIDER#9</td>
<td>138</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>OSPF</td>
<td>138</td>
</tr>
<tr>
<td>OSPF</td>
<td>144</td>
</tr>
<tr>
<td>OSPF LOCAL POLICY ROUTING</td>
<td>147</td>
</tr>
<tr>
<td>OSPF POLICY ROUTING</td>
<td>148</td>
</tr>
<tr>
<td>OSPF LSA</td>
<td>149</td>
</tr>
<tr>
<td>OSPF AUTHENTICATION</td>
<td>150</td>
</tr>
<tr>
<td>OSPF MPLS</td>
<td>153</td>
</tr>
<tr>
<td>OSPF FILTERING</td>
<td>158</td>
</tr>
<tr>
<td>BERLIN HQ DATA CENTRE</td>
<td>160</td>
</tr>
<tr>
<td>OSPF</td>
<td>160</td>
</tr>
<tr>
<td>SERVICE PROVIDER #1</td>
<td>163</td>
</tr>
<tr>
<td>eBGP</td>
<td>163</td>
</tr>
<tr>
<td>SERVICE PROVIDER #2</td>
<td>166</td>
</tr>
<tr>
<td>eBGP</td>
<td>166</td>
</tr>
<tr>
<td>SERVICE PROVIDER #3</td>
<td>169</td>
</tr>
<tr>
<td>eBGP</td>
<td>169</td>
</tr>
<tr>
<td>SERVICE PROVIDER #4</td>
<td>171</td>
</tr>
<tr>
<td>eBGP</td>
<td>171</td>
</tr>
<tr>
<td>SERVICE PROVIDER #5</td>
<td>173</td>
</tr>
<tr>
<td>eBGP</td>
<td>173</td>
</tr>
<tr>
<td>SERVICE PROVIDER #6</td>
<td>176</td>
</tr>
<tr>
<td>iBGP</td>
<td>176</td>
</tr>
<tr>
<td>SERVICE PROVIDER #6</td>
<td>179</td>
</tr>
<tr>
<td>NLRI ADVERTISEMENT</td>
<td>179</td>
</tr>
<tr>
<td>SERVICE PROVIDER #6 #7</td>
<td>180</td>
</tr>
<tr>
<td>eBGP</td>
<td>180</td>
</tr>
<tr>
<td>BGP FILTERING</td>
<td>182</td>
</tr>
<tr>
<td>SERVICE PROVIDER #7 #8</td>
<td>184</td>
</tr>
<tr>
<td>eBGP</td>
<td>184</td>
</tr>
<tr>
<td>SP#7 - SP#8 – SBM HQ – SBM REMOTE OFFICE#1</td>
<td>186</td>
</tr>
<tr>
<td>eBGP</td>
<td>186</td>
</tr>
<tr>
<td>eBGP</td>
<td>188</td>
</tr>
<tr>
<td>SERVICE PROVIDER #9</td>
<td>191</td>
</tr>
<tr>
<td>iBGP</td>
<td>191</td>
</tr>
<tr>
<td>SAN FRANCISCO GROUP HQ</td>
<td>195</td>
</tr>
<tr>
<td>iBGP</td>
<td>195</td>
</tr>
<tr>
<td>eBGP - NEXT HOP SELF</td>
<td>199</td>
</tr>
<tr>
<td>ROUTE PREFERENCE</td>
<td>203</td>
</tr>
<tr>
<td>Control Plane</td>
<td>402</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>NTP - Part I</td>
<td>406</td>
</tr>
<tr>
<td>NTP - Part II</td>
<td>412</td>
</tr>
<tr>
<td>DNS</td>
<td>413</td>
</tr>
<tr>
<td>HTTP</td>
<td>417</td>
</tr>
<tr>
<td>NETFLOW</td>
<td>419</td>
</tr>
<tr>
<td>NETFLOW</td>
<td>420</td>
</tr>
<tr>
<td>Flexible NETFLOW</td>
<td>422</td>
</tr>
<tr>
<td>NAT</td>
<td>425</td>
</tr>
<tr>
<td>EEM I</td>
<td>427</td>
</tr>
<tr>
<td>EEM II</td>
<td>429</td>
</tr>
<tr>
<td>EEM III</td>
<td>431</td>
</tr>
<tr>
<td>EEM IV</td>
<td>432</td>
</tr>
<tr>
<td>TFTP</td>
<td>433</td>
</tr>
<tr>
<td>Sydney Business Model HQ</td>
<td>434</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>434</td>
</tr>
<tr>
<td>NBAR</td>
<td>437</td>
</tr>
<tr>
<td>QOS</td>
<td>439</td>
</tr>
<tr>
<td>SNMP</td>
<td>442</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>444</td>
</tr>
<tr>
<td>Verification</td>
<td>451</td>
</tr>
<tr>
<td>Lab#2</td>
<td>467</td>
</tr>
<tr>
<td>EIGRP Over The Top (OTP)</td>
<td>467</td>
</tr>
<tr>
<td>Lab#3</td>
<td>476</td>
</tr>
<tr>
<td>MPLS Core - Service Provider 9</td>
<td>476</td>
</tr>
<tr>
<td>VLAN Trunk VTP</td>
<td>476</td>
</tr>
<tr>
<td>Etherchannel</td>
<td>481</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>486</td>
</tr>
<tr>
<td>San Francisco Group HQ</td>
<td>491</td>
</tr>
<tr>
<td>VLAN Trunk VTP</td>
<td>491</td>
</tr>
<tr>
<td>Etherchannel</td>
<td>495</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>498</td>
</tr>
<tr>
<td>Sydney Business Model</td>
<td>503</td>
</tr>
<tr>
<td>VLAN Trunk VTP</td>
<td>503</td>
</tr>
<tr>
<td>Etherchannel</td>
<td>506</td>
</tr>
<tr>
<td>Spanning Tree</td>
<td>509</td>
</tr>
<tr>
<td>Troubleshooting Guidelines</td>
<td>515</td>
</tr>
<tr>
<td>Lab#4</td>
<td>518</td>
</tr>
<tr>
<td>Incident#1</td>
<td>518</td>
</tr>
<tr>
<td>Incident#2</td>
<td>519</td>
</tr>
<tr>
<td>Incident#3</td>
<td>520</td>
</tr>
<tr>
<td>Incident#4</td>
<td>522</td>
</tr>
<tr>
<td>Incident#5</td>
<td>524</td>
</tr>
</tbody>
</table>
Foreword

While the CCIE certification has long been the standard for network excellence, previous versions of the CCIE Lab did not test real-life scenarios where topics such as Frame Relay, WCCP to name a few more have now been completely removed from the version CCIEv5 lab with the lab now more focused on relevant topics such as IPv6, VPN and troubleshooting methodologies.

While the CCIE Written exam remains essentially the same, the CCIE Lab exam has significant changes. The entire version 5 Lab exam will be utilized on 100% virtual equipment. Features on Cisco IOS Software Release 15 can now be tested in the lab and along with virtualising the devices the exam provides a more realistic network with much larger network topologies. The main objective of this workbook session is to give an overview of how the exams are conducted and to provide you good guidance on what you need to look at when preparing and taking the exams.

The CCIE lab exam now consists of three specific sections:
- Troubleshooting
- DIAG
- Configuration

We have included a few screenshots from Cisco Live program, see the following:
Troubleshooting Section

Network topology of ~30 virtual routers and switches

Scenario is fully preconfigured but contains faults

2h30 maximum (visible countdown timer + 30 min warning after 2h)

Content designed to be doable within 2h

Incidents’ stem are “symptom-based”

Verifications are “result-based” + constraints

No partial scoring

• Incident#1

Hosts that are connected to the interface E1/0 of R19 are not able to use Telnet to connect to the server R50, which is located in VLAN_100.

Fix the problem so that the following Telnet session establishes:

```
R19#telnet 200.100.200.200 /so e1/0
Trying 200.100.200.200 ... Open
User Access Verification
Password:
R50>
```

While resolving this issue, you are not allowed to create any new interface.

Refer to the Troubleshooting guidelines to determine if your solution is appropriate.

Make sure that you disconnect the telnet session after verification.
Diagnostics Section

Independent scenarios putting candidates into the role of a Network Support engineer who diagnoses networking issues

Analyze, identify, locate and explain the root cause

Recommend optimal troubleshooting procedures leading to the root cause

Recommend network changes isolating the issue without causing more harm

Analyzing, correlating and discerning multiple sources of documentation

- Email threads
- Network topology diagrams
- Console sessions log, Syslogs, Monitoring charts, ...
- Network traffic captures

Designed to be doable within 30 minutes

Tickets stem are very generic

Scenarios provided by additional documentation

Verifications are “deterministic”

Partial scoring possible per ticket

Task #2: Multiple Choice - Multiple Answer

A new service request was escalated to you and the following information was provided to help you understand, diagnose and help resolve the issue:

- Network topology of RandomOffice.org
- Email thread between customer and helpdesk
- Traffic capture

Considering all information provided, which two of the following options are the only possible causes of this issue?

Select 2 answers:

- Slow uplink to the ISP
- Peer-to-peer traffic on a user’s workstation
- Wrong access-list configuration on R20
- Wrong NAT configuration on R20
- Not enough memory on the R20
- Routing issue on the ISP network
- Too many users on the network
- Virus on a user’s workstation opening too many connections
**Configuration Section**

Network topology with virtual routers and switches

Scenario is partly pre-configured and items are inter-dependent!

Item#10 may require Item#1 to be completed! And Vice versa!!

Sequence of items is not aligned to the implementation sequence!!

May include implicit troubleshooting

5h30 maximum (no visible countdown timer, refer to proctor’s clock)

Items’ stem are based on requirements and constraints

Verification rules check for functionalities, not specific configurations

Validate alternate solution configurations

No partial scoring

- **Main IGP topology diagram**
  - One enterprise/corporation
  - Multiple remote sites
  - Multiple Service Providers
  - Host/Server simulated by IOS

- **Console access via**
  - Per-device terminal (PuTTY)
  - Main diagram URL (image-map)
  - Device manager (listing)
Objectives and Audience

CCIEv5.0 Routing and Switching Advanced Configuration and Troubleshooting Labs presents you with full configuration / troubleshooting lab scenarios in exam style format to echo the real CCIE Routing and Switching v5.0 lab exam. This publication gives you the opportunity to put into practice your own extensive theoretical knowledge of subjects to find out how they interact with each other on a larger complex scale.

As the network evolves to support technological advances such as the Internet of Everything and employee mobility, there is a significant demand for expert-level engineers with proven skills to support forward-looking trends. The enhanced CCIE Routing and Switching Exams, along with expert-level training for CCIE, provide sophisticated education and requisite certification to support tomorrow’s advanced networks. These new standards reflect both the evolution of job skills that employers are looking for at the expert level and the evolution of related technologies that are relevant to today’s enterprise network environments. Network engineers who use the expert-level training will be equipped with the knowledge and validated skills required to accelerate expert-level competency in the field.

Cisco announced a major revision of the CCIE® Routing and Switching (R&S) Certification and expert-level training to meet the increasing challenges of enterprise networks evolving in size, scope and complexity. As the network carries more essential services, networking experts are expected to anticipate, diagnose and resolve complex network issues accurately and quickly. The increasing importance of the network to drive significant productivity and cost benefits to organizations as well as the role of the network in transforming businesses have driven worldwide demand for skilled IT staff.

“Cisco,” the “Cisco Logo,” “CCNA,” “CCNP,” “CCDP,” “CCDA,” “CCIE,” “Cisco Certified Network Associate,” “Cisco Certified Design Professional,” “Cisco Certified Design Associate,” “and “Cisco Certified Network Professional,” are registered trademarks of Cisco Systems, Inc. The contents contained herein, is not associated or endorsed by Cisco Systems, Inc.
Warning And Disclaimer

PLEASE READ THIS SUBSCRIPTION LICENSE AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT.

BY ORDERING THIS PRODUCT YOU ARE CONSENTING TO BE BOUND BY THIS LICENSING AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN DO NOT PURCHASE THIS PRODUCT.

This book is designed to provide information about the Cisco Certified Internetwork Expert (CCIE) Routing and Switching (R&S) Lab 5.0 Exam. Maximum effort has been made to make this book accurate and informative as possible, but no warranty or fitness is implied. You should use this book as a general guide.

The authors, shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

This book is written only with the hope of the author that your reading and understanding the contents will alert you to questions that you should ask and pitfalls which you should attempt to avoid before attempting to take you lab exam.

License Agreement

CCIEv5.0 Routing and Switching Advanced Configuration and Troubleshooting Lab Workbook is copyrighted. In addition, this product is at all times the property of Tom Mark Giembicki and Sean Paul Draper, and the customer shall agree to use this product only for themselves, the licensed user. The license for the specific customer remains valid from the purchase date until they pass their CCIE Routing and Switching lab exam.

CCIEv5.0 Routing and Switching Advanced Configuration and Troubleshooting Lab Workbook materials are licensed by individual customer. This material cannot be resold, transferred, traded, sold, or have the price shared in any way. Each specific individual customer must have a license to use this product. The customer agrees that this product is always the property of Tom Mark Giembicki and Sean Paul Draper, and they are just purchasing a license to use it. A Customer’s license will be revoked if they violate this licensing agreement in any way.

Copies of this material in any form or fashion are strictly prohibited. If for any reason a licensed copy of this material is lost or damaged a new copy will be provided free of charge, except for the cost of printing, shipping and handling.

Individuals or entities that knowingly violate the terms of this licensing agreement may be subject to punitive damages that Tom Mark Giembicki and Sean Paul Draper could seek in civil court. In addition, individuals or entities that knowingly violate the terms of this license agreement may be subject to criminal penalties as are allowed by law.
Term and Termination of License Agreement

This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of written and electronic material of this product.

Customer’s rights under this License will terminate immediately without notice from Tom Mark Giembicki and Sean Paul Draper, if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of material in its possession or control. The license for the specific user remains valid from the purchase date until the user passes their lab exam pertaining to the purchased subscription. Once the customer passes the relevant lab exam the license is terminated and all material written or electronic in their possession or control must be destroyed or returned to Tom Mark Giembicki and Sean Paul Draper.

Waranty

No warranty of any kind is provided with this product. There are no guarantees that the use of this product will help a customer pass any exams, tests, or certifications, or enhance their knowledge in any way. The product is provided on an “AS IS” basis.

In no event will Tom Mark Giembicki and Sean Paul Draper, its suppliers, or licensed resellers be liable for any incurred costs, lost revenue, lost profit, lost data, or any other damages regardless of the theory of liability arising out of use or inability to use this product.
CCIE Exam IOS & Category Changes

Equipment List and IOS Requirements
The lab exam tests any feature that can be configured on the equipment and IOS versions indicated here:

3925 series routers – IOS 15.3(T) – Advanced Enterprise Services
For additional information reference CISCO IOS Configuration guide

Catalyst 3560X series switches running IOS Version 15.0S – Advanced IP Services
For additional information reference CISCO IOS Configuration guide

Version 5 of the CCIE exam is organized into 6 categories versus the existing 11:

- **Network Principles** is a new category that includes foundational topics that are covered only on the written exam.

- **Layer 2 Technologies** predominately covers LAN Switching and WAN circuit technologies.

- **Layer 3 Technologies** covers both interior and exterior routing protocols (RIP, EIGRP, OSPF, ISIS and BGP). Both IPv4 and IPv6 will be included as well as more focus on dual-stack technologies. IP Multicast is no longer a separate category it is included in both the Layer 2 and Layer 3 technology category.

- **VPN Technologies** is a new category that includes Tunnelling and Encryption sub-domains. Tunnelling includes MPLS L2 and L3 VPNs and well as DMVPN and IPv6 Tunnelling techniques. Encryption includes IPsec with pre-shared key. GETVPN is also included but only on the written exam.

- **Infrastructure Security** includes both Device and Network Security with both focusing on features supported in ISR routers and CAT 3K switches. It excludes topics that rely on dynamic crypto (PKI) or any remote servers.

- **Infrastructure Servers** includes System Management, Services, Quality of Service (QoS) and network optimization. QoS was a separate category in version 4 of the exam, it is still included is version 5 of the exam, it is just absorbed in a different category. Layer 2 QoS topics are included on the written exam only.
CCIE exam guidelines update

Topics Added to the CCIE Routing and Switching v5.0 Written Exam:
- Describe basic software architecture differences between IOS and IOS XE
- Identify Cisco Express Forwarding Concepts
- Explain General Network Challenges
- Explain IP, TCP and UDP Operations
- Describe Chassis Virtualization and Aggregation Technologies
- Explain PIM Snooping
- Describe WAN Rate-based Ethernet Circuits
- Describe BGP Fast Convergence Features
- ISIS (for IPv4 and IPv6)
- Describe Basic Layer 2 VPN – Wireline
- Describe Basic L2VPN – LAN Services
- Describe GET VPN
- Describe IPv6 Network Address Translation

Topics Added to the CCIE Routing and Switching v5.0 Written and Lab Exams:
- Interpret Packet Capture
- Implement and Troubleshoot Bidirectional Forwarding Detection
- Implement EIGRP (multi-address) Named Mode
- Implement Troubleshoot and Optimize EIGRP and OSPF Convergence and Scalability
- Implement and Troubleshoot DMVPN (single hub)
- Implement and Troubleshoot IPsec with pre-shared key
- Implement and Troubleshoot IPv6 First Hop Security

Topics Moved from the CCIE® RS v4.0 Lab exam to the CCIE® RS v5.0 Written Exam:
- Describe IPv6 Multicast
- Describe RIPv6 (RIPvng)
- Describe IPv6 Tunneling Techniques
- Describe Device Security using IOS AAA with TACACS+ and Radius
- Describe 802.1x
- Describe Layer 2 QoS
- Identify Performance Routing (PfR)

Topics Removed from the CCIE® RS v4.0 Exam:
- Flexlink ISL Layer 2 Protocol Tunneling
- Frame-Relay (LFI, FR Traffic Shaping)
- WCCP
- IOS Firewall and IPS
- RITE, RMON
- RGMP
- RSVP QoS, WRR/SRR
Lab Exam Guidelines

We would advise that you read the whole workbook before you start. This will give you an understanding of where different technologies will be running in the network and should help you visualize the entire network.

This is one of the most important concepts when dealing with the CCIE R&S lab exam administered by Cisco.

Load the initial configuration files for the routers. Refer to the diagram(s) for the interface connections to other routers.

In the real exam no configuration changes can be made to the Internet routers (marked grey) however throughout this workbook the Internet routers will need to be configured for certain tasks.

All of the devices have been preconfigured with initial configurations.

---

Do a Root Cause Analysis before doing any configuration change

The overall scenario targets full reachability between all sites, unless specified.

Revert to initial configuration if in doubt (“manage devices” menu)

There are many valid solutions, grading is based on outcome.

Points are awarded per item if the solution meets all requirements.

Do not remove any feature preconfigured! ACL, PBR, NAT, CoPP, MQC, ...

Do not change routing protocol(s) boundaries, unless it is the issue!

Do not use static route and redistributions unless explicitly requested to.

Use the validation test to confirm resolution (necessary but not sufficient!)

Do backward verifications using the validation test of each incident

Do not change IP addressing or routing protocols boundaries.

Do not add interfaces unless specified.

Plan for regression tests after completed substantial changes
CCIEv5 Routing & Switching
Advanced Configuration & Troubleshooting Lab#1
Questions & Solutions
CCIEv5 R&S L2/L3 Topology

Copyright © 2015 CCIE4ALL. All rights reserved
LAB#1

San Francisco Group HQ

VLAN TRUNK VTP

Configure SW1 and SW2 with the following:
The VTP domain should be configured to "CCIE_Rocks" (without the quotes)
Ensure that VTP traffic is MD5 secured using a password of CCIE_Rocks? (question mark is part of password)
Use VTP version 2
Configure 802.1q trunk links between the switches according to the Layer 2 Diagram
Only active VLANs should be allowed on trunk links
VLAN 811 MTU(Maximum Transport Unit) should be set to 1400
Ensure that VLAN 999 traffic is not tagged when sent over the trunk links
After synchronization both switches must not propagate VLAN configuration changes to each other

Configuration:

SW1
vtp domain CCIE_Rocks
vtp version 2
vtp password CCIE_Rocks? - see note
vtp mode server
 vlan 811
  mtu 1400

interface range Ethernet1/0 - 1 , Ethernet1/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 1,111,118,119,811,999
 switchport mode trunk

vtp mode transparent

SW2
vtp domain CCIE_Rocks
vtp version 2
vtp password CCIE_Rocks? - see note
vtp mode server
 vlan 811
  mtu 1400

interface range Ethernet1/0 - 1 , interface Ethernet1/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport trunk allowed vlan 1,111,118,119,811,999
 switchport mode trunk

vtp mode transparent
Verification:

SW1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name : CCIE_Rocks
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3300
Configuration last modified by 192.168.10.6 at 12-6-14 09:16:07

Feature VLAN:
--------------
VTP Operating Mode : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision : 0
MD5 digest : 0xD9 0x16 0xB7 0xD6 0x00 0x64 0x8A 0xBE 0x41 0x35 0x4B 0xD0 0xAB 0x6E 0xAD 0xA2

SW2#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name : CCIE_Rocks
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3400
Configuration last modified by 192.168.10.6 at 12-10-14 19:45:05

Feature VLAN:
--------------
VTP Operating Mode : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
Configuration Revision : 0
MD5 digest : 0x68 0xA8 0x6D 0x78 0xC3 0xF6 0xB5 0x94 0x42 0x15 0x53 0x12 0xA3 0x95 0xB1 0x62

SW1#show vtp password
VTP Password: CCIE_Rocks?

SW2#show vtp password
VTP Password: CCIE_Rocks?

SW1#show int trunk
Port Mode Encapsulation Status Native vlan
Et1/0 on 802.1q trunking 999
Et1/1 on 802.1q trunking 999
Et1/3 on 802.1q trunking 999

Port Vlans allowed on trunk
Et1/0 1,111,118-119,811,999
Et1/1 1,111,118-119,811,999
Et1/3 1,111,118-119,811,999

Port Vlans allowed and active in management domain
Et1/0 1,111,118-119,811,999
Et1/1 1,111,118-119,811,999
Et1/3 1,111,118-119,811,999

Port Vlans in spanning tree forwarding state and not pruned
Et1/0 1,111,118-119,811,999
Et1/1 1,111,118-119,811,999
Et1/3 1,111,118-119,811,999
### SW2#sh int trunk

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>999</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>999</td>
</tr>
<tr>
<td>Et1/3</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>999</td>
</tr>
</tbody>
</table>

### SW1#show vlan id 811

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>811 R9-SW1</td>
<td>active</td>
<td>Et0/1, Et0/0, Et1/1, Et1/3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
<th>Stp</th>
<th>BrdgMode</th>
<th>Trans1</th>
<th>Trans2</th>
</tr>
</thead>
<tbody>
<tr>
<td>811 enet</td>
<td>100811</td>
<td>1400</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Primary Secondary Type Ports

### SW2#show vlan id 811

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>811 R9-SW1</td>
<td>active</td>
<td>Et0/0, Et1/0, Et1/1, Et1/3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
<th>Stp</th>
<th>BrdgMode</th>
<th>Trans1</th>
<th>Trans2</th>
</tr>
</thead>
<tbody>
<tr>
<td>811 enet</td>
<td>100811</td>
<td>1400</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Primary Secondary Type Ports

---

**Note:** You can configure the system to recognize a particular keystroke (key combination or sequence) as command aliases. In other words, you can set a keystroke as a shortcut for executing a command. To enable the system to interpret a keystroke as a command, use the either of the following key combinations before entering the command sequence:

Ctrl-V or Esc, Q - Configures the system to accept the following keystroke as a user-configured command entry (rather than as an editing command)
Etherchannel

SW1 and SW2 should run an industry standard Etherchannel. Only Ethernet1/0 and Ethernet1/1 should participate in the Etherchannel configuration. If SW1 detects a loop due to an error in this configuration, it should disable both links. Ensure that SW1 initiate the negotiation whereas SW2 should not attempt to negotiate. Ensure that Ethernet1/0 on SW1 is more likely to transmit the packets over the industry Etherchannel - use the best value possible. For all Etherchannel ports, set the load balancing method so that it is based on source and destination mac-address.

**Configuration:**

**SW1**

```text
interface range ethernet1/0 - 1
   channel-group 12 mode active

interface ethernet1/0
   lacp port-priority 0

interface Port-channel12
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 1,111,118,119,811,999
   switchport mode trunk

   port-channel load-balance src-dst-mac

spanning-tree etherchannel guard misconfig
```

**SW2**

```text
interface range ethernet1/0 - 1
   channel-group 12 mode passive

interface ethernet1/0
   lacp port-priority 0

interface Port-channel12
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 1,111,118,119,811,999
   switchport mode trunk

   port-channel load-balance src-dst-mac

spanning-tree etherchannel guard misconfig
```

**Verification:**

```text
SW1#show etherchannel summary | be Num
Number of channel-groups in use: 1
Number of aggregators:          1

Group     Port-channel  Protocol     Ports
---       --------     -----     -------
12         Po12 (SU)     LACP     E1/0(P)  E1/1(P)
```
SW2#sh etherc summ | be Gro
Group Port-channel Protocol Ports
12 Po12(SU)    LACP    Et1/0(P)    Et1/1(P)

SW1#show int po12 switchport
Name: Po12
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,111,118,119,811,999
Pruning VLANs Enabled: 2-1001
Appliance trust: none

SW1#show etherchannel 12 detail
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max port-channels = 16
Protocol: LACP
Minimum Links: 0
Ports in the group:

Port: Et1/0
---
Port state = Up Mstr Assoc In-Bndl
Channel group = 12 Mode = Active
Port-channel = Po12 GC = -
Port index = 0 Load = 0x00
Flags: S - Device is sending Slow LACPDU's F - Device is sending fast LACPDU's.
A - Device is in active mode. P - Device is in passive mode.
Local information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SA</td>
<td>bndl</td>
<td>0x0C</td>
<td>0x101</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SP</td>
<td>0</td>
<td>aabb.cc00-3400</td>
<td>2s</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:02m:39s

Port: Et1/1
---
Port state = Up Mstr Assoc In-Bndl
Channel group = 12 Mode = Active
Port-channel = Po12 GC = -
Port index = 0 Load = 0x00
Flags: S - Device is sending Slow LACPDU's F - Device is sending fast LACPDU's.
A - Device is in active mode. P - Device is in passive mode.
Local information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td></td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SP</td>
<td>32768</td>
<td>aabb.cc00-3400</td>
<td>1s</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:02m:39s
SW2#show etherchannel 12 detail
Group state = L2
Ports: 2  Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
Minimum Links: 0

Ports in the group:

Port: Et1/0
----------------------
Channel group = 12  Mode = Passive
Port-channel = Po12  GC = -
Port index = 0  Load = 0x00
Flags:  S - Device is sending Slow LACPDU s
A - Device is in active mode.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SP</td>
<td>bndl</td>
<td>0</td>
<td>0xC</td>
<td>0xC</td>
<td>0x101</td>
<td>0x3C</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SA</td>
<td>32768</td>
<td>aabb.cc00.3300</td>
<td>23s</td>
<td>0x0</td>
<td>0xC</td>
<td>0x101</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:01m:14s

Port: Et1/1
----------------------
Channel group = 12  Mode = Passive
Port-channel = Po12  GC = -
Port index = 0  Load = 0x00
Flags:  S - Device is sending Slow LACPDU s
A - Device is in active mode.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SP</td>
<td>bndl</td>
<td>32768</td>
<td>0xC</td>
<td>0xC</td>
<td>0x102</td>
<td>0x3C</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SA</td>
<td>32768</td>
<td>aabb.cc00.3300</td>
<td>26s</td>
<td>0x0</td>
<td>0xC</td>
<td>0x102</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:01m:16s

Port-channels in the group:

Port-channel: Po12  (Primary Aggregator)
----------------------
Age of the Port-channel = 0d:00h:01m:42s
Logical slot/port = 16/1  Number of ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Port security = Disabled

Ports in the Port-channel:

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x0</td>
<td>Et1/0</td>
<td>Active</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0x0</td>
<td>Et1/1</td>
<td>Active</td>
<td>0</td>
</tr>
</tbody>
</table>

Time since last port bundled: 0d:00h:00m:37s  Et1/1
### SW1# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
```
src-dst-mac
```
EtherChannel Load-Balancing Addresses Used Per-Protocol:
- **Non-IP**: Source XOR Destination MAC address
- **IPv4**: Source XOR Destination MAC address
- **IPv6**: Source XOR Destination MAC address

### SW1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0111, VLAN0118-VLAN0119, VLAN0811, VLAN0999
Extended system ID is enabled
PortFast Default is disabled
PortFast BPDU Guard Default is disabled
PortFast BPDU Filter Default is disabled
Loopguard Default is disabled
**EtherChannel misconfig guard is enabled**
Configured Pathcost method used is short
UplinkFast is disabled
BackboneFast is disabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>VLAN0111</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VLAN0118</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>VLAN0119</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>VLAN0811</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>VLAN0999</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

6 vlans 0 0 0 16 16

### SW2# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID is enabled
PortFast Default is disabled
PortFast BPDU Guard Default is disabled
PortFast BPDU Filter Default is disabled
Loopguard Default is disabled
**EtherChannel misconfig guard is enabled**
Configured Pathcost method used is short
UplinkFast is disabled
BackboneFast is disabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>VLAN0111</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>VLAN0118</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>VLAN0119</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>VLAN0811</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>VLAN0999</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

6 vlans 6 0 0 10 16
**Note: Spanning Tree**

The multiple spanning-tree (MST) implementation is based on the IEEE 802.1s standard. The per-VLAN spanning-tree plus (PVST+) protocol is based on the IEEE 802.1D standard and Cisco proprietary extensions. The rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- **Root**—A forwarding port elected for the spanning-tree topology
- **Designated**—A forwarding port elected for every switched LAN segment
- **Alternate**—A blocked port providing an alternate path to the root bridge in the spanning tree
- **Backup**—A blocked port in a loopback configuration

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch. In a switch stack, all switches use the same bridge ID for a given spanning-tree instance.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface

When selecting the root port on a switch stack, spanning tree follows this sequence:

- Selects the lowest root bridge ID
- Selects the lowest path cost to the root switch
- Selects the lowest designated bridge ID
- Selects the lowest designated path cost
- Selects the lowest port ID

*directly from Cisco website*
Spanning-Tree MST

All odd VLANs in your network must be assigned to Spanning-tree instance 1
All even VLANs in your network must be assigned to Spanning-tree instance 2
All other VLANs in your network must be assigned to Spanning-tree instance 3
Use domain name as “CISCO” without the quotes and set revision to the lowest value
Ensure SW1 is root switch for instance 1 and backup root switch for instance 2
Ensure SW2 is root switch for Instance 2 and backup root switch for instance 1
Ensure that BPDU received on the ports connecting routers have no effect to your spanning tree decision
Spanning-tree process should wait 30 seconds before it attempts to re-converge if it didn’t receive any spanning-tree configuration messages

Configuration:

**SW1**

```yaml
spanning-tree mode mst

  spanning-tree mst configuration
  name CISCO
  revision 1
  instance 1 vlan 111, 119, 811, 999
  instance 2 vlan 118
  instance 3 vlan 1-4094

spanning-tree mst max-age 30

spanning-tree mst 1 root primary
spanning-tree mst 2 root secondary

interface Ethernet 0/0
  spanning-tree bpduguard disable
  spanning-tree guard root

interface Ethernet 0/1
  spanning-tree bpduguard disable
  spanning-tree guard root

interface Ethernet 0/2
  spanning-tree bpduguard disable
  spanning-tree guard root
```

**SW2**

```yaml
spanning-tree mode mst

  spanning-tree mst configuration
  name CISCO
  revision 1
  instance 1 vlan 111, 119, 811, 999
  instance 2 vlan 118
  instance 3 vlan 1-4094

spanning-tree mst max-age 30

spanning-tree mst 2 root primary
spanning-tree mst 1 root secondary

interface Ethernet 0/0
  spanning-tree bpduguard disable
```
spanning-tree guard root

interface Ethernet0/1
spanning-tree bpduguard disable
spanning-tree guard root

interface Ethernet0/2
spanning-tree bpduguard disable

interface Ethernet0/3
spanning-tree bpduguard disable
spanning-tree guard root

interface Ethernet1/2
spanning-tree bpduguard disable
spanning-tree guard root

Verification:

SW1#show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0-MST1, MST3
Extended system ID is enabled
Portfast Default is disabled
Portfast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short (Operational value is long)
UplinkFast is disabled
BackboneFast is disabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>MST1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>MST2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>MST3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4 msts</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>16</td>
</tr>
</tbody>
</table>

SW2#sh spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST2
Extended system ID is enabled
Portfast Default is disabled
Portfast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short (Operational value is long)
UplinkFast is disabled
BackboneFast is disabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>MST1</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>MST2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>MST3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>4 msts</td>
<td>6</td>
<td>0</td>
<td>11</td>
<td>3</td>
<td>20</td>
</tr>
</tbody>
</table>
### SW1#sh spanning-tree mst 1

#### MST1
- vlans mapped: 111,119,811,999

**Bridge**
- address aabb.cc00.3300
- priority: 24577 (24576 sysid 1)

**Root**
- this switch for MST1

**Interface**
- Role Sts Cost Prio.Nbr Type

<table>
<thead>
<tr>
<th>Port</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/1</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>Et1/3</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.36</td>
<td>Shr</td>
</tr>
<tr>
<td>Po12</td>
<td>Desg</td>
<td>FWD</td>
<td>1000000</td>
<td>128.514</td>
<td>Shr</td>
</tr>
</tbody>
</table>

### SW1#sh spanning-tree mst 2

#### MST2
- vlans mapped: 118

**Bridge**
- address aabb.cc00.3300
- priority: 28674 (28672 sysid 2)

**Root**
- this switch for MST2

**Interface**
- Role Sts Cost Prio.Nbr Type

<table>
<thead>
<tr>
<th>Port</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/2</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.3</td>
<td>Shr</td>
</tr>
<tr>
<td>Et1/3</td>
<td>Altn</td>
<td>BLK</td>
<td>2000000</td>
<td>128.36</td>
<td>Shr</td>
</tr>
<tr>
<td>Po12</td>
<td>Root</td>
<td>FWD</td>
<td>1000000</td>
<td>128.514</td>
<td>Shr</td>
</tr>
</tbody>
</table>

### SW2#sh spanning-tree mst 1

#### MST1
- vlans mapped: 111,119,811,999

**Bridge**
- address aabb.cc00.3400
- priority: 28673 (28672 sysid 1)

**Root**
- this switch for MST1

**Interface**
- Role Sts Cost Prio.Nbr Type

<table>
<thead>
<tr>
<th>Port</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/1</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>Et0/2</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.3</td>
<td>Shr</td>
</tr>
<tr>
<td>Et0/3</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.4</td>
<td>Shr</td>
</tr>
<tr>
<td>Et1/2</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.35</td>
<td>Shr</td>
</tr>
<tr>
<td>Et1/3</td>
<td>Altn</td>
<td>BLK</td>
<td>2000000</td>
<td>128.36</td>
<td>Shr</td>
</tr>
<tr>
<td>Po12</td>
<td>Root</td>
<td>FWD</td>
<td>1000000</td>
<td>128.514</td>
<td>Shr</td>
</tr>
</tbody>
</table>

### SW2#sh spanning-tree mst 2

#### MST2
- vlans mapped: 118

**Bridge**
- address aabb.cc00.3400
- priority: 24578 (24576 sysid 2)

**Root**
- this switch for MST2

**Interface**
- Role Sts Cost Prio.Nbr Type

<table>
<thead>
<tr>
<th>Port</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/3</td>
<td>Desg</td>
<td>FWD</td>
<td>2000000</td>
<td>128.36</td>
<td>Shr</td>
</tr>
<tr>
<td>Po12</td>
<td>Desg</td>
<td>FWD</td>
<td>1000000</td>
<td>128.514</td>
<td>Shr</td>
</tr>
</tbody>
</table>

### SW1#show spanning-tree mst configuration

**Name** [CISCO]
**Revision** 1
**Instances configured** 4

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>1</td>
<td>111,119,811,999</td>
</tr>
<tr>
<td>2</td>
<td>118</td>
</tr>
<tr>
<td>3</td>
<td>1-110,112-117,120-810,812-998,1000-4094</td>
</tr>
</tbody>
</table>
show spanning-tree bridge

<table>
<thead>
<tr>
<th>MST Instance</th>
<th>Bridge ID</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Fwd Dly</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td>32768 (32768, 0)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST1</td>
<td>24577 (24576, 1)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST2</td>
<td>28674 (28672, 2)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST3</td>
<td>32771 (32768, 3)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
</tbody>
</table>

sw spanning-tree mst configuration

Name: [CISCO]
Revision: 1
Instances configured: 4

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>1</td>
<td>111,119,811,999</td>
</tr>
<tr>
<td>2</td>
<td>118</td>
</tr>
<tr>
<td>3</td>
<td>1-110,112-117,120-810,812-998,1000-4094</td>
</tr>
</tbody>
</table>

show spanning-tree bridge

<table>
<thead>
<tr>
<th>MST Instance</th>
<th>Bridge ID</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Fwd Dly</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td>32768 (32768, 0)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST1</td>
<td>24577 (24576, 1)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST2</td>
<td>28673 (28672, 2)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
<tr>
<td>MST3</td>
<td>32771 (32768, 3)</td>
<td>aabb.cc00.3300</td>
<td>2</td>
<td>30</td>
<td>15 mstp</td>
</tr>
</tbody>
</table>

SWI# sh spanning-tree mst interface et 0/1

Ethernet0/1 of MST0 is designated forwarding
Port guard: root (root)
bpdu filter: disable (default)
Bpdus sent 536, received 0

Instance | Role | Sts | Cost | Prio.Nbr | Vlans mapped |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Desg FWD</td>
<td>2000000</td>
<td>128.2</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Desg FWD</td>
<td>2000000</td>
<td>128.2</td>
<td>111,119,811,999</td>
<td></td>
</tr>
</tbody>
</table>

SW2# sh spanning-tree mst interface et 0/2

Ethernet0/2 of MST0 is designated forwarding
Port guard: root (root)
bpdu filter: disable (default)
Bpdus sent 573, received 0

Instance | Role | Sts | Cost | Prio.Nbr | Vlans mapped |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Desg FWD</td>
<td>2000000</td>
<td>128.3</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Desg FWD</td>
<td>2000000</td>
<td>128.3</td>
<td>111,119,811,999</td>
<td></td>
</tr>
</tbody>
</table>
Spanning-Tree Tuning

Ensure that interface Ethernet1/3 is in the forwarding state for MST instance 2 on SW1. You are not allowed to accomplish this by making any changes on SW2. Ensure that spanning tree does consider high speed links in across your infrastructure.

**Note:** “By default Cisco switches use the original spanning tree “short mode” path costs using a 16-bit value. However, as interface bandwidth has increased the 16-bit value does not provide room for future high-speed interfaces. Using the newer spanning tree “long mode” path cost using a 32-bit value provides more granularity in data centers that use extremely high-speed interfaces.”

Following is a table of links speeds and the old and new values for comparison:

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Old STP value</th>
<th>New Long STP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>100</td>
<td>2,000,000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>19</td>
<td>200,000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>4</td>
<td>20,000</td>
</tr>
<tr>
<td>N X 1 Gbps</td>
<td>3</td>
<td>10,000</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2</td>
<td>2,000</td>
</tr>
<tr>
<td>100 Gbps</td>
<td>N/A</td>
<td>200</td>
</tr>
<tr>
<td>1 Tbps</td>
<td>N/A</td>
<td>20</td>
</tr>
<tr>
<td>10 Tbps</td>
<td>N/A</td>
<td>2</td>
</tr>
</tbody>
</table>

**Configuration:**

**SW1**

```
interface Ethernet1/3
  spanning-tree mst 2 cost 1
  spanning-tree pathcost method long
```

**SW2**

```
  spanning-tree pathcost method long
```

**Verification: Before Implementation**

```
SW1#show spanning-tree mst 2
  vlans mapped: 118
  Bridge address aabb.cc00.3300 priority 28674 (28672 sysid 2)
  Root address aabb.cc00.3400 priority 24578 (24576 sysid 2)
  Interface Role Sts Cost Priority Nbr Type
  -------------- ------- ----- -------- ------- -----
  Et0/2 Desg FW 2000000 128.3    Shr
  Et1/3 Altn BLK 2000000 128.36   Shr
  Po12 Root FW 1000000 128.514  Shr

SW1#show spanning-tree pathcost method
Spanning tree default pathcost method used is long (Operational value is long)

SW2#show spanning-tree pathcost method
Spanning tree default pathcost method used is short (Operational value is long)
```
Verification: After Implementation

SW1#show spanning-tree mst 2

##### MST2 vlans mapped: 118
Bridge address aabb.cc00.3300 priority 28674 (28672 sysid 2)
Root address aabb.cc00.3400 priority 24578 (24576 sysid 2)

<table>
<thead>
<tr>
<th>Bridge</th>
<th>address</th>
<th>priority</th>
<th>sysid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aabb.cc00.3300</td>
<td>28674</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>aabb.cc00.3400</td>
<td>24578</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/3</td>
<td>Root</td>
<td>FWD</td>
<td>1</td>
<td>128.36</td>
<td>Shr</td>
</tr>
</tbody>
</table>

SW1#show spanning-tree pathcost method

Spanning tree default pathcost method used is long

SW2#show spanning-tree pathcost method

Spanning tree default pathcost method used is long
Layer 2 Security

R9’s interface Ethernet2/0 mac-address should appear as `aabb.bbaa.dddd`
SW2 should only allow this single MAC address on its interface connecting to R9
SW2 should statically learn R9’s Ethernet2/0 mac-address
If a violation occurs ensure that the switchport is placed in the mode that generates a log locally and
will also send the log to a syslog server 192.168.101.101
Ensure that aging time defines the period of inactivity after which all the dynamically learned secure
addresses age out

**Note:** You should receive a similar output when port security is violated

```
SW2(config)#no service timestamps debug
SW2#debug port-security
All Port Security debugging is on
PSECURE: Violation/duplicate detected upon receiving `aabb.cc00.0902` on vlan 119:
port_num_addrs 1 port_max_addrs 1 vlan_addr_ct 1 vlan_addr_max 1 total_addrs 0:
max_total_addrs 4096
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
aabb.cc00.0902 on port Ethernet0/2.
PSECURE: Security violation, TrapCount:1
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.101.101 port 514 started - CLI initiated
```

```
SW2#sh port-security int et 0/2
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : `aabb.cc00.0902`:119
Security Violation Count   : 1
```

**Configuration:**

**R9**
```
interface Ethernet2/0
mac-address aabb.bbaa.dddd
```

**SW2**
```
interface Ethernet0/2
switchport port-security
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address aabb.bbaa.dddd
loggin on
logging host 192.168.101.101
```
Verification:

```bash
SW2#sh port-security int et 0/2
Port Security : Enabled
Port Status    : Secure-up
Violation Mode : Restrict
Aging Time    : 0 mins
Aging Type     : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : aabb.bbaa.ddd8119
Security Violation Count : 0
```
CDP

R8 should send CDP announcement every 10 seconds and instruct other devices to hold the updates for 40 seconds.

Unsure that CDP packets are not sent or received on its connection to R96.

Disable logging of duplex mismatch detected via CDP messages.

Use the Loopback0 interface for IP address advertisements in CDP messages.

**Configuration:**

```
R8
   no cdp log mismatch duplex
   cdp source-interface Loopback0
   cdp timer 10
   cdp holdtime 40
   interface Ethernet0/0
   no cdp enable
```

**Verification:**

```
R8#sh cdp
   Global CDP information:
      Sending CDP packets every 10 seconds
      Sending a holdtime value of 40 seconds
      Sending CDPv2 advertisements is enabled
      Source interface is Loopback0

R8#sh cdp interface
   Ethernet1/0 is up, line protocol is up
      Encapsulation ARPA
      Sending CDP packets every 10 seconds
      Holdtime is 40 seconds
   Ethernet2/0 is up, line protocol is up
      Encapsulation ARPA
      Sending CDP packets every 10 seconds
      Holdtime is 40 seconds
   Ethernet3/0 is up, line protocol is up
      Encapsulation ARPA
      Sending CDP packets every 10 seconds
      Holdtime is 40 seconds

   cdp enabled interfaces : 3
   interfaces up          : 3
   interfaces down        : 0

R8#sh cdp traffic
   CDP counters :
      Total packets output: 524, Input: 400
      Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
      No memory: 0, Invalid packet: 0
      CDP version 1 advertisements output: 0, Input: 0
      CDP version 2 advertisements output: 524, Input: 400

R8#sh cdp interface et 0/0
   CDP is not enabled on interface Ethernet0/0

R8#sh cdp neighbors et0/0 detail
   Total cdp entries displayed : 0
```
Service Provider#9

VLAN TRUNK VTP

The VTP domain should be configured to "CCIEv5" (without quotes)
VTP traffic should be secured using a password of Cisco? (question mark is part of password)
Configure VTP version 2
SW5 should be the only switch in the layer 2 domain that can modify the VLAN database
Configure SW5 so that the Loopback0 interface is the mandatory source for the VTP updates
Configure the switches so that when they do not require a VLAN locally they inform SW5 that the VLAN is no longer required. Configure only the VTP Server switch and verify and that the configuration was propagated to the VTP Client switches
Ensure SW5 stores the VTP configuration information file as "ccievtp.txt" – without quotes
Ensure that only dot1q encapsulation is supported

Configuration:

**SW3**

```
vtp domain CCIEv5
vtp version 2
vtp password Cisco(Esc+Q)? - see note
vtp mode client

int ran et 0/0 - 2 , et 1/0 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

**SW4**

```
vtp domain CCIEv5
vtp version 2
vtp password Cisco(Esc+Q)? - see note
vtp mode client

int ran et 0/0 - 2 , et 1/0 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

**SW5**

```
vtp domain CCIEv5
vtp version 2
vtp password Cisco(Esc+Q)? - see note
vtp mode server
vtp pruning

vtp interface Loopback0 only
vtp file ccievtp.txt

int ran et 0/0 - 2 , et 1/0 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

Verification:
SW5#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : CCIEv5
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.3700
Configuration last modified by 172.105.105.105 at 12-6-14 10:38:05
Local updater ID is 172.105.105.105 on interface Lo0 (preferred interface)
Preferred interface name is Loopback0 (mandatory)

Feature VLAN:
-------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 29
Configuration Revision            : 28
MD5 digest                        : 0xBF 0x4A 0x2D 0xAD 0x2D 0x64 0x67 0x55
                                      0x22 0xD0 0xF2 0xB3 0xBE 0xA1 0xB1 0x6E

SW5#show vtp password
VTP Password: Cisco?

SW5#dir flash:
Directory of flash:
58057 -rw-  2882  Sep 20 2014 18:23:38 +01:00  running-config
58015 -rw-  2004  Dec 6 2014 11:33:17 +01:00  vlan.dat-00055
58077 -rw-  2004  Dec 6 2014 11:38:05 +01:00  ccievtp.txt
214749552 bytes total (214749552 bytes free)

SW5#more flash:ccievtp.txt
00000000: BADB100D 00000002 02064343 49457635      :[.. ..... ..CC IEv5
00000010: 00000000 00000000 00000000 00000000 .... ..... .... ...
00000020: 00000000 00000000 00000000 0000001C .... ..... .... ...
00000030: AC696969 00000001 31343132 30363130 ,iii .... 1412 0610
00000040: 333833035 BF4A2DAD 2D646755 22D0F2B3 3805 ?J-- -dgU "Pr3
00000050: BEA1B16E 06436973 636F3F00 00000000 >!ln .Cis co?. .... 
00000060: 00000000 00000000 00000000 00000000 .... ..... .... ...
00000070: 00000000 00000000 00000000 00000000 .... ..... .... ...
00000080: 00000000 00000000 00000000 00000000 .... ..... .... ...
00000090: 00000000 00000000 000100D1 01010131 AD4A520D .... ..... .... ..-J
000000A0: 07646566 61756C74 00000000 00000000 .def ault ..... .... 
000000B0: 00000000 00000000 00000000 00000000 .... ..... .... ...
SW3#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name     : CCIEv5
VTP Pruning Mode    : Enabled
VTP Traps Generation: Disabled
Device ID           : aabb.cc00.3500

Configuration last modified by 172.105.105.105 at 12-6-14 10:38:05

Feature VLAN:
-------------
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 29
Configuration Revision      : 28
MD5 digest                  :

0xBF 0x4A 0x2D 0xAD 0x2D 0x64 0x67 0x55
0x22 0xD 0 0xF2 0xB3 0xBE 0xA1 0xB1 0x6E

SW5#show int trunk
Port        Mode         Encapsulation Status      Native vlan
Et0/0       on           802.1q         trunking      1
Et0/1       on           802.1q         trunking      1
Et0/2       on           802.1q         trunking      1
Et1/0       on           802.1q         trunking      1
Et1/1       on           802.1q         trunking      1
Et1/2       on           802.1q         trunking      1
Et1/3       on           802.1q         trunking      1
Et2/0       on           802.1q         trunking      1
Et2/1       on           802.1q         trunking      1
Et2/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094
Et0/2       1-4094
Et1/0       1-4094
Et1/1       1-4094
Et1/2       1-4094
Et1/3       1-4094
Et2/0       1-4094
Et2/1       1-4094

Port        Vlans allowed on trunk
Et2/3       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et0/1       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et0/2       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et1/0       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et1/1       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et1/2       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et1/3       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et2/0       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et2/1       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et2/3       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et0/1       none
Et0/2       none
Et1/0       none
Et1/1       none
Et1/2       none
Et1/3       none
Et2/0       none
Et2/1       none
Et2/3       none

Port        Vlans in spanning tree forwarding state and not pruned
Et2/1       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
Et2/3       1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
SW5#show int ethernet 0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANS: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none

Trunking VLANS Enabled: ALL
Pruning VLANS Enabled: 2-1001
Capture Mode Disabled
Capture VLANS Allowed: ALL
Appliance trust: none

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et0/2</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/2</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et2/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et2/2</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et0/1</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et0/2</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/0</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/2</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et2/1</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et2/2</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et0/1</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et0/2</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et1/0</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et1/2</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et2/1</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et2/2</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et0/1</td>
<td>none</td>
</tr>
<tr>
<td>Et0/2</td>
<td>none</td>
</tr>
<tr>
<td>Et1/0</td>
<td>1</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1</td>
</tr>
<tr>
<td>Et1/2</td>
<td>1</td>
</tr>
<tr>
<td>Et2/1</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Et2/2</td>
<td>1,12-17,23-24,35,46,57,67,92-97,221-223,321-323</td>
</tr>
<tr>
<td>Port</td>
<td>Mode</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>Et0/0</td>
<td>on</td>
</tr>
<tr>
<td>Et0/1</td>
<td>on</td>
</tr>
<tr>
<td>Et0/2</td>
<td>on</td>
</tr>
<tr>
<td>Et1/0</td>
<td>on</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
</tr>
<tr>
<td>Et1/2</td>
<td>on</td>
</tr>
<tr>
<td>Et1/3</td>
<td>on</td>
</tr>
<tr>
<td>Et2/2</td>
<td>on</td>
</tr>
<tr>
<td>Et3/1</td>
<td>on</td>
</tr>
</tbody>
</table>

### Port Vlans allowed on trunk
- Et0/0: 1-4094
- Et0/1: 1-4094
- Et0/2: 1-4094
- Et1/0: 1-4094
- Et1/1: 1-4094
- Et1/2: 1-4094
- Et1/3: 1-4094
- Et2/2: 1-4094
- Et3/1: 1-4094

### Port Vlans allowed and active in management domain
- Et0/0: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et0/1: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et0/2: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et1/0: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et1/1: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et1/2: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et1/3: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et2/2: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et3/1: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323

### Port Vlans in spanning tree forwarding state and not pruned
- Et0/0: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et0/1: 1
- Et0/2: 1
- Et1/0: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et1/1: 1
- Et1/2: 1
- Et1/3: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et2/2: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323
- Et3/1: 1,12-17,23-24,35,46,57,67,92-97,221-223,321-323

**Note:** You can configure the system to recognize a particular keystroke (key combination or sequence) as command aliases. In other words, you can set a keystroke as a shortcut for executing a command. To enable the system to interpret a keystroke as a command, use the either of the following key combinations before entering the command sequence:

- **Ctrl-V** or **Esc, Q** - Configures the system to accept the following keystroke as a user-configured command entry (rather than as an editing command)
Etherchannel

All switches should run the Cisco proprietary Etherchannel Bundle only the following ports into an Etherchannel on each switch:

- SW5 Ethernet 0/0, 0/1, 1/0, 1/1
- SW4 Ethernet 1/0, 1/1
- SW3 Ethernet 1/0, 1/1

Do not configure an Etherchannel between SW3 and SW4

Ensure that SW5 initiate the negotiation whereas SW3 and SW4 should not attempt to negotiate

Ensure that Ethernet0/0 and Ethernet1/0 on SW5 are more likely to transmit the packets over the proprietary Etherchannel, use the best value possible

Ensure that traffic is distributed on individual Ethernet trunks between switches based on the destination MAC address of individual flows

Ensure when any of the interfaces starts flapping they are shut down dynamically by all switches; if they remain stable for 35 seconds, they should be re-enabled

**Configuration:**

**SW5**

```config
interface range Ethernet0/0 - 1
    channel-group 35 mode desirable

interface Ethernet0/0
    pagp port-priority 255

interface range Ethernet1/0 - 1
    channel-group 45 mode desirable

interface Ethernet1/0
    pagp port-priority 255

port-channel load-balance dst-mac
errdisable recovery cause link-flap
errdisable recovery interval 35
```

**SW4**

```config
interface range Ethernet1/0 - 1
    channel-group 45 mode auto

port-channel load-balance dst-mac
errdisable recovery cause link-flap
errdisable recovery interval 35
```

**SW3**

```config
interface range Ethernet1/0 - 1
    channel-group 35 mode auto

port-channel load-balance dst-mac
errdisable recovery cause link-flap
errdisable recovery interval 35
```
Verification:

SW5#sh etherc summ
Flags:  D - down  P - bundled in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)  R - Layer3
        S - Layer2  U - in use  F - failed to allocate aggregator
        N - not in use, minimum links not met
        W - unsuitable for bundling
        D - default port
Number of channel-groups in use: 2
Number of aggregators: 2

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>Po35 (SU)</td>
<td>PAgP</td>
<td>Et0/0(P) Et0/1(P)</td>
</tr>
<tr>
<td>45</td>
<td>Po45 (SU)</td>
<td>PAgP</td>
<td>Et1/0(P) Et1/1(P)</td>
</tr>
</tbody>
</table>

SW3#sh etherc summ | be Num
Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>Po35 (SU)</td>
<td>PAgP</td>
<td>Et1/0(P) Et1/1(P)</td>
</tr>
</tbody>
</table>

SW4#sh etherc summ | be Num
Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>Po45 (SU)</td>
<td>PAgP</td>
<td>Et1/0(P) Et1/1(P)</td>
</tr>
</tbody>
</table>

SW5#sh etherc port-channel
Channel-group listing:

Group: 35

Port-channels in the group:

Port-channel: Po35
Age of the Port-channel = 0d:00h:02m:48s
Logical slot/port = 16/1 Number of ports = 2
GC = 0x00230001 HotStandBy port = null
Port state = Port-channel Ag-INuse
Protocol = PAgP
Port security = Disabled
Ports in the Port-channel:
<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Et0/0</td>
<td>Desirable-S1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Et0/1</td>
<td>Desirable-S1</td>
<td>0</td>
</tr>
</tbody>
</table>
Time since last port bundled: 0d:00h:02m:11s

Group: 45

Port-channels in the group:

Port-channel: Po45
Age of the Port-channel = 0d:00h:02m:47s
Logical slot/port = 16/2 Number of ports = 2
GC = 0x002D0001 HotStandBy port = null
Port state = Port-channel Ag-INuse
Protocol = PAgP
Port security = Disabled
Ports in the Port-channel:
<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/0</td>
<td>Desirable-S1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/1</td>
<td>Desirable-S1</td>
<td>0</td>
</tr>
</tbody>
</table>
Time since last port bundled: 0d:00h:01m:43s
SW5#sh etherc detail

Channel-group listing:

----------------------
Group: 35
Group state = L2
Port-channels: 1 Max Port-channels = 1
Protocol:  PAgP
Minimum Links: 0

Ports in the group:

----------------------
Port: Et0/0

Channel group = 35 Mode = Desirable-S1 Gcchange = 0
Port-channel = Po35 GC = 0x00230001 Pseudo port-channel = Po35
Protocol = PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
A - Device is in Auto mode.  P - Device learns on physical port.
d - PAgP is down.

Timers:  H - Hello timer is running.  Q - Quit timer is running.
S - Switching timer is running.  I - Interface timer is running.

Local information:

Port Flags State Timers Interval Count Priority Method iface
Et0/0 SC U6/S7 H 30s 1 255 Any 19

Partner's information:

Port Name Partner Group Device ID  Port Flags Cap.
Et0/0 SW3  aabb.cc00.3500 Et1/0 5s SAC 230001

Age of the port in the current state: 0d:00h:05m:32s

Port: Et0/1

Channel group = 35 Mode = Desirable-S1 Gcchange = 0
Port-channel = Po35 GC = 0x00230001 Pseudo port-channel = Po35
Protocol = PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
A - Device is in Auto mode.  P - Device learns on physical port.
d - PAgP is down.

Timers:  H - Hello timer is running.  Q - Quit timer is running.
S - Switching timer is running.  I - Interface timer is running.

Local information:

Port Flags State Timers Interval Count Priority Method iface
Et0/1 SC U6/S7 H 30s 1 128 Any 19

Partner's information:

Port Name Device ID  Port Flags Cap.
Et0/1 SW3  aabb.cc00.3500 Et1/1 5s SAC 230001

Age of the port in the current state: 0d:00h:05m:34s

Port-channel: Po35

Age of the Port-channel = 0d:00h:05m:34s
Logical slot/port  = 16/1 Number of ports = 2
GC = 0x00230001 HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = PAgP
Port security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits
0 00 Et0/0 Desirable-S1 0
0 00 Et0/1 Desirable-S1 0

Time since last port bundled: 0d:00h:05m:32s Et0/0
Group: 45
----------
Group state = L2
Ports: 2  Maxports = 8
Port-channels: 1  Max Port-channels = 1
Protocol: PAgP
Minimum Links: 0

Ports in the group:
-------------------

Port: Et1/0
--------
Port state = Up Mstr In-Bndl
Channel group = 45  Mode = Desirable-S1  Gcchange = 0
Port-channel = Po45  GC = 0x002D0001  Pseudo port-channel = Po45
Port index = 0  Load = 0x00
Flags: S - Device is sending Slow hello.  A - Device is in Auto mode.
       C - Device is in Consistent state.  P - Device learns on physical port.
       d - PAgP is down.
Timers: H - Hello timer is running.  Q - Quit timer is running.
       S - Switching timer is running.  I - Interface timer is running.

Local information:
-------------------
Port Flags State Timers Interval Count Priority Method Ifindex
Et1/0  SC U6/S7 H 30s 1 255 Any 20

Partner's information:
-----------------------
Port Name Device ID Port Age Flags Cap.
Et1/0  SW4  aabb.cc00.3600 Et1/0 20s SAC 2D0001

Port: Et1/1
--------
Port state = Up Mstr In-Bndl
Channel group = 45  Mode = Desirable-S1  Gcchange = 0
Port-channel = Po45  GC = 0x002D0001  Pseudo port-channel = Po45
Port index = 0  Load = 0x00
Flags: S - Device is sending Slow hello.  A - Device is in Auto mode.
       C - Device is in Consistent state.  P - Device learns on physical port.
       d - PAgP is down.
Timers: H - Hello timer is running.  Q - Quit timer is running.
       S - Switching timer is running.  I - Interface timer is running.

Local information:
-------------------
Port Flags State Timers Interval Count Priority Method Ifindex
Et1/1  SC U6/S7 H 30s 1 128 Any 20

Partner's information:
-----------------------
Port Name Device ID Port Age Flags Cap.
Et1/1  SW4  aabb.cc00.3600 Et1/0 26s SAC 2D0001

Port-channel: Po45
-------------------
Age of the Port-channel = 0d:00h:06m:08s
Logical slot/port = 16/2  Number of ports = 2
GC = 0x002D0001  HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = PAgP
Port security = Disabled

Ports in the Port-channel:
--------------------------
Index Load Port EC state No of bits
0 0 00  Et1/0 Desirable-S1 0
0 0 00  Et1/1 Desirable-S1 0

Time since last port bundled: 0d:00h:05m:04s  Et1/0
SW3#sh etherc port-channel
Channel-group listing:
-------------
Group: 35
-------------
Port-channels in the group:
Port-channel: Po35
-------------
Age of the Port-channel = 0d:00h:08m:25s
Logical slot/port = 16/1
Number of ports = 2
GC = 0x00230001
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = PAgP
Port security = Disabled
Ports in the Port-channel:
- Index Load Port EC state No of bits
  - 0 0 0 00 Et1/0 Automatic-S1 0
  - 0 0 0 00 Et1/1 Automatic-S1 0
Time since last port bundled: 0d:00h:08m:10s Et1/0

SW4#sh etherc port-channel
Channel-group listing:
-------------
Group: 45
-------------
Port-channels in the group:
Port-channel: Po45
-------------
Age of the Port-channel = 0d:00h:08m:56s
Logical slot/port = 16/1
Number of ports = 2
GC = 0x002D0001
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = PAgP
Port security = Disabled
Ports in the Port-channel:
- Index Load Port EC state No of bits
  - 0 0 0 00 Et1/0 Automatic-S1 0
  - 0 0 0 00 Et1/1 Automatic-S1 0
Time since last port bundled: 0d:00h:08m:28s Et1/0

SW3#sh etherc detail
Channel-group listing:
-------------
Group: 35
-------------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: PAgP
Minimum Links: 0

Port: Et1/0
-------------
Port state = Up Mstr In-Bndl

Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.
### Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SAC</td>
<td>U6/S7</td>
<td>HQ</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>19</td>
</tr>
</tbody>
</table>

### Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SW5</td>
<td>aabb.cc00.3700</td>
<td>Et0/0</td>
<td>15s</td>
<td>SC</td>
<td>230001</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:10m:07s

### Port: Et1/1

- Port state: Up Mstr In-Bndl
- Channel group: 35 Mode: Automatic-Sl Gcchange = 0
- Port-channel: Po35 GC = 0x00230001 Pseudo port-channel = Po35
- Flags: S - Device is sending Slow hello. C - Device is in Consistent state. A - Device is in Auto mode. P - Device learns on physical port. d - PAgP is down.
- Timers: H - Hello timer is running. Q - Quit timer is running. S - Switching timer is running. I - Interface timer is running.

### Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SAC</td>
<td>U6/S7</td>
<td>HQ</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>19</td>
</tr>
</tbody>
</table>

### Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/1</td>
<td>SW5</td>
<td>aabb.cc00.3700</td>
<td>Et0/0</td>
<td>0s</td>
<td>SC</td>
<td>230001</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:10m:09s

Port-channels in the group:

-------------------------------

### Port-channel: Po35

Age of the Port-channel: 0d:00h:10m:22s
- Logical slot/port = 16/1 Number of ports = 2
- GC = 0x00230001 HotStandBy port = null
- Port state = Port-channel Ag-Inuse

### Protocol: PAgP

- Port security = Disabled

Ports in the Port-channel:

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/0</td>
<td>Automatic-Sl</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/1</td>
<td>Automatic-Sl</td>
<td>0</td>
</tr>
</tbody>
</table>

Time since last port bundled: 0d:00h:10m:07s Et1/0

SW5#sh errdisable recovery | ex Dis
-----------------------------

### Link-flap

Enabled

### Timer interval: 35 seconds

Interfaces that will be enabled at the next timeout:

**Note:** SW4 “sh etherc detail” output has been omitted as it should look similar to the output produced on SW3
Spanning-Tree Rapid PVST

SW5 should run spanning tree in **802.1w** mode whereas SW3 and SW4 should operate in their default spanning-tree mode.

Configure SW5 should be the root bridge.

There should be no secondary root bridge in the network.

Ensure that SW5 will always remain the root bridge even if a new switch is added to SW5 Layer 2 network or any existing switch will try and take over the root bridge role.

**Configuration:**

SW5

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 priority 24576

interface Port-channel135
  spanning-tree guard root

interface Port-channel145
  spanning-tree guard root

interface Ethernet0/2
  spanning-tree guard root

interface Ethernet1/2
  spanning-tree guard root

interface Ethernet0/3
  spanning-tree guard root

interface Ethernet3/0
  spanning-tree guard root

interface Ethernet2/0
  spanning-tree guard root

interface Ethernet2/1
  spanning-tree guard root

interface Ethernet2/2
  spanning-tree guard root

interface Ethernet2/3
  spanning-tree guard root

interface Ethernet1/3
  spanning-tree guard root
```
Verification:

SW5#sh spanning-tree | in This VLAN
VLAN0001  This bridge is the root
VLAN0012  This bridge is the root
VLAN0013  This bridge is the root
VLAN0014  This bridge is the root
VLAN0015  This bridge is the root
VLAN0016  This bridge is the root
VLAN0017  This bridge is the root
VLAN0023  This bridge is the root
VLAN0024  This bridge is the root
VLAN0035  This bridge is the root
VLAN0046  This bridge is the root
VLAN0057  This bridge is the root
VLAN0067  This bridge is the root
VLAN0092  This bridge is the root
VLAN0093  This bridge is the root
VLAN0094  This bridge is the root
VLAN0095  This bridge is the root
VLAN0096  This bridge is the root
VLAN0097  This bridge is the root
VLAN0221  This bridge is the root
VLAN0222  This bridge is the root
VLAN0223  This bridge is the root
VLAN0321  This bridge is the root
VLAN0322  This bridge is the root
VLAN0323  This bridge is the root
**SW5#sh spanning-tree summary**

Switch is in rapid-pvst mode

Root bridge for: VLAN0001, VLAN0012-VLAN0017, VLAN0023-VLAN0024, VLAN0035-VLAN0046, VLAN0057, VLAN0067, VLAN0092-VLAN0097, VLAN0221-VLAN0223

Extended system ID is enabled

PortFast Default is disabled

PortFast BPDU Guard Default is disabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

Configured Pathcost method used is short

UplinkFast is disabled

BackboneFast is disabled

<Output omitted>

**SW5#sh spanning-tree bridge**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Bridge ID</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Fwd Dly</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>24577</td>
<td>(24576, 1)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0012</td>
<td>24588</td>
<td>(24576, 12)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0013</td>
<td>24589</td>
<td>(24576, 13)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0014</td>
<td>24590</td>
<td>(24576, 14)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0015</td>
<td>24591</td>
<td>(24576, 15)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0016</td>
<td>24592</td>
<td>(24576, 16)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0017</td>
<td>24593</td>
<td>(24576, 17)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0023</td>
<td>24599</td>
<td>(24576, 23)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0024</td>
<td>24600</td>
<td>(24576, 24)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0035</td>
<td>24611</td>
<td>(24576, 35)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0046</td>
<td>24622</td>
<td>(24576, 46)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0057</td>
<td>24633</td>
<td>(24576, 57)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0067</td>
<td>24643</td>
<td>(24576, 67)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0092</td>
<td>24668</td>
<td>(24576, 92)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0093</td>
<td>24669</td>
<td>(24576, 93)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0094</td>
<td>24670</td>
<td>(24576, 94)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0095</td>
<td>24671</td>
<td>(24576, 95)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0096</td>
<td>24672</td>
<td>(24576, 96)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0097</td>
<td>24673</td>
<td>(24576, 97)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0221</td>
<td>24797</td>
<td>(24576, 221)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0222</td>
<td>24798</td>
<td>(24576, 222)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0223</td>
<td>24799</td>
<td>(24576, 223)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0321</td>
<td>24897</td>
<td>(24576, 321)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0322</td>
<td>24898</td>
<td>(24576, 322)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0323</td>
<td>24899</td>
<td>(24576, 323)</td>
<td>aabb.cc00.3700</td>
<td>2</td>
<td>20</td>
</tr>
</tbody>
</table>

**SW3#sh spanning-tree bridge**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Bridge ID</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Fwd Dly</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>32769</td>
<td>(32768, 1)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0012</td>
<td>32780</td>
<td>(32768, 12)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0013</td>
<td>32781</td>
<td>(32768, 13)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0014</td>
<td>32782</td>
<td>(32768, 14)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0015</td>
<td>32783</td>
<td>(32768, 15)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0016</td>
<td>32784</td>
<td>(32768, 16)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0017</td>
<td>32785</td>
<td>(32768, 17)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0023</td>
<td>32791</td>
<td>(32768, 23)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0024</td>
<td>32792</td>
<td>(32768, 24)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0035</td>
<td>32803</td>
<td>(32768, 35)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0046</td>
<td>32814</td>
<td>(32768, 46)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0057</td>
<td>32825</td>
<td>(32768, 57)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0067</td>
<td>32835</td>
<td>(32768, 67)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0092</td>
<td>32860</td>
<td>(32768, 92)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0093</td>
<td>32861</td>
<td>(32768, 93)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0094</td>
<td>32862</td>
<td>(32768, 94)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0095</td>
<td>32863</td>
<td>(32768, 95)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0096</td>
<td>32864</td>
<td>(32768, 96)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0097</td>
<td>32865</td>
<td>(32768, 97)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0221</td>
<td>32989</td>
<td>(32768, 221)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0222</td>
<td>32990</td>
<td>(32768, 222)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0223</td>
<td>32991</td>
<td>(32768, 223)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0321</td>
<td>33091</td>
<td>(32768, 321)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0322</td>
<td>33090</td>
<td>(32768, 322)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>VLAN0323</td>
<td>33091</td>
<td>(32768, 323)</td>
<td>aabb.cc00.3500</td>
<td>2</td>
<td>20</td>
</tr>
</tbody>
</table>
### SW4 # sh spanning-tree bridge

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Bridge ID</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Fwd Dly</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>32769 (32768, 1) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0012</td>
<td>32780 (32768, 12) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0013</td>
<td>32781 (32768, 13) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0014</td>
<td>32782 (32768, 14) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0015</td>
<td>32783 (32768, 15) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0016</td>
<td>32784 (32768, 16) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0017</td>
<td>32785 (32768, 17) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0023</td>
<td>32791 (32768, 23) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0024</td>
<td>32792 (32768, 24) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0035</td>
<td>32803 (32768, 35) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0046</td>
<td>32814 (32768, 46) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0057</td>
<td>32825 (32768, 57) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0067</td>
<td>32835 (32768, 67) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0092</td>
<td>32860 (32768, 92) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0093</td>
<td>32861 (32768, 93) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0094</td>
<td>32862 (32768, 94) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0095</td>
<td>32863 (32768, 95) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0096</td>
<td>32864 (32768, 96) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0097</td>
<td>32865 (32768, 97) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0221</td>
<td>32989 (32768, 221) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0222</td>
<td>32990 (32768, 222) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0223</td>
<td>32991 (32768, 223) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0321</td>
<td>33089 (32768, 321) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0322</td>
<td>33090 (32768, 322) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
<tr>
<td>VLAN0323</td>
<td>33091 (32768, 323) aabb.cc00.3600</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>ieee</td>
</tr>
</tbody>
</table>

### SW3 # sh spanning-tree summary

**Switch is in pvst mode**

**Root bridge for:** none

- Extended system ID is enabled
- Portfast Default is disabled
- PortFast BPDU Guard Default is disabled
- Portfast BPDU Filter Default is disabled
- Loopguard Default is disabled
- EtherChannel misconfig guard is enabled

Configured Pathcost method used is short

- UplinkFast is disabled
- BackboneFast is disabled

<Output omitted>

### SW4 # sh spanning-tree summary

**Switch is in pvst mode**

**Root bridge for:** none

- Extended system ID is enabled
- Portfast Default is disabled
- PortFast BPDU Guard Default is disabled
- Portfast BPDU Filter Default is disabled
- Loopguard Default is disabled
- EtherChannel misconfig guard is enabled

Configured Pathcost method used is short

- UplinkFast is disabled
- BackboneFast is disabled

<Output omitted>
Spanning-Tree Tuning

Ensure that interface Ethernet1/2 is in the forwarding state rather than the blocking state for all range of VLANs on SW4
Do not use cost or port priority to accomplish this task
You must not make any explicit "spanning-tree" interface changes for this task

**Configuration:**

```
SW4
interface Ethernet1/2
bandwidth 100000
```

**Verification: Before Implementation**

```
SW4#show spanning-tree interface ethernet 1/2
Vlan Role Sts Cost Prio.Nbr Type
------------------- ---- ------ ------ ----
  VLAN0001          Altn BLK 100 128.35   Shr
  VLAN0012          Altn BLK 100 128.35   Shr
  VLAN0013          Altn BLK 100 128.35   Shr
  VLAN0014          Altn BLK 100 128.35   Shr
  VLAN0015          Altn BLK 100 128.35   Shr
  VLAN0016          Altn BLK 100 128.35   Shr
  VLAN0017          Altn BLK 100 128.35   Shr
  VLAN0023          Altn BLK 100 128.35   Shr
  VLAN0024          Altn BLK 100 128.35   Shr
  VLAN0035          Altn BLK 100 128.35   Shr
  VLAN0046          Altn BLK 100 128.35   Shr
  VLAN0057          Altn BLK 100 128.35   Shr
  VLAN0067          Altn BLK 100 128.35   Shr
  VLAN0092          Altn BLK 100 128.35   Shr
  VLAN0093          Altn BLK 100 128.35   Shr
  VLAN0094          Altn BLK 100 128.35   Shr
  VLAN0095          Altn BLK 100 128.35   Shr
  VLAN0096          Altn BLK 100 128.35   Shr
  VLAN0097          Altn BLK 100 128.35   Shr
  VLAN0221          Altn BLK 100 128.35   Shr
  VLAN0222          Altn BLK 100 128.35   Shr
  VLAN0223          Altn BLK 100 128.35   Shr
  VLAN0321          Altn BLK 100 128.35   Shr
  VLAN0322          Altn BLK 100 128.35   Shr
  VLAN0323          Altn BLK 100 128.35   Shr
```

**Verification: After Implementation**

```
SW4#show spanning-tree interface ethernet 1/2
Vlan Role Sts Cost Prio.Nbr Type
------------------- ---- ------ ------ ----
  VLAN0001          Root FWD 19 128.35   Shr
  VLAN0012          Root FWD 19 128.35   Shr
  VLAN0013          Root FWD 19 128.35   Shr
  VLAN0014          Root FWD 19 128.35   Shr
  VLAN0015          Root FWD 19 128.35   Shr
  VLAN0016          Root FWD 19 128.35   Shr
  VLAN0017          Root FWD 19 128.35   Shr
  VLAN0023          Root FWD 19 128.35   Shr
  VLAN0024          Root FWD 19 128.35   Shr
  VLAN0035          Root FWD 19 128.35   Shr
  VLAN0046          Root FWD 19 128.35   Shr
  VLAN0057          Root FWD 19 128.35   Shr
  VLAN0067          Root FWD 19 128.35   Shr
  VLAN0092          Root FWD 19 128.35   Shr
  VLAN0093          Root FWD 19 128.35   Shr
  VLAN0094          Root FWD 19 128.35   Shr
  VLAN0095          Root FWD 19 128.35   Shr
  VLAN0096          Root FWD 19 128.35   Shr
  VLAN0097          Root FWD 19 128.35   Shr
  VLAN0221          Root FWD 19 128.35   Shr
  VLAN0222          Root FWD 19 128.35   Shr
  VLAN0223          Root FWD 19 128.35   Shr
  VLAN0321          Root FWD 19 128.35   Shr
  VLAN0322          Root FWD 19 128.35   Shr
  VLAN0323          Root FWD 19 128.35   Shr
```
Spanning-Tree Timers

Configure the switches for all range of possible VLANs as per the following:

- Broadcast Spanning-Tree hello should be sent every 3 seconds
- Ports should transition to the forwarding after 20 seconds
- Switches should attempt reconfiguration if they do not hear a configuration message within 10 seconds

**Configuration:**

**SW3**

```
spanning-tree vlan 1-4094 hello-time 3
spanning-tree vlan 1-4094 forward-time 10
spanning-tree vlan 1-4094 max-age 10
```

**SW4**

```
spanning-tree vlan 1-4094 hello-time 3
spanning-tree vlan 1-4094 forward-time 10
spanning-tree vlan 1-4094 max-age 10
```

**SW5**

```
spanning-tree vlan 1-4094 hello-time 3
spanning-tree vlan 1-4094 forward-time 10
spanning-tree vlan 1-4094 max-age 10
```

**Verification: Before Implementation**

```
SW5#sh spanning-tree vl 57
VLAN0057
    Spanning Tree enabled protocol rstp
    Root ID    Priority    24633
        Address     aabb.cc00.3700
        This bridge is the root
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
    Bridge ID Priority    24633  (priority 24576 sys-id-ext 57)
        Address     aabb.cc00.3700
        Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time   300 sec
```

**Verification: After Implementation**

```
SW5#sh spanning-tree vl 57
VLAN0057
    Spanning Tree enabled protocol rstp
    Root ID    Priority    24633
        Address     aabb.cc00.3700
        This bridge is the root
        Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec
    Bridge ID Priority    24633  (priority 24576 sys-id-ext 57)
        Address     aabb.cc00.3700
        Hello Time   3 sec  Max Age 10 sec  Forward Delay 10 sec
        Aging Time   300 sec
```
Spanning-Tree Uplinkfast

Ensure that when the Root port is lost, SW3 and SW4 immediately reconverge to an alternate connection.

**Configuration:**

```
SW3
spanning-tree uplinkfast

SW4
spanning-tree uplinkfast
```

**Verification:**

```
SW4#sh spanning-tree vl 94 | in Root|Alt
  Root ID  Priority    24670
  Et0/0    Altn BLK 3100      128.1    Shr
  Et0/1    Altn BLK 3100      128.2    Shr
  Et0/2    Altn BLK 3100      128.3    Shr
  Et1/2    Altn BLK 3100      128.35   Shr
  Po45     Root FWD 3056      128.514  Shr

SW4#conf t
SW4(config)#no service timestamps debug
SW4#debug spanning-tree uplinkfast
Spanning Tree uplinkfast debugging is on
SW4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)#int po 45
SW4(config-if)#sh
SW4(config-if)#do u
All possible debugging has been turned off
SW4(config-if)#ex

SW4#sh spanning-tree vl 94 | in Root|Alt
  Root ID  Priority    24670
  Et0/0    Altn BLK 3100      128.1    Shr
  Et0/1    Altn BLK 3100      128.2    Shr
  Et0/2    Altn BLK 3100      128.3    Shr
  Et1/2    Root FWD 3100      128.35   Shr
```
Router on a stick

All routers have been preconfigured with IP addresses on their Ethernet interfaces. Some switchports on SW3, SW4, and SW5 have also already been preconfigured. Complete the configuration on the routers and their associated switch port accordingly without using secondary addressing to establish ICMP communication with each other. Shutdown all unused interfaces on the switches.

Configuration:

**SW3**

```plaintext
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk

interface Ethernet2/0
  switchport access vlan 16
  switchport mode access

interface Ethernet2/1
  switchport trunk encapsulation dot1q
  switchport mode trunk

interface Ethernet3/0
  switchport access vlan 23
  switchport mode access
```

**SW4**

```plaintext
interface Ethernet2/3
  switchport access vlan 13
  switchport mode access

interface Ethernet3/0
  switchport access vlan 12
  switchport mode access
```

**SW5**

```plaintext
interface Ethernet0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk

interface Ethernet2/2
  switchport access vlan 35
  switchport mode access
```

Verification:
<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po45</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po35</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po45</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po35</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po45</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po45</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et1/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et2/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/0</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/1</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/2</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et3/3</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Po45</td>
<td></td>
<td>connected</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OR? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>172.31.10.25</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet1/0.14</td>
<td>172.31.10.30</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet1/0.15</td>
<td>172.31.10.41</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet1/0.17</td>
<td>172.31.10.33</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet2/0</td>
<td>172.31.10.14</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet3/0</td>
<td>172.31.10.10</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
<tr>
<td>Loopback0</td>
<td>172.100.1.1</td>
<td>YES</td>
<td>TFTP</td>
<td>up</td>
</tr>
</tbody>
</table>
R1#ping 172.31.10.26
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.26, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

R1#ping 172.31.10.29
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.29, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

R1#ping 172.31.10.42
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.42, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms

R1#ping 172.31.10.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

R1#ping 172.31.10.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

R1#ping 172.31.10.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.9, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms

R2#ping 140.60.88.54
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 140.60.88.54, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

R2#ping 140.60.88.46
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 140.60.88.46, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R2#ping 140.60.88.50
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 140.60.88.50, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

R2#ping 172.31.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms

R2#ping 172.31.10.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.10.18, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

Note: All remaining routers within the SP#9 topology should be able to reach other's IP Addresses on their P2P connections
Sydney Business Model HQ

VLAN TRUNK VTP

The VTP domain should be configured to "CISCO" (without quotes)
Do not configure any VTP authentication features
VTPv3 should be configured on both switches
SW6 should be the primary VTP server in the existing Layer 2 domain
Only on SW6 ensure that Virtual Trunking Protocol is disabled on the following interfaces:
  · Ethernet 0/2, 0/3
  · Ethernet 1/0, 1/1
Only active VLANs must be allowed to traverse the trunk between the switches
Ensure that only **dot1q** encapsulation

**Configuration:**

**SW6**

vtp domain CISCO
vtp version 3
vtp mode server

interface range ethernet 0/0 - 1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,10,20,50,78,567,668
  switchport mode trunk

interface range ethernet 0/2 - 3, ethernet 1/0 - 1
no vtp

**Note:** This is an 'exec' mode command

SW6#vtp primary force

**SW7**

vtp domain CISCO
vtp version 3
vtp mode client

interface range Ethernet 0/0 - 1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,10,20,50,78,567,668
  switchport mode trunk

SW6#vtp primary force
This system is becoming primary server for feature vlan
*Dec 19 20:52:03.220: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.3800 has become the primary server for the VLAN VTP feature

SW7#vtp
*Dec 19 20:52:03.833: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.3800 has become the primary server for the VLAN VTP feature
Verification:

SW6#sh vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
---------- ----------- --------------- --------------- --------------- ---------------
VLAN No 1 aabb.cc00.3800 aabb.cc00.3900 SW7

SW7#sh vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
---------- ----------- --------------- --------------- --------------- ---------------
VLAN No 1 aabb.cc00.3800=aabb.cc00.3800 SW6

SW6#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3800

Feature VLAN:
---
VTP Operating Mode : Primary Server
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 1
Primary ID : aabb.cc00.3800
Primary Description : SW6
MD5 digest : 0x18 0x70 0x40 0x4B 0x28 0x43 0x79 0x06
0xAF 0xEF 0xAA 0xAD 0x4C 0xD5 0x99 0x78

Feature MST:
---
VTP Operating Mode : Transparent

Feature UNKNOWN:
---
VTP Operating Mode : Transparent

SW7#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : CISCO
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3900

Feature VLAN:
---
VTP Operating Mode : Client
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 1
Primary ID : aabb.cc00.3800
Primary Description : SW6
MD5 digest : 0x18 0x70 0x40 0x4B 0x28 0x43 0x79 0x06
0xAF 0xEF 0xAA 0xAD 0x4C 0xD5 0x99 0x78

Feature MST:
---
VTP Operating Mode : Transparent

Feature UNKNOWN:
---
VTP Operating Mode : Transparent
### SW6#sh vtp interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>VTP Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>disabled</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>disabled</td>
</tr>
<tr>
<td>Ethernet1/0</td>
<td>disabled</td>
</tr>
<tr>
<td>Ethernet1/1</td>
<td>disabled</td>
</tr>
<tr>
<td>Ethernet1/2</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/3</td>
<td>enabled</td>
</tr>
</tbody>
</table>

### SW7#sh vtp interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>VTP Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/0</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/1</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/2</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/3</td>
<td>enabled</td>
</tr>
</tbody>
</table>
Spanning-TREE Rapid PVST

Both switches must be enabled for IEEE 802.1w
Configure instance per VLAN and rapid transition for forwarding.
Ensure that SW6 is the Root Switch for all range of possible VLANs and it has the best chance to become the root, SW7 should be the backup switch for all range of possible VLANs
Use half of the default values for max age
You have high-priority traffic running on VLAN50 where the Multicast Server is located. Configure SW7 as needed such that the ports connected to Multicast Server these devices will wait five seconds before changing from learning state to forwarding state. Do not use configure anything globally
Do not forget to assign Ethernet1/3 to VLAN 50

Configuration:

SW6
spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 max-age 10
spanning-tree vlan 1-4094 priority 0

SW7
spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 max-age 10
spanning-tree vlan 1-4094 priority 4096
interface Ethernet1/1
spanning-tree portfast
interface Ethernet1/3
switchport access vlan 50
switchport mode access
spanning-tree portfast

Verification:

SW6#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020, VLAN0050, VLAN0078, VLAN0567
VLAN0668
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast is disabled
BackboneFast is disabled
<Output omitted>
SW7#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: none
Extended system ID is enabled
Portfast Default is disabled
Portfast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast is disabled
BackboneFast is disabled

Note: Interface Ethernet1/3 connects to a Fictitious Printer and Ethernet1/0 connects to R17
After changes have been made SW7 shows Ethernet1/3 in the portfast state

SW7#sh spanning-tree interface et 1/3 detail
Port 36 (Ethernet1/3) of VLAN0050 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.36.
Designated root has priority 50, address aabb.cc00.3800
Designated bridge has priority 4146, address aabb.cc00.3900
Designated port id is 128.36, designated path cost 100
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
The port is in the portfast mode
Link type is shared by default
BPDU: sent 11, received 0

Note: Other ports should remain in their default state, example Ethernet1/0

SW7#sh spanning-tree interface et 1/0 detail
Port 33 (Ethernet1/0) of VLAN0078 is designated forwarding
Port path cost 100, Port priority 128, Port Identifier 128.33.
Designated root has priority 78, address aabb.cc00.3800
Designated bridge has priority 4174, address aabb.cc00.3900
Designated port id is 128.33, designated path cost 100
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is shared by default
BPDU: sent 139, received 0
Spanning-Tree Tuning

Ensure that interface Ethernet0/1 is in the forwarding state instead of the blocking state for VLAN 78 on SW7
Do not make any changes on SW7 to accomplish this task

Configuration:

**SW6**

interface Ethernet0/1
spanning-tree vlan 78 port-priority 64

Verification: Before Implementation

```
SW7#sh cdp ne et0/1 | be Device
Device ID        Local Intrfce     Holdtme    Capability  Platform Port ID
SW6              Eth 0/1           155        R S   Linux Uni Eth 0/1
```

```
SW7#sh spanning-tree interface et 0/1
Vlan             Role Sts Cost      Prio.Nbr Type
------------------- ---- ------- -------- -------------------------------
VLAN0001          Altn BLK 100 128.2   Shr
VLAN0010          Altn BLK 100 128.2   Shr
VLAN0020          Altn BLK 100 128.2   Shr
VLAN0050          Altn BLK 100 128.2   Shr
VLAN0078          Altn BLK 100 128.2   Shr
VLAN0567          Altn BLK 100 128.2   Shr
VLAN0668          Altn BLK 100 128.2   Shr
```

```
SW7#sh spanning-tree v1 10
VLAN0010
Spanning tree protocol rstp
Root ID  Priority    10
Address   aabb.cc00.3800
Cost  100
Port  1 (Ethernet0/0)
Hello Time  2 sec Max Age 10 sec Forward Delay 15 sec
Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
Address   aabb.cc00.3900
Hello Time  2 sec Max Age 10 sec Forward Delay 15 sec
Aging Time  300 sec
Interface     Role Sts Cost      Prio.Nbr Type
--------------- --------- -------- -------------------------------
Et0/0               Root FWD 100 128.1   Shr
Et0/1               Altn BLK 100 128.2   Shr
```

```
SW7#sh spanning-tree v1 78
VLAN0078
Spanning tree protocol rstp
Root ID  Priority    78
Address   aabb.cc00.3800
Cost  100
Port  1 (Ethernet0/0)
Hello Time  2 sec Max Age 10 sec Forward Delay 15 sec
Bridge ID  Priority    4174 (priority 4096 sys-id-ext 78)
Address   aabb.cc00.3900
Hello Time  2 sec Max Age 10 sec Forward Delay 15 sec
Aging Time  300 sec
Interface     Role Sts Cost      Prio.Nbr Type
--------------- --------- -------- -------------------------------
Et0/0               Root FWD 100 128.1   Shr
Et0/1               Altn BLK 100 128.2   Shr
Et1/0               Desg FWD 100 128.33   Shr
```
### Verification: After Implementation

```plaintext
SW6#sh spanning-tree interface et 0/1  
<table>
<thead>
<tr>
<th>Vlan</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0010</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0020</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0050</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0078</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>64.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0567</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
<tr>
<td>VLAN0668</td>
<td>Desg</td>
<td>FWD</td>
<td>100</td>
<td>128.2</td>
<td>Shr</td>
</tr>
</tbody>
</table>

SW7#sh spanning-tree vl 10  
```

**VLAN0010**  
Spanning tree enabled protocol rstp  
Root ID | Priority | Address | Cost | Port | Hello Time | Max Age | Forward Delay | Aging Time |
--------|----------|---------|------|------|------------|---------|---------------|-----------|
|         | 10       | aabb.cc00.3800 | 100  | 1 (Ethernet0/0) | 2 sec | Max Age 10 sec | Forward Delay 15 sec | |
|         |          |          |      |      |            |         |               |           | 300 sec |

Bridge ID | Priority | Address | Hello Time | Max Age | Forward Delay | Aging Time |
-----------|----------|---------|------------|---------|---------------|------------|
|           | 4106     | aabb.cc00.3900 | 2 sec     | Max Age 10 sec | Forward Delay 15 sec | 300 sec |

Interface | Role | Sts | Cost | Prio.Nbr | Type |
-----------|------|-----|------|---------|------|
| Et0/0     | Root | FWD | 100  | 128.1   | Shr   |
| Et0/1     | Altn | BLK | 100  | 128.2   | Shr   |

SW7#sh spanning-tree vl 78  
```

**VLAN0078**  
Spanning tree enabled protocol rstp  
Root ID | Priority | Address | Cost | Port | Hello Time | Max Age | Forward Delay | Aging Time |
--------|----------|---------|------|------|------------|---------|---------------|-----------|
|         | 78       | aabb.cc00.3800 | 100  | 2 (Ethernet0/1) | 2 sec | Max Age 10 sec | Forward Delay 15 sec | |
|         |          |          |      |      |            |         |               |           | 300 sec |

Bridge ID | Priority | Address | Hello Time | Max Age | Forward Delay | Aging Time |
-----------|----------|---------|------------|---------|---------------|------------|
|           | 4174     | aabb.cc00.3900 | 2 sec     | Max Age 10 sec | Forward Delay 15 sec | 300 sec |

Interface | Role | Sts | Cost | Prio.Nbr | Type |
-----------|------|-----|------|---------|------|
| Et0/0     | Altn | BLK | 100  | 128.1   | Shr   |
| Et0/1     | Root | FWD | 100  | 128.2   | Shr   |
| Et1/0     | Desg | LRN | 100  | 128.33  | Shr   |
```
L2 Security

Configure L2 security on SW7 interface Ethernet1/1 according to the below output mac-address should appear as aabb.ccdd.aabb
Ensure that link status events are logged

Note: SW7 Interface Ethernet1/1 should already be pre-configured (initial configs) and port security would have already been triggered on the switchport caused by another mac address

SW7#
* Dec 6 12:32:54.660: %PM-4-ERR_DISABLE: psecure-violation error detected on Et1/1, putting Et1/1 in err-disable state
* Dec 6 12:32:54.660: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address aabb.cc00.5400 on port Ethernet1/1

SW7#sh port-security interface et 1/1
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : aabb.cc00.5400:50
Security Violation Count : 1

SW7#sh int status
Port Name Status Vlan Duplex Speed Type
Et0/0 connected trunk auto auto unknown
Et0/1 connected trunk auto auto unknown
Et0/2 connected 668 auto auto unknown
Et0/3 connected 668 auto auto unknown
Et1/0 connected 78 auto auto unknown
Et1/1 err-disabled 50 auto auto unknown
Et1/2 connected 1 auto auto unknown
Et1/3 Fictitious Printer connected 50 auto auto unknown

Configuration:

SW7
interface Ethernet1/1
logging event link-status

SERVER4
interface Ethernet0/0
mac-address aabb.ccdd.aabb
**Verification:**

```bash
SW7#conf t
SW7(config)#int et 1/1
SW7(config-if)#sh
SW7(config-if)#no sh

SW7#sh port-security interface et 1/1
<table>
<thead>
<tr>
<th>Port Security</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td>Secure-up</td>
</tr>
<tr>
<td>Violation Mode</td>
<td>Shutdown</td>
</tr>
<tr>
<td>Aging Time</td>
<td>0 mins</td>
</tr>
<tr>
<td>Aging Type</td>
<td>Absolute</td>
</tr>
<tr>
<td>SecureStatic Address Aging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Maximum MAC Addresses</td>
<td>1</td>
</tr>
<tr>
<td>Total MAC Addresses</td>
<td>1</td>
</tr>
<tr>
<td>Configured MAC Addresses</td>
<td>1</td>
</tr>
<tr>
<td>Sticky MAC Addresses</td>
<td>0</td>
</tr>
<tr>
<td>Last Source Address:Vlan</td>
<td>aabb. ccdd.aabb-50</td>
</tr>
<tr>
<td>Security Violation Count</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Note:
Cisco DHCP server and the relay agent are enabled by default.

"no service dhcp" command disables Cisco DHCP server and the relay agent
“service dhcp” command reenables the functionality

Port 67 (the DHCP server port) is closed in the Cisco DHCP/BOOTP default configuration. There are two logical parts to the service dhcp command: service enabled and service running. The DHCP service is enabled by default, but port 67 does not open until the DHCP service is running. If the DHCP service is running, the show ip sockets details or the show sockets detail command displays port 67 as open.

The Cisco DHCP relay agent is enabled on an interface only when you configure the ip helper-address command. This command enables a DHCP broadcast to be forwarded to the configured DHCP server.

Some DHCP clients send a client identifier (DHCP option 61) in the DHCP packet. To configure manual bindings for such clients, you must enter the client-identifier command with the hexadecimal values that identify the DHCP client. To configure manual bindings for clients that do not send a client identifier option, you must enter the hardware-address DHCP pool configuration command with the hexadecimal hardware address of the client.

You can specify the unique identifier for the client in either of the following ways:
- 7-byte dotted hexadecimal notation. For example, 01b7.0813.8811.66, where 01 represents the Ethernet media type and the remaining bytes represent the MAC address of the DHCP client.
- 27-byte dotted hexadecimal notation. For example, 7665.6e64.6f72.2d30.3032.342e.3937.6230.2e33.3734.312d.4661.302f.31. The equivalent ASCII string for this hexadecimal value is vendor-0024.9741-fa0/1, where vendor represents the vendor, 0024.9741 represents the MAC address of the source interface, and fa0/1 represents the source interface of the DHCP client.

You cannot configure manual bindings within the same pool that is configured with the network command in DHCP pool configuration mode.

*directly from Cisco website*
DHCP manual bindings (7-BYTE)

Configure DHCP service on R12
PC#1 must always receive 192.168.20.100 IP address based on the Client-ID of its Ethernet interface
PC#1 should send a hostname of PC1
DHCP assigned IP address should never expire
DHCP should be configured using the following parameters:

- DNS server 192.168.20.200 192.168.20.201
- Default gateway 192.168.20.12
- Infinite lease
- Pool must be named PC1
- Domain Re-solution.london

Configuration:

PC#1

```
interface Ethernet0/0
   ip address dhcp client-id Ethernet0/0 hostname PC1
```

R12

```
service dhcp

ip dhcp pool PC1
   host 192.168.20.100 255.255.255.0
   client-identifier 01aa.bb0047.00
   client-name PC1
   default-router 192.168.20.12
   dns-server 192.168.20.200 192.168.20.201
   domain-name Re-solution.london
   lease infinite
```
Verification:

PC1(config)#int eth 0/0
PC1(config-if)#shut
PC1(config-if)#no shut

*Dec 6 12:41:18.944: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Dec 6 12:41:19.949: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
*Dec 6 12:41:22.258: %LINK-5-UPDOWN: Interface Ethernet0/0, changed state to up

PC1(config-if)#
*Dec 6 12:41:24.425: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.20.100, mask 255.255.255.0, hostname PC1

PC1#show ip route | beg Gate
Gateway of last resort is 192.168.20.12 to network 0.0.0.0
S*  0.0.0.0/0 [254/0] via 192.168.20.12
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C  192.168.20.0/24 is directly connected, Ethernet0/0
L  192.168.20.100/32 is directly connected, Ethernet0/0

R12#conf t
R12(config)#no service timestamps debug
R12#debug ip dhcp server packet detail
DHCP server packet detail debugging is on.
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPOFFER received from client 01aa.bbcc.0047.00 on interface Ethernet1/0.
DHCPD: Sending DHCPOFFER to client 01aa.bbcc.0047.00 (192.168.20.100). DHCPD: Setting only requested parameters
DHCPD: No option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.4700.
DHCPD: No option 125
DHCPD: DHCPOFFER received from client 01aa.bbcc.0047.00.
DHCPD: Appending default domain from pool
DHCPD: Using hostname 'PC1.Solution.Data.' for dynamic update (from hostname option)
DHCPD: Sending DHCPACK to client 01aa.bbcc.0047.00 (192.168.20.100). DHCPD: Setting only requested parameters
R12#un all
All possible debugging has been turned off

PC1#show ip int brie
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 192.168.20.100 YES DHCP up
Ethernet0/1 unassigned YES unset administratively down
Ethernet0/2 unassigned YES unset administratively down
Ethernet0/3 unassigned YES unset administratively down

PC1#show ip int eth 0/0
Ethernet0/0 is up, line protocol is up
Internet address is 192.168.20.100/24
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes

<Output omitted>
R12#show ip dhcp binding

Bindings from all pools not associated with VRF:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Client-ID/</th>
<th>Lease expiration</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware address/</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.20.100</td>
<td>01aa.bbcc.0047.00</td>
<td>Infinite</td>
<td>Manual</td>
</tr>
</tbody>
</table>

R12#sh ip dhcp pool

Pool PC1:

Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0

Total addresses : 1

Leased addresses : 1

Pending event : none

0 subnet is currently in the pool:

<table>
<thead>
<tr>
<th>Current index</th>
<th>IP address range</th>
<th>Leased addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.100</td>
<td>192.168.20.100 - 192.168.20.100</td>
<td>1</td>
</tr>
</tbody>
</table>

R12#show ip dhcp server statistics

Memory usage : 24431

Address pools : 1
Database agents : 0
Automatic bindings : 0

Manual bindings : 1
Expired bindings : 0
Malformed messages : 0
Secure arp entries : 0

Message Received
BOOTREQUEST : 0
DHCDDISCOVER : 3
DHCPREQUEST : 3
DHCPDECLINE : 0
DHCPRELEASE : 6
DHCPIINFORM : 0

Message Sent
BOOTREPLY : 0
DHCPOFFER : 3
DHCPACK : 3
DHCPNAK : 0
**DHCP (27-BYTE)**

Configure DHCP service on R13
Server#1 must always receive 192.168.30.100 IP address
IP address should expire after 45 days 12 hours and 10 minutes
Do not statically assign host IP Address under DHCP pool
Do not configure DHCP IP Address exclusion anywhere
Use the following parameters for your configuration:

- DNS server 192.168.30.250
- Default gateway 192.168.30.13
- Pool must be named SERVER1

**Configuration:**

```
R13
  service dhcp

  ip dhcp pool SERVER1
  host 192.168.30.100 255.255.255.0
  client-identifier 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3130.302d.4574.302f.30
default-router 192.168.30.13
dns-server 192.168.30.250
```

```
SERVER#1
  interface Ethernet0/0
  ip address dhcp
```
**Verification:**

**Note:** We will shutdown and then unshut Ethernet0/0 on the Web Server in order to speed up DHCP request

```bash
WEBSERVER#1(config)#interface Ethernet0/0
WEBSERVER#1(config-if)# ip address dhcp
WEBSERVER#1(config-if)#sh
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
WEBSERVER#1(config-if)#no sh
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up

R13#deb ip dh server pac detail
DHCP server packet detail debugging is on.
DHCPD: DHCPDISCOVER received from client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3130.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Sending DHCPOFFER to client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3130.302d.4574.302f.30 (192.168.30.100).DHCPD: Setting only requested parameters
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5100.
DHCPD: client's VIP is .
DHCPD: No option 125
DHCPD: DHCREQUEST received from client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3130.302d.4574.302f.30.
DHCPD: No default domain to append - abort update
DHCPD: Sending DHCPACK to client aabb.cc00.5100. DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5100.

WEBSERVER#1(config-if)#
*Dec 19 22:20:32.670: %DHCP-6-ADDRESS.Assign: Interface Ethernet0/0 assigned DHCP address 192.168.30.100, mask 255.255.255.0, hostname WEBSERVER#1

WEBSERVER#1#show ip int brie
Interface IP-Adresse OK? Method Status Protocol
Ethernet0/0 192.168.30.100 YES DHCP up up
Ethernet0/1 unassigned YES unset administratively down down
Ethernet0/2 unassigned YES unset administratively down down
Ethernet0/3 unassigned YES unset administratively down down

WEBSERVER#1#show ip route | beg Gate
Gateway of last resort is 192.168.30.13 to network 0.0.0.0
S* 0.0.0.0/0 [254/0] via 192.168.30.13
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, Ethernet0/0
L 192.168.30.100/32 is directly connected, Ethernet0/0

R13#sh ip dhcp pool
Pool SERVER1 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 1
Leased addresses : 1
Pending event : none
0 subnet is currently in the pool :
Current index IP address range 
192.168.30.100 192.168.30.100 - 192.168.30.100
1
```
R1#sh ip dhcp binding

Bindings from all pools not associated with VRF:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Client-ID/ Hardware address/ User name</th>
<th>Lease expiration</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.30.100</td>
<td>0063.6973.636f.2d61.612e.6363.3030.2e35.3130.302d.4574.302f.30</td>
<td>Infinite</td>
<td>Manual</td>
</tr>
</tbody>
</table>
DHCP Exclusion

Configure DHCP service on R21 using the following parameters:

- DNS server 192.168.50.250
- Default gateway 192.168.50.21
- Pool must be named PC4
- Domain name SolutionData.co.uk

PC#4 must always receive 192.168.50.5 IP address based on the Client ID of its Ethernet0/0 interface. There is a fictitious TFTP server 192.168.51.111 IP Address (Loopback10 R21) where PC#4 configuration file named PC4.txt is stored. PC#4 should download its configuration from the TFTP Server once it obtains its IP Address from the DHCP Server.

Ensure that timestamps for debug messages are disabled on PC#4 and R21.

IP address should expire after 12 hours and 5 minutes (You’ve got 12 hours and 5 minutes to finish the entire Lab before the lease expires).

Configuration:

R21

```
no service timestamps debug

service dhcp

ip dhcp pool PC4
    host 192.168.50.5 255.255.255.0
    client-identifier 01aa.bbcc.004a.00
    bootfile PC4.txt
    default-router 192.168.50.21
    dns-server 192.168.50.250
    domain-name SolutionData.co.uk
    option 150 ip 192.168.51.111
    lease 0 12 5
```

PC#4

```
no service timestamps debug

interface Ethernet0/0
    ip address dhcp client-id Ethernet0/0
```
Verification:

PC4(config)#int eth 0/0
PC4(config-if)#shut
%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
PC4(config-if)#no shut
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
PC4(config-if)#

%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.50.5, mask 255.255.255.0, hostname PC4

R21#debug ip dhcp server packet detail
DHCP server packet detail debugging is on.
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPDISCOVER received from client 01aa.bbcc.004a.00 on interface Ethernet1/0.
DHCPD: Sending DHCPOFFER to client 01aa.bbcc.004a.00 (192.168.50.5). DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.4a00.
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPREQUEST received from client 01aa.bbcc.004a.00.
DHCPD: Appending default domain from pool
DHCPD: Using hostname 'PC4.data.co.uk.' for dynamic update (from hostname option)
DHCPD: Sending DHCPACK to client 01aa.bbcc.004a.00 (192.168.50.5). DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.4a00.

R21#show ip dhcp pool
Pool PC4 :
Utilization mark [high/low] : 100 / 0
Subnet size [first/next] : 0 / 0
Total addresses : 1
Leased addresses : 1
Pending event : none
0 subnet is currently in the pool : Current index IP address range Leased addresses
192.168.50.5 192.168.50.5 - 192.168.50.5 1

PC4#sh ip route | be Gate
Gateway of last resort is 192.168.50.21 to network 0.0.0.0
S* 0.0.0.0/0 [254/0] via 192.168.50.21
192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.50.0/24 is directly connected, Ethernet0/0
L 192.168.50.5/32 is directly connected, Ethernet0/0
DHCP multiple subnet functionality

Configure DHCP service on R14
DHCP pool should be named VLAN20
SW#8 has to remain purely Layer2 device
All devices should be allocated to VLAN 20
The DHCP pool for both primary and a secondary subnet for IP Address assignment:

- Subnet 192.168.60.12/30 (primary) and 192.168.60.16/29 (secondary)
- Pool must be named PC4
- Domain name SolutionData.co.uk

PC#2 should obtain 192.168.60.14/30 from the primary subnet
Server#5 should obtain 192.168.60.18/29 from the secondary subnet
Ensure that a system message is generated and logged for a DHCP primary pool when the pool utilization exceeds 80 and falls below 70
Ensure that timestamps for debug messages are disabled on all devices

**Configuration:**

```
R14
no service timestamps debug
service dhcp
ip dhcp pool VLAN20
  utilization mark high 80 log
  utilization mark low 70 log
  network 192.168.60.12 255.255.255.252
  network 192.168.60.16 255.255.255.248 secondary
  override default-router 192.168.60.17
  domain-name SolutionData.co.uk
  default-router 192.168.60.13
```
PC#2
no service timestamps debug

interface Ethernet0/0
ip address dhcp

SERVER#5
no service timestamps debug

interface Ethernet0/0
ip address dhcp

Verification:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Et0/3, Et1/0, Et1/1, Et1/2, Et1/3</td>
</tr>
<tr>
<td>10</td>
<td>LAN</td>
<td>active</td>
<td>Et0/0</td>
</tr>
<tr>
<td>20</td>
<td>DUMMY-LAN</td>
<td>active</td>
<td>Et0/1, Et0/2</td>
</tr>
</tbody>
</table>

SW8#sh cdp ne
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Local Intrfce</th>
<th>Holdtme</th>
<th>Capability</th>
<th>Platform</th>
<th>Port ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC2</td>
<td>Eth 0/2</td>
<td>121</td>
<td>R B</td>
<td>Linux Uni</td>
<td>Eth 0/0</td>
</tr>
<tr>
<td>SERVER5</td>
<td>Eth 0/1</td>
<td>172</td>
<td>R B</td>
<td>Linux Uni</td>
<td>Eth 0/0</td>
</tr>
</tbody>
</table>

SW8(config-if)#int et 0/0
SW8(config-if)#no switchport access vlan 10
SW8(config-if)#switchport access vlan 20
SW8(config-if)#do wr
Building configuration...
Compressed configuration from 1058 bytes to 660 bytes[OK]
SW8(config-if)#

PC2(config)#int eth 0/0
PC2(config-if)#shut
PC2(config-if)#
%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
PC2(config-if)#no shut
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.60.14, mask 255.255.255.252, hostname PC2
SERVER5(config)#int et 0/0
SERVER5(config-if)#shu

%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down

SERVER5(config-if)#no sh

%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up

*Dec 19 22:54:07.492: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.60.18, mask 255.255.255.248, hostname SERVER5

R14#deb ip dh ser pac de
DHCP server packet detail debugging is on.

DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPCDISCOVER received from client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Allocate an address without class information (192.168.60.12)
DHCPD: Saving workspace (ID=0x16000000)
DHCPD: New packet workspace 0x2B92058 (ID=0x60000000)
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPCDISCOVER received from client 0063.6973.636f.2d61.6162.622a.6363.3030.2e35.3530.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Allocate an address without class information (192.168.60.12)
DHCPD: Saving workspace (ID=0x60000000)
DHCPD: Reprocessing saved workspace (ID=0x60000000)
DHCPD: DHCPCDISCOVER received from client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Sending DHCPOFFER to client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30 (192.168.60.14).DHCPD: Setting only requested parameters
DHCPD: No option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.4800.
DHCPD: New packet workspace 0x2B961B0 (ID=0x37000004)
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPRREQUEST received from client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30.
DHCPD: No default domain to append - abort update
DHCPD: DHCPRPACK to client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Sending DHCPACK to client 0063.6973.636f.2d61.6162.622a.6363.3030.2e34.3830.302d.4574.302f.30 (192.168.60.14).DHCPD: Setting only requested parameters
DHCPD: No option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5500.
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPRREQUEST received from client 0063.6973.636f.2d61.6162.622a.6363.3030.2e35.3530.302d.4574.302f.30.
DHCPD: No default domain to append - abort update
DHCPD: DHCPRPACK to client 0063.6973.636f.2d61.6162.622a.6363.3030.2e35.3530.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Sending DHCPACK to client 0063.6973.636f.2d61.6162.622a.6363.3030.2e35.3530.302d.4574.302f.30 (192.168.60.18).DHCPD: Setting only requested parameters
DHCPD: No option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5500.

R14#un all
All possible debugging has been turned off

SERVER5(config)#int et 0/0
SERVER5(config-if)#shu

%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down

R14#sh ip dhcp pool
POOL VLAN20:
Utilization mark (high/low)    : 80 / 70
Subnet size (first/next)      : 0 / 0
Total addresses               : 8
Leased addresses              : 2
Pending event                 : none
2 subnets are currently in the pool:
Current index | IP address range | Leased addresses
0.0.0.0        | 192.168.60.13   | 192.168.60.14     | 1
192.168.60.11  | 192.168.60.17   | 192.168.60.22     | 1
R14#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/ Hardware address/ User name
                  Lease expiration        Type
192.168.60.14       0063.6973.636f.2d61. Dec 20 2014 11:54 PM  Automatic
                    6162.622e.6363.3030. 2e34.3830.302d.4574. 302f.30
192.168.60.18       0063.6973.636f.2d61. Dec 20 2014 11:54 PM  Automatic
                    6162.622e.6363.3030. 2e35.3530.302d.4574. 302f.30

PC2#sh ip route | ex C|L
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
ia - IS-IS inter area, * - candidate default, U - per-user static route
a - application route
+ - replicated route, % - next hop override
Gateway of last resort is 192.168.60.14 to network 0.0.0.0
S*    0.0.0.0/0 [254/0] via 192.168.60.14
   192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
SERVER5#sh ip route | be 0.0.0
Gateway of last resort is 192.168.60.17 to network 0.0.0.0
S*    0.0.0.0/0 [254/0] via 192.168.60.17
   192.168.60.0/24 is variably subnetted, 3 subnets, 2 masks
   192.168.60.13/32 [254/0] via 192.168.60.17, Ethernet0/0
C    192.168.60.16/29 is directly connected, Ethernet0/0
L    192.168.60.18/32 is directly connected, Ethernet0/0

Note: Check reachability across VLAN20 domain

PC2#ping 192.168.60.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.60.13, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

SERVER5#ping 192.168.60.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.60.17, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms

PC2#ping 192.168.60.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.60.18, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
Note:

DHCP server selects an address pool that contains multiple subnets, the DHCP server allocates an IP address from the subnets as follows:

- When the DHCP server receives an address assignment request, it looks for an available IP address in the primary subnet.
- When the primary subnet is exhausted, the DHCP server automatically looks for an available IP address in any of the secondary subnets maintained by the DHCP server. The server inspects the subnets for address availability in the order of subnets that were added to the pool.
- If the giaddr matches a secondary subnet in the pool, the DHCP server allocates an IP address from that particular secondary subnet (even if IP addresses are available in the primary subnet and irrespective of the order of secondary subnets that were added).

*directly from Cisco website*
Berlin HQ Data Centre

**DHCP Exclusion**

Configure DHCP service on R15
Server#2 must always receive **172.31.100.100** IP address
Do not use DHCP ‘Client ID’ for your solution
DHCP Server must send 5 packets to a pool address before assigning the address to a requesting client. The packet should time out after 700 milliseconds
Ensure that DHCP IP Address conflicts are being logged
Ensure DHCP IP Addresses expire after 11 hours and 37 minutes
Ensure that timestamps for debug messages are disabled on all devices

**Configuration:**

**R15**

```
no service timestamps debug

service dhcp

ip dhcp excluded-address 172.31.100.1 172.31.100.99
ip dhcp excluded-address 172.31.100.101 172.31.100.254

ip dhcp ping packets 5
ip dhcp ping timeout 700
ip dhcp conflict logging

ip dhcp pool SERVER2
network 172.31.100.0 255.255.255.0
default-router 172.31.100.15
```
Verification:

SERVER2(config)#int et 0/0
SERVER2(config-if)#ip add dh
SERVER2(config-if)#shu
SERVER2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
SERVER2(config-if)#no sh

%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Interface Ethernet0/0, changed state to up

%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 172.31.100.100, mask 255.255.255.0, hostname SERVER2

R15#deb ip dh server packet detail debugging is on.
DHCPD: client's VPN is ..
DHCPD: No option 125
DHCPD: DHCPDISCOVER received from client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3230.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Allocate an address without class information (172.31.100.0)
DHCPD: Saving workspace (ID=0x25000000)
DHCPD: New packet workspace 0x27454F0 (ID=0x7C000002)
DHCPD: client's VPN is ..
DHCPD: No option 125

DHCPD: DHCPDISCOVER received from client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3230.302d.4574.302f.30 on interface Ethernet1/0.
DHCPD: Allocating an address (172.31.100.0)
DHCPD: Allocating a workspace (ID=0x25000000)
DHCPD: New packet workspace 0x27454F0 (ID=0x7C000002)
DHCPD: Sending DHCPOFFER to client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3230.302d.4574.302f.30
DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5200.
DHCPD: client's VPN is ..
DHCPD: No option 125

DHCPD: DHCPREQUEST received from client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3230.302d.4574.302f.30
DHCPD: Sending DHCPACK to client 0063.6973.636f.2d61.6162.622e.6363.3030.2e35.3230.302d.4574.302f.30
DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: broadcasting BOOTREPLY to client aabb.cc00.5200.
R15#un all
All possible debugging has been turned off

R15#sh ip dh pool
Pool SERVER2:
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool:
Current index IP address range Leased addresses
172.31.100.101 - 172.31.100.1 - 172.31.100.254 1
**Bindings from all pools not associated with VRF:**

<table>
<thead>
<tr>
<th>IP address</th>
<th>Client-ID/ Hardware address/ User name</th>
<th>Lease expiration</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.100.100</td>
<td>0063.6973.636f.2d61. 6162.622e.6363.3030. 2e35.3230.302d.4574. 302f.30</td>
<td>Dec 21 2014 12:26 AM</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
Sydney Business Model HQ

PPPoE

Configure PPPoE between R17 and R18 – see Diagram
R18 must assign the same IP address back to R17 via PPPoE
Use PPPoe default group
Ensure R17 always gets the same IP address as per the topology
You are not allowed to use DHCP
R18 must require R17 to authenticate using PAP
PPP PAP hostname should be R17
Use “CISCO” as the PAP password
You are allowed to create only two additional interfaces
Do not create or assign statically any IP Addresses to any interfaces
Ensure that there is no fragmentation on the link

Configuration:

R17
interface Dialer1
  ip address negotiated
  ip mtu 1492
  encapsulation ppp
dialer pool 1
dialer idle-timeout 0
dialer persistent
  ppp pap sent-username R17 password 0 CISCO

interface Ethernet2/0
  no ip address
  pppoe-client dial-pool-number 1

R18
ip local pool R17_POOL 192.168.78.17

username R17 password 0 CISCO

interface Virtual-Templatel
  ip unnumbered Ethernet2/0
  encapsulation ppp
  ip mtu 1492
  peer default ip address pool R17_POOL
  ppp authentication pap

pppoe-group pppoe global
virtual-template 1

interface Ethernet2/0
  pppoe enable group global
Verification:

**Note:** We will first check if Layer 2 domain is configured correctly. R17 and R18 should be able to reach each other on VLAN 78. Let’s assign a temporary IP Address to R17:

R17(config)#int et 2/0
R17(config-if)#ip address 192.168.78.17 255.255.255.252
R17(config-if)#no sh
R17(config-if)#do ping 192.168.78.18 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.78.18, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/1/10 ms

**Note:** Layer 2 portion is working as expected

R17(config-if)#do show int et 2/0
Building configuration...
Current configuration : 44 bytes
! interface Ethernet2/0
  no ip address
end

R17(config-if)#
%DIALER-6-BIND: Interface Vi1 bound to profile Di1
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

R17(config-if)#do show ip int brie | exc unas
Interface          IP-Address     OK? Method Status                Protocol
Ethernet0/0         155.84.74.30   YES TFTP up                    up
Ethernet1/0          192.168.100.17 YES TFTP up                    up
Dialer1              192.168.78.17 YES IPCP up                    up
Loopback0            192.168.17.17 YES TFTP up                    up

R18#
*Dec 6 13:44:07.705: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
*Dec 6 13:44:07.705: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up

R17#show pppoe session
1 client session
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
SID  LocMAC                                      VA  Type
N/A   1  aabb.cc00.1202  Et2/0  Di1  Vi1        UP
aabb.cc00.1102  Di2  UP
R18#show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total

<table>
<thead>
<tr>
<th>Uniq ID</th>
<th>PPPoE</th>
<th>RemMAC</th>
<th>Port</th>
<th>VT</th>
<th>VA</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SID</td>
<td>LocMAC</td>
<td>VA-st</td>
<td>Type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>aabb.cc00.1102 Et2/0 1</td>
<td>Vi2.1</td>
<td>PTA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>aabb.cc00.1202</td>
<td></td>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>

R18#sh pppoe summary
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)

<table>
<thead>
<tr>
<th></th>
<th>TOTAL</th>
<th>PTA</th>
<th>FWDED</th>
<th>TRANS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet2/0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

R17#sh pppoe summary
1 client session

R17#ping 192.168.78.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.78.18, timeout is 2 seconds:
!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
Sydney Business Remote Office – SP#7

Multilink PPP

Configure PPP Multilink between R19 and R94 using their serial interfaces
Ensure that minimum of 2 serial interfaces are required to make the multilink active
Ensure that CDP is disabled on the connection
R94 must require R19 to authenticate using CHAP however R19 must not require R94 to authenticate
Do not use PPP chap hostname on R19
CHAP password should be “CCIE” (without quotes)
Make sure that all CHAP passwords are not encrypted in the configuration
Use TACACS server at 75.6.224.150 as authentication server
If the server is not reachable R94 should fallback to the local database and then no authentication
Do not use AAA Default authentication
For Tacacs security configuration use the following:
  Port – 88
  Tacacs password – “CCIETacacs+” (without quotes)
  Tacacs server must be configured under aaa group named TACACS_SERVER
Use the Multilink interface to source Tacacs packets from

Configuration:

R19

no service password-encryption

interface Multilink1
  ip address 155.84.74.38 255.255.255.252
  ppp chap password 0 CCIE
  ppp multilink
  ppp multilink links minimum 2 mandatory
  ppp multilink group 1
  no cdp enable

interface Serial1/0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1

interface Serial2/0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
no service password-encryption

aaa new-model

aaa group server tacacs+ TACACS_SERVER
    server 75.6.224.150

aaa authentication ppp PPP_MULTILINK group TACACS_SERVER local none

username R19 password 0 CCIE

interface Multilink1
    ip address 155.84.74.37 255.255.255.252
    ppp authentication chap PPP_MULTILINK
    ppp multilink
    ppp multilink links minimum 2 mandatory
    ppp multilink group 1
    no cdp enable

interface Serial3/0
    no ip address
    encapsulation ppp
    ppp multilink
    ppp multilink group 1

interface Serial4/0
    no ip address
    encapsulation ppp
    ppp multilink
    ppp multilink group 1

ip tacacs source-interface multilink 1

tacacs-server host 75.6.224.150 port 88 key CCIE	tacacs+

Verification:

R19#debug ppp authentication
    PPP authentication debugging is on

R94#debug ppp authentication
    PPP authentication debugging is on
R19#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R19(config)#int s 1/0
R19(config-if)#no sh
%LINK-3-UPDOWN: Interface Serial1/0, changed state to up
Se1/0 CHAP: I CHALLENGE id 1 len 24 from "R94"
Se1/0 CHAP: Using hostname from configured hostname
Se1/0 CHAP: Using password from interface CHAP
Se1/0 CHAP: O RESPONSE id 1 len 24 from "R19"

R19(config-if)#int s 2/0
R19(config-if)#no sh
%LINK-3-UPDOWN: Interface Serial2/0, changed state to up
Se2/0 CHAP: I CHALLENGE id 1 len 24 from "R94"
Se2/0 CHAP: Using hostname from configured hostname
Se2/0 CHAP: Using password from interface CHAP
Se2/0 CHAP: O RESPONSE id 1 len 24 from "R19"

R94#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R94(config)#int s 3/0
R94(config-if)#int s 4/0
R94(config-if)#no sh
%LINK-3-UPDOWN: Interface Serial3/0, changed state to up
Se3/0 CHAP: O CHALLENGE id 1 len 24 from "R94"
Se4/0 CHAP: O CHALLENGE id 1 len 24 from "R94"
Se3/0 CHAP: I RESPONSE id 1 len 24 from "R94"
Se3/0 CHAP: I RESPONSE id 1 len 24 from "R19"
Se3/0 CHAP: I RESPONSE id 1 len 24 from "R19"

R94#un all
All possible debugging has been turned off
R19#un all
All possible debugging has been turned off

R19#show ip int bri | inc \.
Ethernet0/0                 192.168.150.19  YES TFTP  up                    up
Multilink1                 155.84.74.38    YES manual up

R94#sh ppp multilink
Multilink1
   Bundle name: R19
   Remote Username: R19
   Remote Endpoint Discriminator: [1] R19
   Local Username: R94
   Local Endpoint Discriminator: [1] R94
   Bundle up for 00:09:44, total bandwidth 3088, load 1/255
   Receive buffer limit 24000 bytes, frag timeout 1000 ms
   0/0 fragments/bytes in reassembly list
   0 lost fragments, 0 reordered
   0/0 discarded fragments/bytes, 0 lost received
   0x3 received sequence, 0x4 sent sequence
   Member links: 2 active, 0 inactive (max 255, min 2)
   Se4/0, since 00:09:45
   Se3/0, since 00:09:44
   No inactive multilink interfaces

R19#sh ppp multilink
Multilink1
   Bundle name: R94
   Remote Username: R94
   Remote Endpoint Discriminator: [1] R94
   Local Username: R19
   Local Endpoint Discriminator: [1] R94
   Bundle up for 00:09:58, total bandwidth 3088, load 1/255
   Receive buffer limit 24000 bytes, frag timeout 1000 ms
   0/0 fragments/bytes in reassembly list
   0 lost fragments, 0 reordered
   0/0 discarded fragments/bytes, 0 lost received
   0x4 received sequence, 0x3 sent sequence
   Member links: 2 active, 0 inactive (max 255, min 2)
   Se1/0, since 00:10:00
   Se2/0, since 00:09:58
   No inactive multilink interfaces

R19#show interfaces multilink 1
Multilink1 is up, line protocol is up
   Hardware is multilink group interface
   Internet address is 155.84.74.38/30
   MTU 1500 bytes, BW 3088 Kbit/sec, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation PPP, LCP Open, multilink Open
   Open: IPCP, loopback not set
   Keepalive set (10 sec)
   DTR is pulsed for 2 seconds on reset
   <Output omitted>
R19#show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Link is a member of Multilink bundle Multilink1, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:04:40, output 00:00:01, output hang never
<Output omitted>

R94#show tacacs
Tcacs+ Server - public:
  Server address: 75.6.224.150
  Server port: 88
  Socket opens: 2
  Socket closes: 2
  Socket aborts: 0
  Socket errors: 0
  Socket Timeouts: 0
  Failed Connect Attempts: 0
  Total Packets Sent: 0
  Total Packets Recv: 0
SP#3/SP#4

PPP PAP/CHAP

Enable PPP encapsulation for the Serial link connecting R98 and R99
R99 should attempt to authenticate R98 using PAP and then CHAP
R98 should refuse CHAP authentication and use PAP
Use the name R98PAP and the password of CISCO to accomplish this
R98 should authenticate R99 using CHAP only
R99 should use the name R99PPP and the password of CISCO

Configuration:

R98
username R99PPP password CISCO
interface Serial1/0
encapsulation ppp
ppp authentication chap
ppp chap refuse
ppp pap sent-username R98PAP password 0 CISCO

R99
username R98PAP password CISCO
interface Serial1/0
encapsulation ppp
ppp authentication ppp chap
ppp chap hostname R99PPP
ppp chap password 0 CISCO

Verification:

R98#sh ppp interface serial 1/0
<Output omitted>
PPP Session Info
----------------
Interface          : Se1/0
PPP ID             : 0xA0000001
Phase              : UP
Stage              : Local Termination
Peer Name          : R99PPP
Peer Address       : 66.171.14.1
<Output omitted>
Se1/0 LCP: [Open]
Our Negotiated Options
Se1/0 LCP:  AuthProto CHAP (0x0305C22305)
Se1/0 LCP:  MagicNumber 0xb0490b5 (0x0506bd0490b5)
Peer’s Negotiated Options
Se1/0 LCP:  AuthProto PAP (0x0304C023)
Se1/0 LCP:  MagicNumber 0xb04a009 (0x0506bd04a009)
Se1/0 IPCP: [Open]
Our Negotiated Options
Se1/0 IPCP:  Address 66.171.14.2 (0x030642AB0E02)
Peer’s Negotiated Options
Se1/0 IPCP:  Address 66.171.14.1 (0x030642AB0E01)
<Output omitted>
R99#show ppp interface s1/0
PPP Serial Context Info
---------------------
Interface: S1/0
PPP ID: 0x4B000041
Phase: UP
Stage: Local Termination
Peer Name: R98PAP
Peer Address: 66.171.14.2

Se1/0 LCP: [Open]
Our Negotiated Options
Se1/0 LCP: AuthProto PAP (0x0304C023)
Se1/0 LCP: MagicNumber 0xBBEB50B7 (0x0506BBEB50B7)
Peer’s Negotiated Options
Se1/0 LCP: AuthProto CHAP (0x0305C22305)
Se1/0 LCP: MagicNumber 0xBBEB625D (0x0506BBEB625D)
Se1/0 IPCP: [Open]
Our Negotiated Options
Se1/0 IPCP: Address 66.171.14.1 (0x030642AB0E01)
Peer’s Negotiated Options
Se1/0 IPCP: Address 66.171.14.2 (0x030642AB0E02)

R98#debug ppp authentication
PPP authentication debugging is on
R98
Se1/0 PAP: Using default call direction
Se1/0 PAP: Treating connection as a dedicated line
Se1/0 PAP: Session handle[2000044] Session id[66]
Se1/0 PAP: Using hostname from interface PAP
Se1/0 PAP: Using password from interface PAP
Se1/0 PAP: O AUTH id 1 len 17 from "R98PAP"
Se1/0 CHAP: O CHALLENGE id 1 len 24 from "R98"
Se1/0 CHAP: I RESPONSE id 1 len 27 from "R99PPP"
Se1/0 PPP: Sent CHAP LOGIN Request
Se1/0 PPP: Received LOGIN Response PASS
Se1/0 CHAP: O SUCCESS id 1 len 4
Se1/0 PAP: I AUTH-ACK id 1 len 5
PPP EAP

Configure PPP encapsulation on the circuit connecting R92 and R97
Both routers should attempt to authenticate each other using EAP
Use the name R92EAP and R97EAP and the password of CISCO for this task
Ensure remote IP Address of the remote peer does not appear in router’s routing table

**Configuration:**

**R92**

username R97EAP password CISCO

interface Serial3/0
  encapsulation ppp
  no peer neighbor-route
  ppp authentication eap
  ppp eap identity R92EAP
  ppp eap password 0 CISCO
  ppp eap local

**R97**

username R92EAP password CISCO

interface Serial2/0
  encapsulation ppp
  no peer neighbor-route
  ppp authentication eap
  ppp eap identity R97EAP
  ppp eap password 0 CISCO
  ppp eap local

**Verification:**

R92#deb ppp authentication
PPP authentication debugging is on
*Dec 20 00:52:12.545: %SYS-5-CONFIG_I: Configured from console by console
*Dec 20 00:52:12.692: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
Se3/0 PPP: Using default call direction
Se3/0 PPP: Treating connection as a dedicated line
Se3/0 PPP: Session handle[6000002] Session id[2]
Se3/0 EAP: O REQUEST IDENTITY id 1 len 5
Se3/0 EAP: I REQUEST IDENTITY id 1 len 5
Se3/0 EAP: O RESPONSE IDENTITY id 1 len 11 from "R92EAP"
Se3/0 EAP: I RESPONSE IDENTITY id 1 len 11 from "R97EAP"
Se3/0 EAP: O REQUEST MD5 id 2 len 28 from "R92EAP"
Se3/0 EAP: I REQUEST MD5 id 2 len 28 from "R97EAP"
Se3/0 PPP: Sent EAP SENDAUTH Request
Se3/0 EAP: O RESPONSE MD5 id 2 len 28 from "R97EAP"
Se3/0 PPP: Received SENDAUTH Response BEGIN
Se3/0 EAP: Using hostname from interface EAP
Se3/0 EAP: Using password from interface EAP
Se3/0 EAP: O RESPONSE MD5 id 2 len 28 from "R92EAP"
Se3/0 PPP: Sent CHAP LOGIN Request
Se3/0 EAP: I SUCCESS id 2 len 4
Se3/0 EAP: O SUCCESS id 2 len 4
Dec 20 00:52:12.793: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up
R92#un all
All possible debugging has been turned off

R92#sh ppp statistics
Type PPP Statistic

--- ------------------------------- TOTAL SINCE CLEARED
14 PPP Handles Allocated 2 2
15 PPP Handles Freed 1 1
19 PPP Encapped Interfaces 1 1
20 PPP Fast Starts 1 1
24 LCP Timeout+ 3 3

Type PPP Statistic PEAK CURRENT
--- -------------------------------
1 Links at LCP Stage 1 0
2 Links at Unauthenticated Name Stage 1 0
3 Links at Authenticated Name Stage 1 0
7 Links at Local Termination Stage 1 1

20 Successful LCP negotiations 1 1
22 Entered Authentication Stage 1 1
28 IPCP UP Sessions 1 1
57 EAP authentication attempts 1 1
58 EAP authentication successes 1 1
95 Total Sessions 1 1
96 Non-MLP Sessions 1 1
98 Total Links 1 1
99 Non-MLP Links 1 1

Type PPP Statistic TOTAL SINCE CLEARED
--- -------------------------------
29 Lower Layer disconnected 1 1

R92#show ip route | inc 86.191.16.* connected
C 86.191.16.4/30 is directly connected, Serial3/0
L 86.191.16.6/32 is directly connected, Serial3/0
C 86.191.16.8/30 is directly connected, Serial4/0
L 86.191.16.10/32 is directly connected, Serial4/0

R97#show ip route | inc 86.191.16.* connected
C 86.191.16.0/30 is directly connected, Serial1/0
L 86.191.16.2/32 is directly connected, Serial1/0
C 86.191.16.4/30 is directly connected, Serial2/0
L 86.191.16.5/32 is directly connected, Serial2/0
Note:

The EIGRP composite metric is not scaled correctly for high-bandwidth interfaces or Ethernet channels resulting in incorrect or inconsistent routing behavior. The lowest delay that can be configured for an interface is 10 microseconds. As a result, interfaces with a higher speed, such as a 10 Gigabit Ethernet (GE) interface or high-speed interfaces channeled together, such as in the case of a GE Etherchannel, will appear to Enhanced Interior Gateway Routing Protocol (EIGRP) as a single GE interface. This may cause undesirable equal-cost-load balancing. To resolve this issue, the EIGRP Wide Metrics feature introduces 64-bit metric calculations and Routing Information Base (RIB) scaling. This provides the ability to support interfaces (either directly or via channeling techniques like port-channels or ether-channels) up to approximately 4.2 terabits.

Adjusting EIGRP metric weights can dramatically affect network performance. Because of the complexity of this task, we recommend that you do not change the default K values without guidance from an experienced network designer.

By default, the EIGRP composite cost metric is a 32-bit quantity that is the sum of segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. The formula used to scale and invert the bandwidth value is \( \frac{107}{\text{minimum bandwidth in kilobits per second}} \). However, with the EIGRP Wide Metrics feature, the EIGRP composite cost metric is scaled to include 64-bit metric calculations for EIGRP named mode configurations.

With the calculation of larger bandwidths, EIGRP can no longer fit the computed metric into a 4-byte unsigned long value needed by the Cisco IOS RIB. To set the RIB scaling factor for EIGRP, use the `metric rib-scale` command. When configured, the `metric rib-scale` command results in all EIGRP routes in the RIB to be cleared and replaced with the new metric values.

**EIGRP Classic to Named Mode Conversions**

- You must use the `eigrp upgrade-cli` command to convert Enhanced Interior Gateway Routing Protocol (EIGRP) configurations from classic mode to named mode. If multiple classic mode configurations exist, you must use this command per EIGRP autonomous system number in classic mode.
- The `eigrp upgrade-cli` command blocks the router from accepting any other command until the conversion is complete (the console is locked). The time taken to complete the conversion depends on the size of the configuration. However, the conversion is a one-time activity.
- The `eigrp upgrade-cli` command is available only under EIGRP classic router configuration mode. Therefore, you can convert configurations from classic mode to named mode but not vice-versa.

There are two ways we can create EIGRP neighbor relationship:

- **Use “network” command:** this is the more popular way to create EIGRP neighbor relationship. That router will check which interfaces whose IP addresses belong to the and turn EIGRP on that interface. EIGRP messages are sent via multicast packets.
- **Use “neighbor” command:** The interface(s) that have this command applied no longer send or receive EIGRP unicast packets.

EIGRP messages are sent via unicast. The router only accepts EIGRP packets from peers that are explicitly configured with a neighbor statement. Consequently, any messages coming from routers without a corresponding neighbor statement are discarded.

*directly from Cisco website*
Note:

Feasibility condition in EIGRP

The advertised metric from an EIGRP neighbor (peer) to the local router is called Advertised Distance (or reported distance) while the metric from the local router to that network is called Feasible Distance. For example, R1 advertises network 10.10.10.0/24 with a metric of 20 to R2. For R2, this is the advertised distance. R2 calculates the feasible distance by adding the metric from the advertised router (R1) to itself. So in this case the feasible distance to network 10.10.10.0/24 is 20 + 50 = 70.

Before a router can be considered a feasible successor, it must pass the feasibility condition rule. In short, the feasibility condition says that if we learn about a prefix from a neighbor, the advertised distance from that neighbor to the destination must be lower than our feasible distance to that same destination. Therefore we see the Advertised Distance always smaller than the Feasible Distance to satisfy the feasibility condition.

Function of an EIGRP sequence TLV packet

The function of an EIGRP sequence TLV packet is to list the peers that should not listen to the next multicast packet during the reliable multicast process. EIGRP sends updates and other information between routers using multicast packets to 224.0.0.10. For example in the topology below, R1 made a change in the topology and it needs to send updates to R2 & R3. It sends multicast packets to EIGRP multicast address 224.0.0.10. Both R2 & R3 can receive the updates and acknowledge back to R1 using unicast.

But what if R1 sends out updates, only R2 replies but R3 never does? In the case a router sends out a multicast packet that must be reliably delivered (like in this case), an EIGRP process will wait until the RTO (retransmission timeout) period has passed before beginning a recovery action. This period is calculated from the SRTT (smooth round-trip time). After R1 sends out updates it will wait for this period to expire. Then it makes a list of all the neighbors from which it did not receive an Acknowledgement (ACK). Next it sends out a packet telling these routers stop listening to multicast until they are been notified that it is safe again. Finally the router will begin sending unicast packets with the information to the routers that didn’t answer, continuing until they are caught up:

- R1 sends out updates to 224.0.0.10
- R2 responds but R3 does not
- R1 waits for the RTO period to expire
- R1 then sends out an unreliable-multicast packet, called a sequence TLV (Type-Length-Value) packet, which tells R3 not to listen to multicast packets any more
- R1 continues sending other multicast traffic it has to R3 using unicast to R3, until it acknowledges all the packets
- Once R3 has caught up, R1 will send another sequence TLV, telling R3 to begin listening to multicast again.

The sequence TLV packet contains a list of the nodes that should not listen to multicast packets while the recovery takes place. But notice that the TLV packet in step 6 does not contain any nodes in the list.

Note: In the case R3 still does not reply in step 4, R1 will attempt to retransmit the unicast 16 times or continue to retransmit until the hold time for the neighbor in question expires. After this time, R1 will declare a retransmission limit exceeded error and will reset the neighbor.

*directly from Cisco website*
San Francisco Group Remote Site

EIGRP
Configure EIGRP using Autonomous-System 150
The Router-ID must be configured to the router’s Loopback0 interface
Do not forget to advertise Loopback0 and Loopback1 interfaces into EIGRP
Ensure wildcard mask reflects subnet mask

R12 will be the only EIGRP enabled device.
Ensure that any neighboring upstream router will not query R12 for any lost routes

Use EIGRP 64bit version
Configure R12 so that "sh ip eig top" and "sh ip prot" as per both verification outputs below

Configuration:

R12
router eigrp San_Francisco_Group
   address-family ipv4 unicast autonomous-system 150
topology base
distance eigrp 91 171
exit-af-topology
network 192.12.12.12 0.0.0.0
network 192.168.20.0 0.0.0.255
network 192.168.21.0 0.0.0.15
eigrp router-id 192.12.12.12
eigrp stub connected summary
exit-address-family

Verification:

R12#sh ip eig top
EIGRP-IPv4 VR(San_Francisco_Group) Topology Table for AS(150)/ID(192.12.12.12)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, 
r - reply Status, s - sia Status

P 192.12.12.12/32, 1 successors, FD is 163840
   via Connected, Loopback0
P 192.168.21.0/28, 1 successors, FD is 163840
   via Connected, Loopback1
P 192.168.20.0/24, 1 successors, FD is 131072000
   via Connected, Ethernet1/0
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates

EIGRP-IPv4 VR(San_Francisco_Group) Address-Family Protocol for AS(150)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
Metric rib-scale 128

Metric version 64bit
NSF-aware route hold timer is 240

Stub, connected, summary
Topology : 0 (base)
    Active Timer: 3 min
        Distance: internal 91 external 171
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
        Total Prefix Count: 3
    Total Redist Count: 0
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
    192.12.12/32
    192.168.20.0
    192.168.21.0/28
Routing Information Sources:
    Gateway         Distance      Last Update
        Distance: internal 91 external 171
San Francisco Group Data Centre

EIGRP

Configure EIGRP using Autonomous-System 150
The Router-ID must be configured to the router’s Loopback0 interface
Advertise Loopback0 of R13 into EIGRP without using network statement
Do not advertise Loopback1 into EIGRP at this point
Use EIGRP 64bit version
Ensure that your configuration produces below verification outputs

Configuration:

```
R13
router eigrp San_Francisco_Group
    address-family ipv4 unicast autonomous-system 150
topology base
    redistribute connected metric 1000 1 255 1 1500 route-map LOOPBACK
exit-of-topology
    network 192.168.30.13 0.0.0.0
eigrp router-id 192.13.13.13
exit-address-family
    route-map LOOPBACK permit 10
    match interface Loopback0
```

Verification:

```
R13#sh ip eig top
EIGRP-IPv4 VR(San_Francisco_Group) Topology Table for AS(150)/ID(192.13.13.13)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.13.13.13/32, 1 successors, FD is 656015360 via Connected (656015360/0)
P 192.168.30.0/24, 1 successors, FD is 131072000 via Connected, Ethernet1/0

R13#sh ip eig top 192.13.13.13/32
EIGRP-IPv4 VR(San_Francisco_Group) Topology Entry for AS(150)/ID(192.13.13.13) for 192.13.13.13/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 656015360
Descriptor Blocks:
0.0.0.0, from Connected, Send flag is Ox0
Composite metric is (656015360/0), route is External
Vector metric:
    Minimum bandwidth is 1000 Kbit
    Total delay is 10000000 picoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
    Originating router is 192.13.13.13
External data:
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```
R13#sh ip eigr top 192.168.30.0/24
EIGRP-IPv4 VR(San_Francisco_Group) Topology Entry for AS(150)/ID(192.13.13.13) for 192.168.30.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 131072000
Descriptor Blocks:
0.0.0.0 (Ethernet1/0), From Connected, Send flag is 0x0
Composite metric is (131072000/0), route is Internal
Vector metric:
  Minimum bandwidth is 10000 Kbit
  Total delay is 1000000000 picoseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 0
  Originating router is 192.13.13.13

R13#sh ip prot
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
Redistributing: connected
EIGRP-IPv4 VR(San_Francisco_Group) Address-Family Protocol for AS(150)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 240
  Router-ID: 192.13.13.13
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 2
    Total Redist Count: 1
  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    192.168.30.13/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    Distance: internal 90 external 170
San Francisco Group HQ

EIGRP

Configure EIGRP using Autonomous-System 150

The Router-ID must be configured to the router’s Loopback0 interface

Advertise Loopback0 of all devices and Loopback1 of R8 and R9 into EIGRP

Use EIGRP 64bit version

EIGRP instance should be named "San_Francisco_HQ" without the quotes

On R9 wildcard mask should be relevant to the subnet mask

Configuration:

**SW1**

```plaintext
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
network 192.101.101.101 0.0.0.0
network 192.168.10.6 0.0.0.0
network 192.168.10.13 0.0.0.0
eigrp router-id 192.101.101.101
ext-address-family
```

**SW2**

```plaintext
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
network 192.102.102.102 0.0.0.0
network 192.168.10.10 0.0.0.0
network 192.168.10.17 0.0.0.0
eigrp router-id 192.102.102.102
exit-address-family
```

**R8**

```plaintext
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
network 192.8.8.8 0.0.0.0
network 192.188.188.188 0.0.0.0
network 192.168.10.1 0.0.0.0
network 192.168.10.5 0.0.0.0
network 192.168.10.21 0.0.0.0
eigrp router-id 192.8.8.8
exit-address-family
```
R9
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
  exit-af-topology
  network 192.9.9.9 0.0.0.0
  network 192.199.199.199 0.0.0.0
  network 192.168.10.0 0.0.0.3
  network 192.168.10.8 0.0.0.3
eigrp router-id 192.9.9.9
exit-address-family

R10
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
  exit-af-topology
  network 192.10.10.10 0.0.0.0
  network 192.168.10.14 0.0.0.0
  network 192.168.10.25 0.0.0.0
eigrp router-id 192.10.10.10
exit-address-family

R11
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
  exit-af-topology
  network 192.11.11.11 0.0.0.0
  network 192.168.10.18 0.0.0.0
  network 192.168.10.22 0.0.0.0
  network 192.168.10.26 0.0.0.0
eigrp router-id 192.11.11.11
exit-address-family

Verification:

R8#sh ip eig ne
EIGRP-IPv4 VR(San_Francisco_HQ) Address-Family Neighbors for AS(150)
H   Address                 Interface
Hold Uptime   SRTT   RTO  Q  Seq
(sec)         (ms)       Cnt Num
2   192.168.10.22           Et2/0                    11 00:01:19    5   100  0  7
1   192.168.10.2            Et1/0
     12 00:02:29    3   100  0  11
0   192.168.10.6            Et3/0                    11 00:03:05    4   100  0  11

R9#sh ip eig ne detail
EIGRP-IPv4 VR(San_Francisco_HQ) Address-Family Neighbors for AS(150)
H   Address                 Interface
Hold Uptime   SRTT   RTO  Q  Seq
(sec)         (ms)       Cnt Num
1   192.168.10.10             Et2/0         14 00:03:36  800 4800 0  11
Version 7.0/3.0, Retrans: 1, Retries: 0, Prefixes: 7
Topology-ids from peer - 0
0   192.168.10.1              Et1/0         13 00:03:36  808 4848 0  19
Version 14.0/2.0, Retrans: 1, Retries: 0, Prefixes: 10
Topology-ids from peer - 0
R1#sh ip prot
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 VR(San_Francisco_HQ) Address-Family Protocol for AS(150)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
Metric rib-scale 128
Metric version 64bit
NSF-aware route hold timer is 240
Router-ID: 192.10.10.10
Topology: 0 (base)
  Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
  Total Prefix Count: 15
  Total Redist Count: 0
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  192.10.10.10/32
  192.168.10.14/32
  192.168.10.25/32
Routing Information Sources:
  Gateway  Distance  Last Update
  192.168.10.13  90  00:04:22
  192.168.10.26  90  00:04:22
Distance: internal 90 external 170

R9#sh ip prot
Routing Protocol is "eigrp 150"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 VR(San_Francisco_HQ) Address-Family Protocol for AS(150)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
Metric rib-scale 128
Metric version 64bit
NSF-aware route hold timer is 240
Router-ID: 192.9.9.9
Topology: 0 (base)
  Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
  Total Prefix Count: 15
  Total Redist Count: 0
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  192.9.9.9/32
  192.168.10.0/30
  192.168.10.8/30
  192.199.199.199/32
Routing Information Sources:
  Gateway  Distance  Last Update
  192.168.10.1  90  00:06:22
  192.168.10.10 90  00:06:22
Distance: internal 90 external 170
EIGRP Metric

On R9 configure **Loopback 100 192.99.99.99/32** with a description of **“Metric Test”** without the quotes. Redistribute this prefix into EIGRP using metric values of 1 1 1 1. You are not allowed to use an ACL or match an interface under a route map. Any configuration instances should be named **“Metric”** without the quotes. Ensure R8, R10, and R11 can see Lo:100 prefix in their EIGRP topology table and the routing table.

**Configuration:**

**R9**

```
interface Loopback100
  description Metric Test
  ip address 192.99.99.99 255.255.255.255

ip prefix-list Metric seq 5 permit 192.99.99.99/32
route-map Metric permit 10
  match ip address prefix-list Metric

router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
  redistribute connected metric 1 1 1 1 route-map Metric
exit-af-topology
metric rib-scale 153
exit-address-family
```

**R8**

```
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
metric rib-scale 153
exit-address-family
```

**R10**

```
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
metric rib-scale 153
exit-address-family
```

**R11**

```
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
topology base
exit-af-topology
metric rib-scale 153
exit-address-family
```
Verification:

R8#sh ip eigrp topology 192.99.99/32
EIGRP-IPv4 VR(San Francisco_HQ) Topology Entry for AS(150)/ID(192.8.8.8) for 192.99.99/32
State is Passive, Query origin flag is 1, 0 Successor(s), FD is Infinity, RIB is 4294967295
Descriptor Blocks:
192.168.10.2 (Ethernet1/0), from 192.168.10.2, Send flag is 0x0
  Composite metric is (655426191360/655360655360), route is External
  Vector metric:
    Minimum bandwidth is 1 Kbit
    Total delay is 1010000000 picoseconds
    Reliability is 1/255
    Minimum MTU is 1
    Hop count is 1
    Originating router is 192.9.9.9
  External data:
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)

R8#sh ip route 192.99.99.99
% Network not in table

Note: The RIB’s metric can’t exceed 32-bits, and there are circumstances with the new, more granular metrics won’t fit into the RIB. So all metrics, regardless of if the value would fit into 32-bits, are divided by the rib-scale value. The rib-scale is 128 by default:

655426191360/128 = 5120517120

One important note here is that with wide metrics, the EIGRP calculated metric no longer fits into the RIB. The largest number that can be represented in a 32-bit unsigned integer is 4,294,967,295 scale is 128 by default:

5120517120 > 4294967296

therefore it cannot be represented in the RIB:

R8#sh ip route 192.99.99.99
% Network not in table

This is a valid, routable prefix that simply can’t make it into the RIB because of compatibility between the EIGRP topology table and the RIB. You need to adjust the rib-scale to make this work: Metric rib-scale 153

655426191360/153 = 4283831316 < 4294967296

On all routers:

    router eigrp San_Francisco_HQ
    address-family ipv4 unicast autonomous-system 150
    metric rib-scale 153
R8#sh ip eigrp topology 192.99.99.99/32
EIGRP-IPv4 VR(San Francisco_HQ) Topology Entry for AS(150)/ID(192.8.8.8) for 192.99.99.99/32
Descriptor Blocks:
192.168.10.2 (Ethernet1/0), from 192.168.10.2, Send flag is 0x0
Composite metric is (655426191360/655360655360), route is External
Vector metric:
Minimum bandwidth is 1 Kbit
Total delay is 1010000000 picoseconds
Reliability is 1/255
Load is 1/255
Minimum MTU is 1
Hop count is 1
Originating router is 192.9.9.9
External data:
AS number of route is 0
External protocol is Connected, external metric is 0
Administrator tag is 0 (0x00000000)
192.168.10.22 (Ethernet2/0), from 192.168.10.22, Send flag is 0x0
Composite metric is (655492382720/655426846720), route is External
Vector metric:
Minimum bandwidth is 1 Kbit
Total delay is 2020000000 picoseconds
Reliability is 1/255
Load is 1/255
Minimum MTU is 1
Hop count is 3
External data:
Originating router is 192.9.9.9
AS number of route is 0
External protocol is Connected, external metric is 0
Administrator tag is 0 (0x00000000)

R8#sh ip route 192.99.99.99
Routing entry for 192.99.99.99/32
Known via "eigrp 150", distance 170, metric 4283831316, type external
Last update from 192.168.10.2 on Ethernet1/0, 00:14:11 ago
Routing Descriptor Blocks:
* 192.168.10.2, from 192.168.10.2, 00:14:11 ago, via Ethernet1/0
   Route metric is 4283831316, traffic share count is 1
   Total delay is 1010 microseconds, minimum bandwidth is 1 Kbit
   Reliability 1/255, minimum MTU 1 bytes
   Loading 1/255, Hops 1
**EIGRP Offset-List**

Unless there is a link failure between R9 and SW2, R9 should always choose SW2 as an exit point to reach Loopback1 of R8 within EIGRP HQ AS150 domain

Do not use distribute list for this task

Do not use prefix list for your solution

**Configuration:**

```
R9:
   router eigrp San_Francisco_HQ
   address-family ipv4 unicast autonomous-system 150
topology base
   offset-list 1 in 2147483647 Ethernet1/0
   exit-af-topology
   exit-address-family

   access-list 1 permit 192.188.188.188
```

**Verification: Before Implementation**

```
R9#sh ip route 192.188.188.188
Routing entry for 192.188.188.188/32
   Known via "eigrp 150", distance 90, metric 857215, type internal
   Redistributing via eigrp 150
   Last update from 192.168.10.1 on Ethernet1/0, 00:24:32 ago
   Routing Descriptor Blocks:
      * 192.168.10.1, from 192.168.10.1, 00:24:32 ago, via Ethernet1/0
         Route metric is 857215, traffic share count is 1
   Total delay is 1002 microseconds, minimum bandwidth is 10000 Kbit
   Reliability 255/255, minimum MTU 1500 bytes
   Loading 1/255, Hops 1

R9#sh ip eig top 192.188.188.188/32
EIGRP-IPv4 VR(San_Francisco_HQ) Topology Entry for AS(150)/ID(192.9.9.9) for 192.188.188.188/32
   State is Passive, Query origin flag is 1, 1 Successor(s), FD is 131153920, RIB is 857215
   Descriptor Blocks:
      192.168.10.1 (Ethernet1/0), from 192.168.10.1, Send flag is 0x0
         Composite metric is (131153920/163840), route is Internal
         Vector metric:
            Minimum bandwidth is 10000 Kbit
            Total delay is 1001250000 picoseconds
            Reliability is 255/255
            Load is 1/255
            Minimum MTU is 1500
         Hop count is 1
         Originating router is 192.8.8.8
```
Verification: After Implementation

R9#
*Dec 20 02:33:37.016: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.1 (Ethernet1/0) is resync: intf route configuration changed

R9#sh ip route 192.188.188.188
Routing entry for 192.188.188.188/32
Known via "eigrp 150", distance 90, metric 1713894, type internal
Redistributing via eigrp 150
Last update from 192.168.10.10 on Ethernet2/0, 00:00:36 ago
Routing Descriptor Blocks:
  * 192.168.10.10, from 192.168.10.10, 00:00:36 ago, via Ethernet2/0
    Route metric is 1713894, traffic share count is 1
    Total delay is 3002 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 3

R9#sh ip eig top 192.188.188.188/32
EIGRP-IPv4 VR(San_Francisco_HQ) Topology Entry for AS(150)/ID(192.9.9.9) for 192.188.188.188/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 262225920, RIB is 1713894
Descriptor Blocks:
  192.168.10.10 (Ethernet2/0), from 192.168.10.10, Send flag is 0x0
    Composite metric is (262225920/196689920), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 3001250000 picoseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
    Hop count is 3
  192.168.10.1 (Ethernet1/0), from 192.168.10.1, Send flag is 0x0
    Composite metric is (2278637567/2147647487), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 33769249985 picoseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
    Hop count is 1
    Originating router is 192.8.8.8

Note: R8 Loopback1 192.188.188.188/32 is reachable via SW2 whereas R8 Loopback0 192.8.8.8/32 directly via R8

R9#sh ip route 192.8.8.8
Routing entry for 192.8.8.8/32
Known via "eigrp 150", distance 90, metric 857215, type internal
Redistributing via eigrp 150
Last update from 192.168.10.1 on Ethernet1/0, 00:29:12 ago
Routing Descriptor Blocks:
  * 192.168.10.1, from 192.168.10.1, 00:29:12 ago, via Ethernet1/0
    Route metric is 857215, traffic share count is 1
    Total delay is 1002 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
R9#sh ip eigrp top 192.8.8.8/32
EIGRP-IPv4 VR(San_Francisco_HQ) Topology Entry for AS(150)/ID(192.9.9.9) for 192.8.8.8/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 131153920, RIB is 857215
Descriptor Blocks:
192.168.10.1 (Ethernet1/0), from 192.168.10.1, Send flag is 0x0
  Composite metric is (131153920/163840), route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1001250000 picoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
    Originating router is 192.8.8.8

R9#sh ip route | in Incom
Incoming update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Incoming routes in Ethernet1/0 will have 2147483647 added to metric if on list 1

R9#sh access-list 1
Standard IP access list 1
  10 permit 192.188.188.188 (2 matches)
EIGRP Distribute List

Ensure that R10 always uses R11 to reach Loopback1 of R9
This configuration should not affect any other prefix
Do not use offset list for this task
Do not use ACL anywhere in your configuration

Configuration:

R10
router eigrp San_Francisco_HQ
    address-family ipv4 unicast autonomous-system 150
topology base
distribute-list prefix NETWORK gateway GATEWAY in Ethernet1/0
exit-af-topology
exit-address-family

    ip prefix-list GATEWAY seq 5 permit 192.168.10.13/32
    ip prefix-list NETWORK seq 5 deny 192.199.199.199/32
    ip prefix-list NETWORK seq 10 permit 0.0.0.0/0 le 32

Verification: Before Implementation

R10#sh ip route 192.199.199.199
Routing entry for 192.199.199.199/32
  Known via "eigrp 150", distance 90, metric 1289838, type internal
  Redistributing via eigrp 150
  Last update from 192.168.10.13 on Ethernet1/0, 00:43:06 ago
Routing Descriptor Blocks:
  * 192.168.10.26, from 192.168.10.26, 00:43:06 ago, via Ethernet2/0
    Route metric is 1289838, traffic share count is 1
    Total delay is 2012 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 3
  192.168.10.13, from 192.168.10.13, 00:43:06 ago, via Ethernet1/0
    Route metric is 1289838, traffic share count is 1
    Total delay is 2012 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 3
R10#sh ip eig top 192.199.199.199/32
EIGRP-IPv4 VR(San_Francisco_HQ) Topology Entry for AS(150)/ID(192.10.10.10) for 192.199.199.199/32
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 197345280, RIB is 1289838
Descriptor Blocks:
192.168.10.13 (Ethernet1/0), from 192.168.10.13, Send flag is 0x0
  Composite metric is (197345280/131809280), route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 201250000 picoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
  Hop count is 3

192.168.10.26 (Ethernet2/0), from 192.168.10.26, Send flag is 0x0
  Composite metric is (197345280/131809280), route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 201250000 picoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
  Hop count is 3

Verification: After Implementation

R10#
*Dec 20 02:52:27.487: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.13 (Ethernet1/0) is resync: intf route configuration changed

R10#sh ip route 192.199.199.199
Routing entry for 192.199.199.199/32
  Known via "eigrp 150", distance 90, metric 1289838, type internal
  Redistributing via eigrp 150
  Last update from 192.168.10.26 on Ethernet2/0, 00:00:26 ago
Routing Descriptor Blocks:
  * 192.168.10.26, from 192.168.10.26, 00:00:26 ago, via Ethernet2/0
    Route metric is 1289838, traffic share count is 1
    Total delay is 2012 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 3

R10#sh ip eig top 192.199.199.199/32
EIGRP-IPv4 VR(San_Francisco_HQ) Topology Entry for AS(150)/ID(192.10.10.10) for 192.199.199.199/32
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 197345280, RIB is 1289838
Descriptor Blocks:
192.168.10.26 (Ethernet2/0), from 192.168.10.26, Send flag is 0x0
  Composite metric is (197345280/131809280), route is Internal
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 201250000 picoseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
  Hop count is 3
Note:

A route tag:

- is a 32-bit value attached to routes
- used to filter routes and apply administrative policies, such as redistribution and route summarization, to tagged routes
- you can tag routes within a route map by using the set tag command. You can match tagged routes and apply administrative policies to tagged routes within a route map by using the match tag or match tag list command. The match tag list command is used to match a list of route tags.

Route tags will not be displayed in dotted-decimal format if the route-tag notation global configuration command is not enabled on the device.

Prior to the EIGRP Route Tag Enhancements feature, EIGRP routes could only be tagged using plain decimals (range: 1 to 4294967295).

This feature enables users to specify and display route tag values as dotted decimals (range: 0.0.0.0 to 255.255.255.255), similar to the format used by IPv4 addresses.

This enhancement is intended to simplify the use of route tags as users can now filter routes by using the route tag wildcard mask.

This feature also allows you to configure a default route tag for all internal EIGRP routes without using route maps. Use the eigrp default-route-tag command in address family configuration mode to configure a default route tag for internal EIGRP routes.

*directly from Cisco website*
**EIGRP Route Tag**

Configure the following Loopback interfaces and IP Addresses on R8:

- Loopback101: 1.1.1.1/32
- Loopback102: 2.2.2.2/32
- Loopback103: 3.3.3.3/32
- Loopback104: 4.4.4.4/32
- Loopback105: 5.5.5.5/32
- Loopback106: 6.6.6.6/32
- Loopback107: 7.7.7.7/32

Redistribute these networks into EIGRP using the following criteria:

- These prefixes should be seen as an EIGRP external routes
- 1.1.1.1 / 2.2.2.2 / 3.3.3.3 should be tagged with 100.100.100.1 value
- 4.4.4.4 / 5.5.5.5 should be tagged with 100.100.200.1 value
- 6.6.6.6 and 7.7.7.7 should be tagged with 100.100.101.1 value
- R11 should filter all prefixes that begin with 100.100 and have an even 3rd octet
- All route tags should be seen in a dotted-decimal notation
- Do not use ACL or prefix list for your solution

**Configuration:**

```
R8

interface Loopback101
 ip address 1.1.1.1 255.255.255.255

interface Loopback102
 ip address 2.2.2.2 255.255.255.255

interface Loopback103
 ip address 3.3.3.3 255.255.255.255

interface Loopback104
 ip address 4.4.4.4 255.255.255.255

interface Loopback105
 ip address 5.5.5.5 255.255.255.255

interface Loopback106
 ip address 6.6.6.6 255.255.255.255

interface Loopback107
 ip address 7.7.7.7 255.255.255.255

route-map tag-routes permit 10
 match interface Loopback101 Loopback102 Loopback103
 set tag 100.100.100.1

route-map tag-routes permit 20
 match interface Loopback104 Loopback105
 set tag 100.100.200.1

route-map tag-routes permit 30
 match interface Loopback106 Loopback107
 set tag 100.100.101.1
```
route-tag notation dotted-decimal

router eigrp San_Francisco_HQ
    address-family ipv4 unicast autonomous-system 150
topology base
    redistribute connected route-map tag-routes
    exit-af-topology
    exit-address-family

R11
route-tag notation dotted-decimal
route-tag list binary-match seq 5 permit 100.100.0.0 0.0.254.255

route-map filter deny 10
    match tag list binary-match

route-map filter permit 20

router eigrp San_Francisco_HQ
    address-family ipv4 unicast autonomous-system 150
topology base
distribute-list route-map filter in Ethernet1/0
distribute-list route-map filter in Ethernet2/0
distribute-list route-map filter in Ethernet3/0
    exit-af-topology
    exit-address-family

Verification: Before Implementation

R11#sh ip route eig | in EX
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
D EX 1.1.1.1 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 2.2.2.2 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 3.3.3.3 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 4.4.4.4 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 5.5.5.5 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 6.6.6.6 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 7.7.7.7 [170/857215] via 192.168.10.21, 00:14:40, Ethernet2/0
D EX 192.168.10.21 (Ethernet2/0), from 192.168.10.21, Send flag is 0x0
    Originating router is 192.8.8.8
    Administrator tag is 1684300801 (0x64646401)
D EX 192.168.10.25 (Ethernet1/0), from 192.168.10.25, Send flag is 0x0
    Originating router is 192.8.8.8
    Administrator tag is 1684300801 (0x64646401)
D EX 192.168.10.17 (Ethernet3/0), from 192.168.10.17, Send flag is 0x0
    Originating router is 192.8.8.8
    Administrator tag is 1684300801 (0x64646401)

R11#sh ip eig top 1.1.1.1/32 | in tag|router|Ethernet
192.168.10.21 (Ethernet2/0), from 192.168.10.21, Send flag is 0x0
    Originating router is 192.8.8.8

Administrator tag is 1684300801 (0x64646401)
Verification: After Implementation

R1#sh ip eig top 1.1.1.1/32 | in tag|router|Ethernet
192.168.10.21 (Ethernet2/0), from 192.168.10.21, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.100.1
192.168.10.25 (Ethernet1/0), from 192.168.10.25, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.100.1
192.168.10.17 (Ethernet3/0), from 192.168.10.17, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.100.1

R11(config-router-af)#
*Dec 20 03:41:34.071: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.25 (Ethernet1/0) is resync: intf route configuration changed
R11(config-router-af)#
*Dec 20 03:41:36.295: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.21 (Ethernet2/0) is resync: intf route configuration changed
R11(config-router-af)#
*Dec 20 03:41:38.959: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.17 (Ethernet3/0) is resync: intf route configuration changed

R11#sh ip route 1.1.1.1
% Network not in table

R11#sh ip eig top 1.1.1.1/32 | in tag|router|Ethernet
R11#

R11#sh ip route | in EX
D  EX 6.6.6.6 [170/857215] via 192.168.10.21, 00:02:28, Ethernet2/0
D  EX 7.7.7.7 [170/857215] via 192.168.10.21, 00:02:28, Ethernet2/0
D  EX 192.99.99.99
R11#

R11#sh ip eig top 6.6.6.6/32 | in tag|router|Ethernet
192.168.10.21 (Ethernet2/0), from 192.168.10.21, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.101.1
192.168.10.17 (Ethernet3/0), from 192.168.10.17, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.101.1
192.168.10.25 (Ethernet1/0), from 192.168.10.25, Send flag is 0x0
  Originating router is 192.8.8.8
  Administrator tag is 100.100.101.1
R11#sh ip route tag 100.100.100.1
R11#sh ip route tag 100.100.200.1
R11#sh ip route tag 100.100.101.1
Routing entry for 6.6.6.6/32
Known via "eigrp 150", distance 170, metric 857215
Tag 100.100.101.1, type external
Redistributing via eigrp 150
Last update from 192.168.10.21 on Ethernet2/0, 00:21:21 ago
Routing Descriptor Blocks:
  * 192.168.10.21, from 192.168.10.21, 00:21:21 ago, via Ethernet2/0
    Route metric is 857215, traffic share count is 1
    Total delay is 1002 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
    Route tag 100.100.101.1
Routing entry for 7.7.7.7/32
Known via "eigrp 150", distance 170, metric 857215
Tag 100.100.101.1, type external
Redistributing via eigrp 150
Last update from 192.168.10.21 on Ethernet2/0, 00:21:21 ago
Routing Descriptor Blocks:
  * 192.168.10.21, from 192.168.10.21, 00:21:21 ago, via Ethernet2/0
    Route metric is 857215, traffic share count is 1
    Total delay is 1002 microseconds, minimum bandwidth is 10000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
    Route tag 100.100.101.1
EIGRP Authentication

Note:
SHA-256 Authentication
Enhanced Interior Gateway Routing Protocol (EIGRP) authentication is configurable on a per-interface basis; this means that packets exchanged between neighbors connected through an interface are authenticated. EIGRP supports:

- **Message digest algorithm 5 (MD5) authentication** to prevent the introduction of unauthorized information from unapproved sources. MD5 authentication is defined in RFC 1321.
- **Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication method.** When you use the HMAC-SHA-256 authentication method, a shared secret key is configured on all devices attached to a common network. For each packet, the key is used to generate and verify a message digest that gets added to the packet. The message digest is a one-way function of the packet and the secret key.

If HMAC-SHA-256 authentication is configured in an EIGRP network, EIGRP packets will be authenticated using HMAC-SHA-256 message authentication codes. The HMAC algorithm takes as input the data to be authenticated (that is, the EIGRP packet) and a shared secret key that is known to both the sender and the receiver; the algorithm gives a 256-bit hash output that is used for authentication. If the hash value provided by the sender matches the hash value calculated by the receiver, the packet is accepted by the receiver; otherwise, the packet is discarded.

Typically, the shared secret key is configured to be identical between the sender and the receiver. To protect against packet replay attacks because of a spoofed source address, the shared secret key for a packet is defined as the concatenation of the user-configured shared secret (identical across all devices participating in the authenticated domain) with the IPv4 or IPv6 address (which is unique for each device) from which the packet is sent.

*directly from Cisco website*

---

Configure strongest authentication with a password of **EIGRP** between all devices.

Any additional connections to EIGRP AS150 on SW1 or SW2 should be encrypted using the same password without further configuration on any of these devices.

The authentication should protect from replay attack.

Do not configure a key chain for your solution.

**Configuration:**

**SW1**

```plaintext
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
  af-interface default
    authentication mode hmac-sha-256 EIGRP
  exit-af-interface
  topology base
  exit-af-topology
  exit-address-family
```

**SW2**

```plaintext
router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
  af-interface default
    authentication mode hmac-sha-256 EIGRP
  exit-af-interface
  topology base
  exit-af-topology
  exit-address-family
```
R8
router eigrp San_Francisco_HQ
address-family ipv4 unicast autonomous-system 150
af-interface Ethernet1/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
af-interface Ethernet2/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
af-interface Ethernet3/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
topology base
exit-af-topology
exit-address-family

R9
router eigrp San_Francisco_HQ
address-family ipv4 unicast autonomous-system 150
af-interface Ethernet1/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
af-interface Ethernet2/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
topology base
exit-af-topology
exit-address-family

R10
router eigrp San_Francisco_HQ
address-family ipv4 unicast autonomous-system 150
af-interface Ethernet1/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
af-interface Ethernet2/0
    authentication mode hmac-sha-256 EIGRP
exit-af-interface
topology base
exit-af-topology
exit-address-family
R11
router eigrp San_Francisco_HQ
address-family ipv4 unicast autonomous-system 150

af-interface Ethernet1/0
  authentication mode hmac-sha-256 EIGRP
  exit-af-interface

af-interface Ethernet2/0
  authentication mode hmac-sha-256 EIGRP
  exit-af-interface

af-interface Ethernet3/0
  authentication mode hmac-sha-256 EIGRP
  exit-af-interface

topology base
  exit-af-topology
  exit-address-family

Verification:

R8#sh ip eigrp interfaces detail | in mode|Lo|Et
Lo0 0 0/0 0/0 0 0/0 0 0
Authentication mode is not set
Et1/0 1 0/0 0/0 12 0/2 50 0
Authentication mode is HMAC-SHA-256, key-chain is not set
Et3/0 1 0/0 0/0 8 0/2 50 0
Authentication mode is HMAC-SHA-256, key-chain is not set
Et2/0 1 0/0 0/0 13 0/2 68 0
Authentication mode is HMAC-SHA-256, key-chain is not set
Lo1 0 0/0 0/0 0 0/0 0 0
Authentication mode is not set

SW1#sh ip eigrp interfaces detail | in mode|Lo|Et|Vl
Lo0 0 0/0 0/0 0 0/0 0 0
Authentication mode is HMAC-SHA-256, key-chain is not set
Vl118 1 0/0 0/0 13 0/0 50 0
Authentication mode is HMAC-SHA-256, key-chain is not set
Et0/0 1 0/0 0/0 21 0/2 88 0
Authentication mode is HMAC-SHA-256, key-chain is not set

Note: Other devices should produce similar output

Reference: EIGRP/SAF HMAC-SHA-256 Authentication
**EIGRP bfd**

R8 and R9 must be configured for path detection on their Ethernet segment using the following parameters:
- **Interval 60**
- **Min_rx 60**
- **Multiplier 8**

Do not enable BFD on any other interfaces

---

**Configuration:**

**R8**

```shell
interface Ethernet1/0
  bfd interval 60 min_rx 60 multiplier 8

router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
    af-interface Ethernet1/0
      bfd
    exit-af-interface
```

**R9**

```shell
interface Ethernet1/0
  bfd interval 60 min_rx 60 multiplier 8

router eigrp San_Francisco_HQ
  address-family ipv4 unicast autonomous-system 150
    af-interface Ethernet1/0
      bfd
    exit-af-interface
```

---

**Verification:**

```bash
R8#sh bfd neighbors
IPv4 Sessions
   NeighAddr    LD/RD  RH/RS  State  Int
192.168.10.2  1/1    Up     Up     Et1/0
```
R8#sh ip eigrp int detail et 1/0
EIGRP-IPv4 VR(San_Francisco_HQ) Address-Family Interfaces for AS(150)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Un/Reliable</th>
<th>SRTT</th>
<th>Un/Reliable</th>
<th>Flow Timer</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1</td>
<td>0/0</td>
<td>12</td>
<td>0/2</td>
<td>50</td>
<td>0</td>
</tr>
</tbody>
</table>

Hello-interval is 5, Hold-time is 15
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 21/0
Hello's sent/expedited: 645/3
Un/reliable mcasts: 0/22 Un/reliable ucasts: 26/6
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 1 Out-of-sequence rcvd: 3

Topo-ld is not set
Authentication mode is HMAC-SHA-256, key-chain is not set
BFD is enabled

R9#sh bfd ne details
IPv4 Sessions

<table>
<thead>
<tr>
<th>NeighAddr</th>
<th>LD/RD</th>
<th>RH/RS</th>
<th>State</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.1</td>
<td>1/1</td>
<td>Up</td>
<td>Up</td>
<td>Et1/0</td>
</tr>
</tbody>
</table>

Session state is UP and using echo function with 60 ms interval.

OurAddr: 192.168.10.2
Handle: 1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 8

Received MinRxInt: 1000000, Received Multiplier: 8

Holdown (hits): 0(0), Hello (hits): 1000(359)
Rx Count: 362, Rx Interval (ms) min/max/avg: 2/1871/881 last: 494 ms ago
Tx Count: 361, Tx Interval (ms) min/max/avg: 2/1137/883 last: 434 ms ago
Elapsed time watermarks: 0 0 (last: 0)

Registered protocols: EIGRP

Uptime: 00:05:18
Last packet: Version: 1

State bit: Up  Demand bit: 0
Poll bit: 0  Final bit: 0
C bit: 0  Multiplier: 8
My Discr.: 1  Your Discr.: 1
Min tx interval: 1000000  Min rx interval: 1000000

Min Echo interval: 60000
Berlin HQ Home User

EIGRP

Configure EIGRP AS 200
The Router-ID must be configured to the router's Loopback0 interface
Advertise Loopback0 of R21 into EIGRP
With a single command ensure that R21 will not accept prefixes if they're more than 25 hops away
Ensure R21 will not establish EIGRP adjacencies with any device
Use EIGRP 32bit version for your configuration

Configuration:

R21
  router eigrp 200
  metric maximum-hops 25
  network 192.21.21.21 0.0.0.0
  network 192.168.50.21 0.0.0.0
  passive-interface default
eigrp router-id 192.21.21.21

Verification:

R21#sh ip prot
Routing Protocol is "eigrp 200"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS (200)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
Router-ID: 192.21.21.21
  Topology: 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 25
    Maximum metric variance 1
  
Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  192.21.21.21/32
  192.168.50.21/32
Routing Information Sources:
  Gateway   Distance   Last Update
  Distance: internal 90 external 170
Berlin Remote Office

EIGRP

Configure EIGRP AS 200
The Router-ID must be configured to the router’s Loopback0 interface
Advertise Loopback0 of R14 into EIGRP
Ensure all interfaces are in a passive state
Wildcard mask should be relevant to the subnet mask
Do not use EIGRP 64bit version in your configuration

Configuration:

R14
router eigrp 200
network 192.14.14.14 0.0.0.0
network 192.168.60.12 0.0.0.3
network 192.168.60.16 0.0.0.7
passive-interface default

Verification:

R14#sh ip prot
Routing Protocol is "eigrp 200"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Default networks flagged in outgoing updates
    Default networks accepted from incoming updates
    EIGRP-IPv4 Protocol for AS(200)
        Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
        NSF-aware route hold timer is 240
        Topology: 0 (base)
            Active Timer: 3 min
            Distance: internal 90 external 170
            Maximum path: 4
            Maximum hopcount 100
            Maximum metric variance 1

    Automatic Summarization: disabled
    Maximum path: 4
    Routing for Networks:
        192.168.60.12/30
        192.168.60.16/29

    Routing Information Sources:
    Gateway     Distance     Last Update
    Distance: internal 90 external 170
Sydney Business Model HQ

EIGRP

Configure EIGRP AS 250
The Router-ID must be configured to the router’s Loopback0 interface
EIGRP must be enabled only on relevant interfaces – see main diagram
Advertise Loopback0 (including Loopback1 of R16) of all devices including DNS Server IP Address
VLAN78 must also be enabled for EIGRP
Use EIGRP Classic mode in your configuration

Configuration:

R16
router eigrp 250
  network 192.16.16.16 0.0.0.0
  network 192.166.166.166 0.0.0.0
  network 192.168.100.16 0.0.0.0
  network 192.168.110.16 0.0.0.0
  passive-interface default
  no passive-interface Ethernet1/0
  no passive-interface Ethernet2/0
eigrp router-id 192.16.16.16

R17
router eigrp 250
  network 192.17.17.17 0.0.0.0
  network 192.168.78.17 0.0.0.0
  network 192.168.100.17 0.0.0.0
  passive-interface default
  no passive-interface Ethernet1/0
  no passive-interface Dialer1
eigrp router-id 192.17.17.17

R18
router eigrp 250
  network 192.18.18.18 0.0.0.0
  network 192.168.78.18 0.0.0.0
  network 192.168.110.18 0.0.0.0
  passive-interface default
  no passive-interface Ethernet1/0
  no passive-interface Virtual-Template1
eigrp router-id 192.18.18.18

SW6
router eigrp 250
  network 192.106.106.106 0.0.0.0
  network 192.168.100.106 0.0.0.0
  network 192.168.120.106 0.0.0.0
  passive-interface default
  no passive-interface Vlan567
eigrp router-id 192.106.106.106
**SW7**

```plaintext
router eigrp 250
network 192.107.107.107 0.0.0.0
network 192.168.110.107 0.0.0.0
network 192.168.130.107 0.0.0.0
network 192.168.140.107 0.0.0.0
passive-interface default
no passive-interface Vlan668
eigrp router-id 192.107.107.107
```

**Verification:**

```
R16#sh ip eigrp
EIGRP-IPv4 Neighbors for AS(250)

<table>
<thead>
<tr>
<th>#</th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime (sec)</th>
<th>SRTT (ms)</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>192.168.110.107</td>
<td>Et2/0</td>
<td>10 00:01:36</td>
<td>1</td>
<td>100</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>192.168.100.106</td>
<td>Et1/0</td>
<td>10 00:02:06</td>
<td>2</td>
<td>100</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>192.168.110.18</td>
<td>Et2/0</td>
<td>13 00:04:46</td>
<td>4</td>
<td>100</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>0</td>
<td>192.168.100.17</td>
<td>Et1/0</td>
<td>14 00:05:57</td>
<td>9</td>
<td>100</td>
<td>0</td>
<td>9</td>
</tr>
</tbody>
</table>

**Note:** Other devices within Sydney Business Model HQ should produce similar output.
DHCP

R17 must be configured to provide the following parameters for DHCP client Server#4
Assign IP Address based on the Client ID of Ethernet0/0
Use a name of your choice of DHCP pool
Domain name for the clients should be data.co.uk
IP address of DNS servers available for the clients should be R16’s Loopback0
Server#4 should always obtain .100 in the last octet of IPv4 address
Clients should not need to renew their IP addresses
Ensure IP Address conflicts are logged

Configuration:

R17

```
service dhcp

ip dhcp conflict logging

ip dhcp pool SERVER4
  host 192.168.140.100 255.255.255.0
  client-identifier 01aa.bbcc.ddaa.bb
  default-router 192.168.140.107
  domain-name data.co.uk
  dns-server 192.16.16.16
  lease infinite
```

SW7

```
interface Vlan50
  ip helper-address 192.17.17.17
```

SERVER#4

```
interface Ethernet0/0
  ip address dhcp client-id Ethernet0/0
```

Verification:

R17#debug ip dh server pac detail
DHCP server packet detail debugging is on.
R17#
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPDISCOVER received from client 01aa.bbcc.ddaa.bb through relay 192.168.140.107.
DHCPD: Sending DHCPOFFER to client 01aa.bbcc.ddaa.bb (192.168.140.100).DHCPD: Setting only requested parameters
DHCPD: no option 125
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: DHCPREQUEST received from client 01aa.bbcc.ddaa.bb.
DHCPD: Appending default domain from pool
DHCPD: Using hostname 'SERVER4.data.co.uk.' for dynamic update (from hostname option)
DHCPD: Sending DHCPACK to client 01aa.bbcc.ddaa.bb (192.168.140.100).DHCPD: Setting only requested parameters
DHCPD: no option 125
R17#un all
All possible debugging has been turned off
Note: Server 4 was assigned 192.168.140.100 and we are also able to reach it all the way from R17 Lo:0

SERVER4(config-if)#
*Dec 20 11:21:29.221: %DHCP-6-ADDRESS.Assign: Interface Ethernet0/0 assigned DHCP address 192.168.140.100, mask 255.255.255.0, Hostname SERVER4

R17#ping 192.168.140.100 so loo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
Packet sent with a source address of 192.17.17.17
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Note: Last thing is we will check DHCP pool and bindings on R17

R17#sh ip dhcp pool
Pool SERVER4 :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 1
  Leased addresses : 1
  Pending event : none
  0 subnet is currently in the pool :
  Current index IP address range Leased addresses
  192.168.140.100 192.168.140.100 - 192.168.140.100 1

R17#sh ip dh bin
Bindings from all pools not associated with VRF:
  IP address Client-ID/ Hardware address/ User name Lease expiration Type
  192.168.140.100 01aa.bbc.cc dd aa bb Infinite Manual

Note: and ensure the SW7 is forwarding DHCP request based on its helper address configuration

SW7#sh ip int vl 50 | in add
  Internet address is 192.168.140.107/24
  Broadcast address is 255.255.255.255
  Helper address is 192.168.140.100
  Network address translation is disabled
Sydney Business Remote Office (1)

EIGRP

Configure EIGRP AS 250
The Router-ID must be configured to the router's Loopback0 interface
EIGRP must be enabled only on relevant interfaces – see diagram
Advertise Loopback1 – 9 (Internal User Subnets) on R19 into EIGRP using a single statement
Do not forget to also advertise Loopback0 into EIGRP
Use EIGRP 32bit version in your configuration

Configuration:

R19
   router eigrp 250
   network 192.19.19.19 0.0.0.0
   network 192.168.128.0 0.0.31.255
   network 192.168.150.0 0.0.0.255
   passive-interface default
   eigrp router-id 192.19.19.19

Verification:

R19#sh ip prot
Routing Protocol is "eigrp 250"
   Outgoing update filter list for all interfaces is not set
   Incoming update filter list for all interfaces is not set
   Default networks flagged in outgoing updates
   Default networks accepted from incoming updates
   EIGRP-IPv4 Protocol for AS(250)
      Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
      NSF-aware route hold timer is 240
   Router-ID: 192.19.19.19
      Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1
      Automatic Summarization: disabled
      Maximum path: 4
      Routing for Networks:
         192.19.19.19/32
         192.168.150.0
         192.168.128.0/19
      Routing Information Sources:
         Gateway        Distance        Last Update
         Distance: internal 90 external 170
Sydney Business Remote Office(2)

EIGRP

Configure EIGRP AS 250
The Router-ID must be configured to the router’s Loopback0 interface
EIGRP must be enabled only on relevant interfaces – see diagram
Do not forget to include Netflow Collector Loopback0 IP Address of R20

Later in the lab Loopback 1 – 15 (Internal User Subnets) on R20 must be seen by R17 and R18 as an external routes
Do not use prefix list
Use a single permit statement for your solution

Configuration:

R20

router eigrp 250
  network 192.20.20.20 0.0.0.0
  network 192.168.160.20 0.0.0.0
  redistribute connected route-map CONNECTED
  passive-interface default
  eigrp router-id 192.20.20.20

  access-list 1 permit 192.168.128.0 0.0.63.255
  route-map CONNECTED permit 10
  match ip address 1

Verification:

Note: Looks like we need to perform redistribution on R20 to meet the R17 and R18 requirement (see question)

R20#sh ip prot
Routing Protocol is "eigrp 250"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates

Redistributing: connected

EIGRP-IPv4 Protocol for AS(250)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240

Router-ID: 192.20.20.20
Topology : 0 (base)
  Active Timer: 3 min
  Distance: internal 90 external 170
  Maximum path: 4
  Maximum hopcount 100
  Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:

  192.20.20.20/32
  192.168.160.20/32

Routing Information Sources:

  Gateway Distance Last Update
  Distance: internal 90 external 170
R20#sh ip eigrp top
EIGRP-IPv4 Topology Table for AS(250)/ID(192.20.20.20)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, 
r - reply Status, s - sia Status
P 192.168.171.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.170.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.173.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.20.20.20/32, 1 successors, FD is 128256
  via Connected, Loopback0
P 192.168.166.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.160.0/24, 1 successors, FD is 281600
  via Connected, Ethernet0/0
P 192.168.161.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.172.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.168.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.164.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.165.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.167.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.163.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.175.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.169.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.162.0/24, 1 successors, FD is 128256
  via Connected (128256/0)
P 192.168.174.0/24, 1 successors, FD is 128256
  via Connected (128256/0)

**Note:** And we have used a single ACL entry to match all prefixes

R20#sh access-lists 1
Standard IP access list 1
  10 permit 192.168.128.0, wildcard bits 0.0.63.255 (45 matches)
Why does R3 prefer the path through R1 to reach host 10.1.1.1?

The default formula to calculate OSPF bandwidth is $BW = \frac{\text{Bandwidth Reference}}{\text{interface bandwidth [bps]}} = 10^8 / \text{interface bandwidth [bps]}$

BW of the R1-R3 link = $10^8 / 100\text{Mbps} = 10^8 / 10^8 = 1$
BW of the R2-R3 link = $10^8 / 1\text{Gbps} = 10^8 / 10^9 = 1$ (round up)

Therefore OSPF considers the two above links have the same Bandwidth -> R3 will go to 10.1.1.1 via the R1-R3 link. The solution here is to increase the Bandwidth Reference to a higher value using the "auto-cost reference-bandwidth" command under OSPF router mode.

Router(config)#router ospf 1
Router(config-router)#auto-cost reference-bandwidth 10000

This will increase the reference bandwidth to 10000 Mbps which increases the BW of the R2-R3 link to $10^8 \times 10^2 / 10^8 = 100$.

*directly from Cisco website*
Service Provider#9

OSPF

Use an OSPF process ID of 65000 for all OSPF devices
OSPF Router IDs must be stable and must be configured using IP address of routers Loopback0 interfaces
The Loopback0 interfaces must belong to **OSPF AREA 0** and they should not be seen as host routes
Do not use the "network" statement anywhere in your configuration
Refer to the Main Topology Diagram

The Loopback1 (Solarwinds Server) and Loopback2 (Test Network) interfaces of R6 must belong to **OSPF AREA 1**

Interface Loopback10 should be the **ONLY** prefix on R5 which metric increases as it traverses throughout the network
Do not use an ACL or prefix list to accomplish this

---

**Configuration:**

```
R1
router ospf 65000
  router-id 172.100.1.1

interface Loopback0
  ip ospf network point-to-point
  ip ospf 65000 area 0

interface Ethernet0/0
  ip ospf 65000 area 0

interface Ethernet1/0.14
  ip ospf 65000 area 0

interface Ethernet1/0.15
  ip ospf 65000 area 0

interface Ethernet1/0.17
  ip ospf 65000 area 0

interface Ethernet2/0
  ip ospf 65000 area 0

interface Ethernet3/0
  ip ospf 65000 area 0
```
R2
router ospf 65000
   router-id 172.100.2.2

interface Loopback0
   ip ospf network point-to-point
   ip ospf 65000 area 0

interface Loopback2
   ip ospf 65000 area 0

interface Ethernet1/0.12
   ip ospf 65000 area 0

interface Ethernet1/0.23
   ip ospf 65000 area 0

interface Ethernet1/0.24
   ip ospf 65000 area 0

R3
router ospf 65000
   router-id 172.100.3.3

interface Loopback0
   ip ospf network point-to-point
   ip ospf 65000 area 0

interface Loopback1
   ip ospf 65000 area 0

interface Loopback2
   ip ospf 65000 area 0

interface Ethernet0/0.35
   ip ospf 65000 area 0

interface Ethernet1/0
   ip ospf 65000 area 0

interface Ethernet2/0
   ip ospf 65000 area 0

R4
router ospf 65000
   router-id 172.100.4.4

interface Loopback0
   ip ospf network point-to-point
   ip ospf 65000 area 0

interface Ethernet0/0.24
   ip ospf 65000 area 0

interface Ethernet0/0.46
   ip ospf 65000 area 0

interface Ethernet1/0
   ip ospf 65000 area 0
R5
route-map CONNECTED permit 10
match interface Loopback10
set metric-type type-1

router ospf 65000
router-id 172.100.5.5
redistribute connected subnets route-map CONNECTED

interface Loopback0
ip ospf network point-to-point
ip ospf 65000 area 0

interface Ethernet0/0.15
ip ospf 65000 area 0

interface Ethernet0/0.57
ip ospf 65000 area 0

interface Ethernet1/0
ip ospf 65000 area 0

R6
router ospf 65000
router-id 172.100.6.6

interface Loopback0
ip ospf network point-to-point
ip ospf 65000 area 0

interface Loopback1
ip ospf 65000 area 1

interface Loopback2
ip ospf 65000 area 1

interface Ethernet0/0.46
ip ospf 65000 area 0

interface Ethernet1/0
ip ospf 65000 area 0

interface Ethernet2/0
ip ospf 65000 area 0

R7
router ospf 65000
router-id 172.100.7.7

interface Loopback0
ip ospf network point-to-point
ip ospf 65000 area 0

interface Loopback2
ip ospf 65000 area 0

interface Ethernet1/0.17
ip ospf 65000 area 0

interface Ethernet1/0.67
ip ospf 65000 area 0

interface Ethernet2/0
ip ospf 65000 area 0
Verification:

R1#sh ip osp ne

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.4.4</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:38</td>
<td>172.31.10.29</td>
<td>Ethernet1/0.14</td>
</tr>
<tr>
<td>172.100.5.5</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:37</td>
<td>172.31.10.42</td>
<td>Ethernet1/0.15</td>
</tr>
<tr>
<td>172.100.7.7</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:38</td>
<td>172.31.10.34</td>
<td>Ethernet1/0.17</td>
</tr>
<tr>
<td>172.100.2.2</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:37</td>
<td>172.31.10.13</td>
<td>Ethernet2/0</td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:37</td>
<td>172.31.10.9</td>
<td>Ethernet3/0</td>
</tr>
<tr>
<td>172.100.6.6</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:38</td>
<td>172.31.10.26</td>
<td>Ethernet0/0</td>
</tr>
</tbody>
</table>

Note: We will check R1 border routers to ensure we meet question requirement for both R5 and R6 Loopbacks

R1#sh ip osp border-routers

OSPF Router with ID (172.100.1.1) (Process ID 65000)

Base Topology (MTID 0)

Internal Router Routing Table

Codes: i - Inter-area route, I - Intra-area route

i 172.100.5.5 [10] via 172.31.10.42, Ethernet1/0.15, ASBR, Area 0, SPF 11
i 172.100.6.6 [10] via 172.31.10.26, Ethernet0/0, ABR, Area 0, SPF 11

Note: and R1 routing table

R1#sh ip route osp | be Gate

Gateway of last resort is not set

172.31.0.0/16 is variably subnetted, 20 subnets, 3 masks

O  172.31.10.0/30 [110/20] via 172.31.10.13, 00:01:05, Ethernet2/0
    [110/20] via 172.31.10.9, 00:01:05, Ethernet3/0
O  172.31.10.4/30 [110/20] via 172.31.10.42, 00:01:05, Ethernet1/0.15
    [110/20] via 172.31.10.9, 00:01:05, Ethernet3/0
O  172.31.10.16/30 [110/20] via 172.31.10.29, 00:01:05, Ethernet1/0.14
    [110/20] via 172.31.10.13, 00:01:05, Ethernet2/0
O  172.31.10.20/30 [110/20] via 172.31.10.29, 00:01:05, Ethernet1/0.14
    [110/20] via 172.31.10.13, 00:01:05, Ethernet2/0
O  172.31.10.36/30 [110/20] via 172.31.10.42, 00:01:05, Ethernet1/0.15
    [110/20] via 172.31.10.34, 00:01:05, Ethernet1/0.17
O  172.31.10.44/30 [110/20] via 172.31.10.34, 00:01:05, Ethernet1/0.17
    [110/20] via 172.31.10.26, 00:01:05, Ethernet0/0

172.31.0.0/16 is subnetted, 14 subnets

O  172.100.2.2 [110/11] via 172.31.10.13, 00:01:05, Ethernet2/0
O  172.100.3.3 [110/11] via 172.31.10.9, 00:01:05, Ethernet3/0
O  172.100.4.4 [110/11] via 172.31.10.29, 00:01:05, Ethernet1/0.14
O  172.100.5.5 [110/11] via 172.31.10.42, 00:01:05, Ethernet1/0.15
O  172.100.6.6 [110/11] via 172.31.10.26, 00:01:05, Ethernet0/0
O  172.100.7.7 [110/11] via 172.31.10.34, 00:01:05, Ethernet1/0.17
O  172.100.122.122 [110/11] via 172.31.10.13, 00:01:05, Ethernet2/0
O  172.100.133.133 [110/11] via 172.31.10.9, 00:01:05, Ethernet3/0
O  172.100.166.166 [110/11] via 172.31.10.26, 00:01:05, Ethernet0/0

172.100.177.177 [110/11] via 172.31.10.34, 00:01:05, Ethernet1/0.17
**Note:** We are looking good. Lo:0 of R5 metric varies from R5 Lo:10

R1#sh ip route 172.100.5.5
Routing entry for 172.100.5.5/32
Known via "ospf 65000", distance 110, **metric 11, type intra area**
Last update from 172.31.10.42 on Ethernet1/0.15, 00:03:52 ago
Routing Descriptor Blocks:
  * 172.31.10.42, from 172.100.5.5, 00:03:52 ago, via Ethernet1/0.15
    Route metric is 11, traffic share count is 1

R1#sh ip route 172.100.55.55
Routing entry for 172.100.55.55/32
Known via "ospf 65000", distance 110, **metric 30, type extern 1**
Last update from 172.31.10.42 on Ethernet1/0.15, 00:02:48 ago
Routing Descriptor Blocks:
  * 172.31.10.42, from 172.100.5.5, 00:02:48 ago, via Ethernet1/0.15
    Route metric is 30, traffic share count is 1

**Note:** Perform final OSPF checks on all devices start from R1

R1#sh ip prot
Routing Protocol is "ospf 65000"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
**Router ID 172.100.1.1**
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:

Routing on Interfaces Configured Explicitly (Area 0):
  Loopback0
  Ethernet1/0.14
  Ethernet1/0.15
  Ethernet1/0.17
  Ethernet2/0
  Ethernet3/0
  Ethernet0/0
Routing Information Sources:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.7.7</td>
<td>110</td>
<td>00:01:49</td>
</tr>
<tr>
<td>172.100.6.6</td>
<td>110</td>
<td>00:01:44</td>
</tr>
<tr>
<td>172.100.5.5</td>
<td>110</td>
<td>00:01:44</td>
</tr>
<tr>
<td>172.100.4.4</td>
<td>110</td>
<td>00:01:44</td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>110</td>
<td>00:01:44</td>
</tr>
<tr>
<td>172.100.2.2</td>
<td>110</td>
<td>00:01:44</td>
</tr>
</tbody>
</table>

Distance: (default is 110)
**Note:** and R6 which should be ABR

R6#sh ip prot
Routing Protocol is "ospf 65000"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.100.6.6
It is an area border router
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
  Loopback0
  Ethernet0/0.46
  Ethernet1/0
  Ethernet2/0
Routing on Interfaces Configured Explicitly (Area 1):
  Loopback2
  Loopback1
Routing Information Sources:
<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.7.7</td>
<td>110</td>
<td>00:01:27</td>
</tr>
<tr>
<td>172.100.1.1</td>
<td>110</td>
<td>00:01:12</td>
</tr>
<tr>
<td>172.100.4.4</td>
<td>110</td>
<td>00:01:38</td>
</tr>
<tr>
<td>172.100.5.5</td>
<td>110</td>
<td>00:01:27</td>
</tr>
<tr>
<td>172.100.2.2</td>
<td>110</td>
<td>00:01:38</td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>110</td>
<td>00:02:46</td>
</tr>
</tbody>
</table>
Distance: (default is 110)

**Note:** and R5 that should perform ASBR function

R5#sh ip prot
Routing Protocol is "ospf 65000"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.100.5.5
It is an autonomous system boundary router
Redistributing External Routes from connected, includes subnets in redistribution
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
  Loopback0
  Ethernet0/0.15
  Ethernet0/0.57
  Ethernet1/0
Routing Information Sources:
<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.7.7</td>
<td>110</td>
<td>00:07:28</td>
</tr>
<tr>
<td>172.100.6.6</td>
<td>110</td>
<td>00:07:28</td>
</tr>
<tr>
<td>172.100.1.1</td>
<td>110</td>
<td>00:07:13</td>
</tr>
<tr>
<td>172.100.4.4</td>
<td>110</td>
<td>00:08:51</td>
</tr>
<tr>
<td>172.100.2.2</td>
<td>110</td>
<td>00:07:51</td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>110</td>
<td>00:07:51</td>
</tr>
</tbody>
</table>
Distance: (default is 110)

**Note:** You should be able to produce similar output on other devices within the Service Provider#9 infrastructure
OSPF

Ensure that R1 is elected as the Designated Router for all its OSPF connections and that it maintains the best chance of being re-elected as such in the event of the network failure. All other routers should always remain in the DROTHER state towards R1.

Ensure that R1 does not advertise the preconfigured secondary address under interface Ethernet3/0 of 172.31.100.100/24 into OSPF network. Do not use any filtering techniques to achieve this.

Configuration:

R1
interface Ethernet0/0
  ip ospf priority 255

interface Ethernet1/0.14
  ip ospf priority 255

interface Ethernet1/0.15
  ip ospf priority 255

interface Ethernet1/0.17
  ip ospf priority 255

interface Ethernet2/0
  ip ospf priority 255

interface Ethernet3/0
  ip ospf priority 255
  ip ospf 65000 area 0 secondaries none

R2
interface Ethernet1/0.12
  ip ospf priority 0

interface Ethernet1/0.23
  ip ospf priority 0

interface Ethernet1/0.24
  ip ospf priority 0

R3
interface Ethernet0/0.35
  ip ospf priority 0

interface Ethernet1/0
  ip ospf priority 0

interface Ethernet2/0
  ip ospf priority 0

R4
interface Ethernet0/0.24
  ip ospf priority 0

interface Ethernet0/0.46
  ip ospf priority 0

interface Ethernet1/0
  ip ospf priority 0
R5
interface Ethernet0/0.15
   ip ospf priority 0
interface Ethernet0/0.57
   ip ospf priority 0
interface Ethernet1/0
   ip ospf priority 0

R6
interface Ethernet0/0.46
   ip ospf priority 0
interface Ethernet1/0
   ip ospf priority 0
interface Ethernet2/0
   ip ospf priority 0

R7
interface Ethernet1/0.17
   ip ospf priority 0
interface Ethernet1/0.67
   ip ospf priority 0
interface Ethernet2/0
   ip ospf priority 0

**Verification: Before Implementation**

```
R1#sh ip ospf interface 3/0
Ethernet3/0 is up, line protocol is up
Internet Address 172.31.10.10/30, Area 0, Attached via Interface Enable
Process ID 65000, Router ID 172.100.1.1, Network Type BROADCAST, Cost: 10
Topology-MTID Cost Disabled Shutdown Topology Name
0 10 no no Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.100.3.3, Interface address 172.31.10.9
<Output omitted>
```

**Verification: After Implementation**

```
R1#sh ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
172.100.4.4 0 FULL/DROTHER 00:00:39 172.31.10.29 Ethernet1/0.14
172.100.5.5 0 FULL/DROTHER 00:00:39 172.31.10.42 Ethernet1/0.15
172.100.7.7 0 FULL/DROTHER 00:00:39 172.31.10.34 Ethernet1/0.17
172.100.2.2 0 FULL/DROTHER 00:00:39 172.31.10.13 Ethernet2/0
172.100.3.3 0 FULL/DROTHER 00:00:39 172.31.10.9  Ethernet3/0
172.100.6.6 0 FULL/DROTHER 00:00:39 172.31.10.26 Ethernet0/0
```
**Note:** *R1 is now DR for the topology*

```
R7#sh ip os ne
Neighbor ID     Pri   State      Dead Time   Address       Interface
172.100.5.5       0   2WAY/DROTHER    00:00:37    172.31.10.37    Ethernet2/0
172.100.6.6       0   2WAY/DROTHER    00:00:35    172.31.10.45    Ethernet1/0.67
172.100.1.1     255   FULL/DR      00:00:34    172.31.10.33    Ethernet1/0.17
```

**Note:** and it is only advertising it primary IP Address of its Ethernet3/0 interface and the secondary IP Address is excluded. Let’s move on to the next question.

```
R1#sh ip prot
Routing Protocol is: "ospf 65000"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.100.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
Routing on Interfaces Configured Explicitly (Area 0):
  Loopback0
  Ethernet1/0.14
  Ethernet1/0.15
  Ethernet1/0.17
  Ethernet2/0
  **Ethernet3/0 (primary address only)**
Routing Information Sources:
  Gateway         Distance      Last Update
  172.100.7.7          110      00:06:43
  172.100.6.6          110      00:06:38
  172.100.5.5          110      00:06:38
  172.100.4.4          110      00:06:38
  172.100.3.3          110      00:06:38
  172.100.2.2          110      00:06:38
Distance: (default is 110)
```

```
R1#sh ip os int et 3/0
Ethernet3/0 is up, line protocol is up
  Internet Address 172.31.10.10/30, Area 0, Attached via Interface Enable
  Process ID 65000, Router ID 172.100.1.1, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost  Disabled  Shutdown  Topology Name
  0                10    no        no        Base
  **Enabled by interface config, excluding secondary ip addresses**
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 172.100.1.1, Interface address 172.31.10.10
<Output omitted>
```
**OSPF Local Policy Routing**

Ensure that R7 Loopback 2 always chooses R5 to route ICMP traffic towards R2 Loopback 2. Ensure all other packets are not affected by any of the policies.

**Configuration:**

```plaintext
R7
access-list 100 permit icmp host 172.100.177.177 host 172.100.122.122
route-map ROUTE_PREF permit 10
match ip address 100
set ip next-hop 172.31.10.37
route-map ROUTE_PREF permit 20
ip local policy route-map ROUTE_PREF
```

**Verification:**

R7(config)#no service timestamps debug
R7(config)#exit
R7#debug ip policy
Policy routing debugging is on.

*Note: ICMP Ping test shows “policy match” for R2 and R7 Loo:2 interfaces*

R7#ping 172.100.122.122 source loo 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.122.122, timeout is 2 seconds:
Packet sent with a source address of 172.100.177.177
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/8 ms

**IP:** s=172.100.177.177 (local), d=172.100.122.122, len 100, policy match
**IP:** route map ROUTE_PREF, item 10, permit
**IP:** s=172.100.177.177 (local), d=172.100.122.122 (Ethernet2/0), len 100, policy routed
**IP:** local to Ethernet2/0 172.31.10.37

*Note: and “policy rejected” when the traffic is source from any other IP Address but Loo:2 of R7*

R7#ping 172.100.122.122 source loo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.122.122, timeout is 2 seconds:
Packet sent with a source address of 172.100.7.7
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms

**IP:** s=172.100.7.7 (local), d=172.100.122.122, len 100, policy match
**IP:** route map ROUTE_PREF, item 20, permit
**IP:** s=172.100.7.7 (local), d=172.100.122.122, len 100, policy rejected -- normal forwarding
**IP:** s=172.100.7.7 (local), d=172.100.122.122, len 100, policy match
**IP:** route map ROUTE_PREF, item 20, permit

R7#un all
All possible debugging has been turned off
OSPF Policy Routing

Ensure that R6 Loopback 2 always chooses R4 to route TELNET traffic towards R3 Loopback 2
Ensure all other packets are not affected by any of the policies
Configure R3 to allow TELNET connectivity for testing
Do not configure R6 for this task

Configuration:

R1

access-list 100 permit tcp host 172.100.166.166 host 172.100.133.133 eq telnet
route-map ROUTE-PREF permit 10
match ip address 100
set ip next-hop 172.31.10.29
route-map ROUTE-PREF permit 20
interface Ethernet0/0
ip policy route-map ROUTE-PREF

R3

line vty 0 4
transport input telnet

Verification:

R1#debug ip policy
Policy routing debugging is on

Note: Similar to the previous question but we will use Telnet for testing instead of ICMP ping

R6#telnet 172.100.133.133 /source-interface lo0 2
Trying 172.100.133.133 ... Open
Password required, but none set
[Connection to 172.100.133.133 closed by foreign host]

R1#
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, len 44, FIB policy match
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, len 44, PBR Counted
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, g=172.31.10.29, len 44, FIB policy routed
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, len 40, FIB policy match
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, len 40, PBR Counted
IP: s=172.100.166.166 (Ethernet0/0), d=172.100.133.133, g=172.31.10.29, len 40, FIB policy routed

R6#telnet 172.100.133.133
Trying 172.100.133.133 ... Open
Password required, but none set
[Connection to 172.100.133.133 closed by foreign host]

R1#
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 52, FIB policy match
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 52, PBR Counted
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 52, FIB policy rejected - normal forwarding
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 40, FIB policy match
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 40, PBR Counted
IP: s=172.31.10.26 (Ethernet0/0), d=172.100.133.133, len 40, FIB policy rejected - normal forwarding
**OSPF LSA**

R3 should generate a warning message and not accept any more nonself-generated LSAs once the maximum of 14,000 has been exceeded.

**Configuration:**

```
R3
  router ospf 65000
    max-lsa 14000 warning-only
```

**Verification:**

```
R3#sh ip os 65000
<Output omitted>
  Maximum number of non self-generated LSA allowed 14000 (warning-only)
  Current number of non self-generated LSA 15
  Threshold for warning message 75%
  Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  Router is not originating router-LSAs with maximum metric
<Output omitted>
```

**Note:** You should see below syslog message once the LSA limit has been reached

```
R3(config)#
*Dec 20 12:54:30.637: %OSPF-4-OSPF_MAX_LSA_THR: Threshold for maximum number of non self-generated LSA has been reached "ospf 65000" - 0 LSAs
*Dec 20 12:54:30.637: %OSPF-4-OSPF_MAX_LSA: Maximum number of non self-generated LSA has been exceeded "ospf 65000" - 15 LSAs
```
OSPF Authentication

Configure OSPF authentication across your OSPF domain. OSPF packets should be authenticated using a bit message authentication codes as specified in the output.

Use a key chain for your solution and name it as specified in the output with a password of OSPF_SHA.

Configuration:

R1
key chain OSPF_CRYPTO
  key 1
    key-string OSPF_SHA
    cryptographic-algorithm hmac-sha-256

interface Ethernet0/0
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0.14
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0.15
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0.17
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet2/0
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet3/0
  ip ospf authentication key-chain OSPF_CRYPTO

R2
key chain OSPF_CRYPTO
  key 1
    key-string OSPF_SHA
    cryptographic-algorithm hmac-sha-256

interface Ethernet1/0.23
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0.12
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0.24
  ip ospf authentication key-chain OSPF_CRYPTO

R3
key chain OSPF_CRYPTO
  key 1
    key-string OSPF_SHA
    cryptographic-algorithm hmac-sha-256

interface Ethernet0/0.35
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet1/0
  ip ospf authentication key-chain OSPF_CRYPTO

interface Ethernet2/0
  ip ospf authentication key-chain OSPF_CRYPTO
R4
key chain OSPF_CRYPTO
key 1
  key-string OSPF_SHA
  cryptographic-algorithm hmac-sha-256
interface Ethernet0/0.24
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet0/0.46
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet1/0
  ip ospf authentication key-chain OSPF_CRYPTO

R5
key chain OSPF_CRYPTO
key 1
  key-string OSPF_SHA
  cryptographic-algorithm hmac-sha-256
interface Ethernet0/0.15
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet0/0.57
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet1/0
  ip ospf authentication key-chain OSPF_CRYPTO

R6
key chain OSPF_CRYPTO
key 1
  key-string OSPF_SHA
  cryptographic-algorithm hmac-sha-256
interface Ethernet0/0.46
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet1/0
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet2/0
  ip ospf authentication key-chain OSPF_CRYPTO

R7
key chain OSPF_CRYPTO
key 1
  key-string OSPF_SHA
  cryptographic-algorithm hmac-sha-256
interface Ethernet1/0.17
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet1/0.67
  ip ospf authentication key-chain OSPF_CRYPTO
interface Ethernet2/0
  ip ospf authentication key-chain OSPF_CRYPTO
Verification:

```
R1#sh ip os int | in Crypto|Algor|Ethernet
Ethernet1/0.14 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
Ethernet1/0.15 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
Ethernet1/0.17 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
Ethernet2/0 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
Ethernet3/0 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
Ethernet0/0 is up, line protocol is up
  Cryptographic authentication enabled
    Sending SA: Key 1, Algorithm HMAC-SHA-256 - key chain OSPF_CRYPTO
```

Note: Other devices should produce similar output
OSPF MPLS

Enable label switching on all routers within OSPF domain using Loopback0 interface for MPLS router ID. All devices except for R1, R4, and R5 must use LDP, ensuring that TDP can be used on unused interfaces without specifically configuring these interfaces for TDP. Do not use interface level command to enable MPLS on R1, R4, or R5. Ensure that the LDP sessions are ‘always’ sourced from the Loopback0 interface on all devices.

Configuration:

R1
mpls ldp router-id Loopback0 force
router ospf 65000
mpls ldp autoconfig area 0

R2
mpls ldp router-id Loopback0 force
mpls label protocol tdp
interface Ethernet1/0.12
mpls label protocol ldp
mpls ip
interface Ethernet1/0.23
mpls label protocol ldp
mpls ip
interface Ethernet1/0.24
mpls label protocol ldp
mpls ip

R3
mpls ldp router-id Loopback0 force
mpls label protocol tdp
interface Ethernet0/0.35
mpls label protocol ldp
mpls ip
interface Ethernet1/0
mpls label protocol ldp
mpls ip
interface Ethernet2/0
mpls label protocol ldp
mpls ip

R4
mpls ldp router-id Loopback0 force
router ospf 65000
mpls ldp autoconfig area 0

R5
mpls ldp router-id Loopback0 force
router ospf 65000
mpls ldp autoconfig area 0
R6
mpls ldp router-id Loopback0 force
mpls label protocol tdp
interface Ethernet0/0.46
mpls label protocol ldp
mips ip
interface Ethernet1/0
mpls label protocol ldp
mips ip
interface Ethernet2/0
mpls label protocol ldp
mips ip

R7
mpls ldp router-id Loopback0 force
mpls label protocol tdp
interface Ethernet1/0.17
mpls label protocol ldp
mips ip
interface Ethernet1/0.67
mpls label protocol ldp
mips ip
interface Ethernet2/0
mpls label protocol ldp
mips ip

Verification:

Note: Let’s chose R1 and check for MPLS neigbours?

R1#sh mpl ld ne | in Pee
Peer LDP Ident: 172.100.2.2:0; Local LDP Ident 172.100.1.1:0
Peer LDP Ident: 172.100.3.3:0; Local LDP Ident 172.100.1.1:0
Peer LDP Ident: 172.100.4.4:0; Local LDP Ident 172.100.1.1:0
Peer LDP Ident: 172.100.5.5:0; Local LDP Ident 172.100.1.1:0
Peer LDP Ident: 172.100.6.6:0; Local LDP Ident 172.100.1.1:0

Note: and MPLS enabled interfaces

R1#sh mpls int
Interface              IP            Tunnel   BGP Static Operational
Ethernet0/0            Yes (ldp)     No       No  No  No     Yes
Ethernet2/0            Yes (ldp)     No       No  No  No     Yes
Ethernet3/0            Yes (ldp)     No       No  No  No     Yes
Ethernet1/0.14         Yes (ldp)     No       No  No  No     Yes
Ethernet1/0.15         Yes (ldp)     No       No  No  No     Yes
Ethernet1/0.17         Yes (ldp)     No       No  No  No     Yes
**Note:** The question states "no interface level command" so below output is what we expect

```
R1#sh ip ospf mpls ldp interface
Loopback0
  Process ID 65000, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet1/0.14
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet1/0.15
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet1/0.17
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet2/0
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet3/0
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
Ethernet0/0
  Process ID 65000, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization : Not required
  Holdown timer is disabled
  Interface is up
```

```
R1#sh mpls ldp discovery detail
  Local LDP Identifier: 172.100.1.1:0
  Discovery Sources:
      Interfaces:
      Ethernet0/0 (ldp): xmit/recv
      Enabled: IGP config;
      Hello interval: 5000 ms;  Transport IP addr: 172.100.1.1
      LDP Id: 172.100.6.6:0
      Src IP addr: 172.31.10.26;  Transport IP addr: 172.100.6.6
      Hold time: 15 sec; Proposed local/peer: 15/15 sec
      Reachable via 172.100.6.6/32
      Password: not required, none, in use
      Clients: IPv4, mLDP
```
Note: For local and outgoing labels let’s check label path for instance between R2 and R7 Loopbacks
R2 attaches label 30 for the destination of 172.100.7.7 and perform label swap 30 → 27 as it send the packet towards R1

R2#sh mpl forwarding-table 172.100.7.7 32 detail

<table>
<thead>
<tr>
<th>Local Label</th>
<th>Outgoing Label</th>
<th>Prefix</th>
<th>Bytes</th>
<th>Label</th>
<th>Outgoing</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>27</td>
<td>172.100.7.7/32</td>
<td>0</td>
<td>Et1/0.12</td>
<td>172.31.10.14</td>
<td></td>
</tr>
</tbody>
</table>

MAC/Encaps=18/22, MRU=1500, Label Stack(27)
AABBCC000102AABBCC0002018100000C8847 0001B000
No output feature configured
As expected R1 receives that packet from R2 with the label of 27 then perform a Penultimate Hop Popping (PHP) – see below

Note:

The process is important in a Layer 3 MPLS VPN (RFC2547) environment as it reduces the load on the LER. If this process didn’t happen, the LER would have to perform at least 2 label lookups:
1. The outer label, identifying that the packet was destined to have its label stripped off this router.
2. The inner label, to identify which Virtual Routing/Forwarding (VRF) instance to use for the subsequent IP routing lookup.

In a large network this can result in the CPU load on the LER reaching unacceptable levels. By having PHP for an LER done on the LSRs connected to it, the load is effectively distributed among its neighbour routers.

PHP functionality is achieved by the LER advertising a label with a value of 3 to its neighbours. This label is defined as implicit-null and informs the neighbouring LSR(s) to perform PHP.

Implicit NULL Label

The implicit NULL label is the label that has a value of 3. An egress LSR assigns the implicit NULL label to a FEC if it does not want to assign a label to that FEC, thus requesting the upstream LSR to perform a pop operation. In the case of a plain IPv4-over-MPLS network, such as an IPv4 network in which LDP distributes labels between the LSRs, the egress LSR assigns the implicit NULL label to its connected and summarized prefixes. The benefit of this is that if the egress LSR were to assign a label for these FECs, it would receive the packets with one label on top of it. It would then have to do two lookups. First, it would have to look up the label in the LFIIB, just to figure out that the label needs to be removed; then it would have to perform an IP lookup. These are two lookups, and the first is unnecessary.

The solution for this double lookup is to have the egress LSR signal the last but one (or penultimate) LSR in the label switched path (LSP) to send the packets without a label. The egress LSR signals the penultimate LSR to use implicit NULL by not sending a regular label, but by sending the special label with value 3. The result is that the egress LSR receives an IP packet and only needs to perform an IP lookup to be able to forward the packet. This enhances the performance on the egress LSR.

The use of implicit NULL at the end of an LSP is called penultimate hop popping (PHP). The LFIIB entry for the LSP on the PHP router shows a "Pop Label" as the outgoing label

*directly from Cisco website*
OSPF Filtering

The Solarwinds Server Prefix 172.100.166.166/32 must appear as prefix in AREA 1 only. It must never appear in any other areas.

Your solution must work even if a new area was added to the OSPF domain.

Do not modify the administrator distance of OSPF

Configuration:

R6
ip prefix-list AREA_0_OUT seq 10 deny 172.100.66.66/32
ip prefix-list AREA_0_OUT seq 20 permit 0.0.0.0/0 le 32

router ospf 65000
area 1 filter-list prefix AREA_0_OUT out

Verification:

Note: For instance let's check R3 before making any configuration changes and we can see all inter area routes originated from R6 (ABR) that connects to both AREA 0 and AREA 1

R3#sh ip route osp | in IA
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
O IA 172.100.66.66 [110/21] via 172.31.10.10, 00:00:01, Ethernet1/0
O IA 172.100.166.166 [110/21] via 172.31.10.10, 00:09:19, Ethernet1/0

R3#sh ip ospf database summary
OSPF Router with ID (172.100.3.3) (Process ID 65000)
Summary Net Link States (Area 0)

Link State ID: 172.100.66.66 (summary Network Number)
Advertising Router: 172.100.6.6
LS Seq Number: 80000001
Checksum: 0x2762
Length: 28
Network Mask: /32
MTID: 0        Metric: 1
Routing Bit Set on this LSA in topology Base with MTID 0
LS age: 676
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)

Link State ID: 172.100.166.166 (summary Network Number)
Advertising Router: 172.100.6.6
LS Seq Number: 80000001
Checksum: 0xEAD5
Length: 28
Network Mask: /32
MTID: 0        Metric: 1
Routing Bit Set on this LSA in topology Base with MTID 0
LS age: 84
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)

R3#sh ip ospf database | be Summary

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.66.66</td>
<td>172.100.6.6</td>
<td>157</td>
<td>0x80000001</td>
<td>0x002762</td>
</tr>
<tr>
<td>172.100.166.166</td>
<td>172.100.6.6</td>
<td>748</td>
<td>0x80000001</td>
<td>0x00EAD5</td>
</tr>
</tbody>
</table>
Note: The output should be similar on R1 R2 R3 R4 R5 and R7 – after we have made the change on R6 we can see that 172.100.66.66/32 prefix no longer appears in Area 0

R3#sh ip route osp | in IA
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   O IA 172.100.166.166 [110/21] via 172.31.10.10, 00:10:09, Ethernet1/0

R3#sh ip ospf database summary
   OSPF Router with ID (172.100.3.3) (Process ID 65000)
   Summary Net Link States (Area 0)
   Routing Bit Set on this LSA in topology Base with MTID 0
   LS age: 945
   Options: (No TOS-capability, DC, Upward)
   LS Type: Summary Links(Network)
   Link State ID: 172.100.166.166 (summary Network Number)
   Advertising Router: 172.100.6.6
   LS Seq Number: 80000001
   Checksum: 0xead5
   Network Mask: /32
      MTID: 0         Metric: 1

R3#sh ip ospf database | be Summary
   Summary Net Link States (Area 0)
   Link ID         ADV Router      Age         Seq#       Checksum
   172.100.166.166 172.100.6.6     954         0x80000001 0xead5
Berlin HQ Data Centre

OSPF

Configure OSPF 100
The Router-ID must be configured to the router’s Loopback0 interface
Advertise only Loopback0 and Ethernet1/0 of R15 into OSPF
R15 must not establish OSPF adjacency with any devices at this point in your infrastructure

Configuration:

R15
router ospf 100
  router-id 172.15.15.15
  passive-interface default
  network 172.15.15.15 0.0.0.0 area 0
  network 172.31.100.15 0.0.0.0 area 0

Verification:

R15#sh ip prot
Routing Protocol is "ospf 100"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Routing Information Sources:
  Gateway          Distance      Last Update
  Distance: (default is 110)
Service Provider #1

eBGP

Establish eBGP peering between AS25432 and AS29737 using routers physical interfaces
Advertise 197.0.0.0/9 prefixes (SP#1) with origin of incomplete and community value of 23545:196
Ethernet0/0 prefix should be advertised with community value of 0:896
All other prefixes should be advertised by default
Ensure that R97 stores internally all received updates from R96
Disable IPv4 unicast address family peering capabilities on the routers
BGP process should log changes to its neighbor adjacencies

Configuration:

**SP96**

```
ip bgp-community new-format
access-list 10 permit 197.0.0.0 0.255.255.255
access-list 20 permit 155.84.74.0 0.0.0.3
route-map RedConnBGP permit 10
match ip address 10
set community 23545:196
route-map RedConnBGP permit 20
match ip address 20
set community 0:896
route-map RedConnBGP permit 30
router bgp 25432
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 86.191.16.2 remote-as 29737
address-family ipv4
redistribute connected route-map RedConnBGP
neighbor 86.191.16.2 activate
neighbor 86.191.16.2 send-community
exit-address-family
```
**Verification:**

R96#show ip bgp neighbors 86.191.16.2 advertised-routes | beg Net

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>86.191.16.0/30</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>155.84.74.0/30</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.0.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.16.0/20</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.32.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.48.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.64.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.80.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.96.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.112.150/32</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.128.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
<tr>
<td>197.0.144.0/22</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>?</td>
</tr>
</tbody>
</table>

Total number of prefixes 12

**Note:** Because of the "route-map permit 30 statement" R96 is also advertising its connected Serial Link prefix. R97 as it is directly connected to the same network (local admin distance 0), by default it will reject any received updates for this prefix and install it as a RIB-Failure in its BGP table.

R97#show ip bgp neighbors 86.191.16.1 received-routes | beg Net

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>86.191.16.0/30</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>155.84.74.0/30</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.0.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.16.0/20</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.32.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.48.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.64.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.80.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.96.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.112.150/32</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.128.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>197.0.144.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
</tbody>
</table>

Total number of prefixes 12

R97#sh ip bgp rib-failure

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>RIB-failure</th>
<th>RIB-NH Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>86.191.16.0/30</td>
<td>86.191.16.1</td>
<td>Higher admin distance</td>
<td>n/a</td>
</tr>
</tbody>
</table>

R97#sh ip bgp 86.191.16.0/30

BGP routing table entry for 86.191.16.0/30, version 2
Paths: (1 available, best #1, table default, RIB-failure(17))
Not advertised to any peer
Refresh Epoch 1
25432, (received & used)
86.191.16.1 from 86.191.16.1 (197.0.144.150)
Origin incomplete, metric 0, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0

R97#sh ip route 86.191.16.0

Routing entry for 86.191.16.0/30
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Serial1/0
  Route metric is 0, traffic share count is 1
R97#show ip bgp community 23545:196 | beg Network

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 197.0.0.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.16.0/20</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.32.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.48.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.64.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.80.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.96.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.112.150/32</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.128.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 197.0.144.0/22</td>
<td>86.191.16.1</td>
<td>0</td>
<td>0</td>
<td>25432</td>
<td>?</td>
</tr>
</tbody>
</table>

Note: and we are also receiving all community tags from R96 so we can move onto the next question

R97#show ip bgp 197.0.112.150/32
BGP routing table entry for 197.0.112.150/32, version 11
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
25432, (received & used)
86.191.16.1 from 86.191.16.1 (197.0.144.150)
Origin incomplete, metric 0, localpref 100, valid, external, best
Community: 23545:196
rx pathid: 0, tx pathid: 0x0

R97#show ip bgp 155.84.74.0/30
BGP routing table entry for 155.84.74.0/30, version 16
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 2
25432, (received & used)
86.191.16.1 from 86.191.16.1 (197.0.144.150)
Origin incomplete, metric 0, localpref 100, valid, external, best
Community: 0:896
rx pathid: 0, tx pathid: 0x0

R97#debug ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
*Dec 20 13:48:34.270: %BGP-5-ADJCHANG: neighbor 86.191.16.1 Up
BGP(0): 86.191.16.1 recvd UPDATE w/ attr: nexthop 86.191.16.1, origin ?, metric 0, merged path 25432, AS_PATH, community 23545:196
BGP(0): 86.191.16.1 recvd 197.0.0.0/22
BGP(0): 86.191.16.1 recvd 197.0.16.0/20
BGP(0): 86.191.16.1 recvd 197.0.32.0/22
BGP(0): 86.191.16.1 recvd 197.0.48.0/22
BGP(0): 86.191.16.1 recvd 197.0.64.0/22
BGP(0): 86.191.16.1 recvd 197.0.80.0/22
BGP(0): 86.191.16.1 recvd 197.0.96.0/22
BGP(0): 86.191.16.1 recvd 197.0.112.150/32
BGP(0): 86.191.16.1 recvd 197.0.128.0/22
BGP(0): 86.191.16.1 recvd 197.0.144.0/22
BGP(0): 86.191.16.1 recvd UPDATE w/ attr: nexthop 86.191.16.1, origin ?, metric 0, merged path 25432, AS_PATH
BGP(0): 86.191.16.1 recvd 155.84.74.0/30
BGP(0): 86.191.16.1 recvd UPDATE w/ attr: nexthop 86.191.16.1, origin ?, metric 0, merged path 25432
BGP(0): 86.191.16.1 recvd 86.191.16.0/30
BGP(0): Revise route installing 1 of 1 routes for 86.191.16.0/30 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 155.84.74.0/30 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.0.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.16.0/20 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.32.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.48.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.64.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.80.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.96.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.112.150/32 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.128.0/22 to main IP table
BGP(0): Revise route installing 1 of 1 routes for 197.0.144.0/22 to main IP table
Service Provider #2

eBGP

Establish eBGP peering between AS29737 and AS10001 using routers physical interfaces
Ensure that the following (SP#2) prefixes are advertised as follows:
63.58.0.0/16 and 63.59.0.0/16 origin as incomplete - community value of 29737:979
63.63.0.0/16 origin as incomplete - community value of 29738:979
63.69.0.0/16 origin as incomplete - community value of 29739:979 (Including Global NTP)
63.70.0.0/16 origin of IGP - community value of 29740:979
All other prefixes should be advertised by default
Disable IPv4 unicast address family peering capabilities on the routers
BGP process should log changes to its neighbor adjacencies

Configuration:

SP97

access-list 10 permit 63.58.0.0 0.0.255.255
access-list 10 permit 63.59.0.0 0.0.255.255
access-list 11 permit 63.63.0.0 0.0.255.255
access-list 12 permit 63.69.0.0 0.0.255.255
access-list 13 permit 63.70.0.0 0.0.255.255

route-map RedConnBGP permit 10
match ip address 10
set community 29737:979

route-map RedConnBGP permit 20
match ip address 11
set community 29738:979

route-map RedConnBGP permit 30
match ip address 12
set community 29739:979

route-map RedConnBGP permit 40
match ip address 13
set origin igp
set community 29740:979

route-map RedConnBGP permit 50

router bgp 29737
neighbor 86.191.16.6 remote-as 10001
address-family ipv4
redistribute connected route-map RedConnBGP
neighbor 86.191.16.6 activate
neighbor 86.191.16.6 send-community
exit-address-family
SP92

ip bgp-community new-format

router bgp 10001
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 86.191.16.5 remote-as 29737

address-family ipv4
neighbor 86.191.16.5 activate
neighbor 86.191.16.5 send-community
exit-address-family

Verification:

Note: Debug on R92 to ensure we are receiving the prefixes including their community values

R92#debug ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
R92#clear ip bgp *

%BGP-5-ADJCHANGE: neighbor 86.191.16.5 Up
BGP: nbr_topo global 86.191.16.5 IPv4 Unicast:base (0x47CA188:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 86.191.16.5 IPv4 Unicast:base (0x47CA188:1) refresh_epoch is 2
BGP(0): 86.191.16.5 rcvd UPDATE w/ attr: nexthop 86.191.16.5, origin ?, merged path 29737 25432, AS_PATH , community 23545:196
BGP(0): 86.191.16.5 rcvd 197.0.0.0/22
BGP(0): 86.191.16.5 rcvd 197.0.16.0/22
BGP(0): 86.191.16.5 rcvd 197.0.32.0/22
BGP(0): 86.191.16.5 rcvd 197.0.48.0/22
BGP(0): 86.191.16.5 rcvd 197.0.64.0/22
BGP(0): 86.191.16.5 rcvd 197.0.80.0/22
BGP(0): 86.191.16.5 rcvd 197.0.96.0/22
BGP(0): 86.191.16.5 rcvd 197.0.112.150/32
BGP(0): 86.191.16.5 rcvd 197.0.128.0/22
BGP(0): 86.191.16.5 rcvd 197.0.144.0/22
BGP(0): 86.191.16.5 rcvd UPDATE w/ attr: nexthop 86.191.16.5, origin ?, metric 0, merged path 29737, AS_PATH , community 29737:979
BGP(0): 86.191.16.5 rcvd 63.58.16.0/20
BGP(0): 86.191.16.5 rcvd 63.59.128.0/20
BGP(0): 86.191.16.5 rcvd 63.59.144.150/32
BGP(0): 86.191.16.5 rcvd UPDATE w/ attr: nexthop 86.191.16.5, origin ?, metric 0, merged path 29737, AS_PATH , community 29737:979
BGP(0): 86.191.16.5 rcvd 63.69.0.150/32
BGP(0): 86.191.16.5 rcvd 63.69.16.0/20
BGP(0): 86.191.16.5 rcvd UPDATE w/ attr: nexthop 86.191.16.5, origin ?, metric 0, merged path 29737, AS_PATH , community 29737:979
BGP(0): 86.191.16.5 rcvd 63.70.96.0/20
BGP(0): 86.191.16.5 rcvd 63.70.112.0/20
BGP(0): 86.191.16.5 rcvd 86.191.16.0/30
BGP(0): 86.191.16.5 rcvd 86.191.16.4/30
BGP(0): 86.191.16.5 rcvd 63.70.112.0/20
BGP(0): 86.191.16.5 rcvd UPDATE w/ attr: nexthop 86.191.16.5, origin ?, merged path 29737 25432, AS_PATH , community 0:896
BGP(0): 86.191.16.5 rcvd 155.84.74.0/30
BGP(0): 86.191.16.5 rcvd 155.84.74.4/30
BGP(0): 86.191.16.5 rcvd 155.84.74.8/30
R92#no all
All possible debugging has been turned off
R92#
Note: and finally let's check R92 neighbour 86.191.16.5

R92#show ip bgp neighb 86.191.16.5
BGP neighbor is 86.191.16.5, remote AS 29737, external link
   BGP version 4, remote router ID 63.70.112.150
   BGP state = Established, up for 00:03:01
   Last read 00:00:09, last write 00:00:12, hold time is 180, keepalive interval is 60 seconds
   Neighbor sessions:
      1 active, is not multisession capable (disabled)
   Neighbor capabilities:
      Route refresh: advertised and received(new)
      
For address family: IPv4 Unicast
   Session: 86.191.16.5
   BGP table version 24, neighbor version 24/0
   Output queue size : 0
   Index 1, Advertise bit 0
   1 update-group member
   Community attribute sent to this neighbor
      Slow-peer detection is disabled
      Slow-peer split-update-group dynamic is disabled
   Prefix activity:
      Prefixes Current: 0 23 (Consumes 1840 bytes)
      Prefixes Total: 0 23
      Implicit Withdraw: 0 0
      Explicit Withdraw: 0 0
      Used as bestpath: n/a 23
      Used as multipath: n/a 0
   Outbound Inbound
   Local Policy Denied Prefixes: 
   Bestpath from this peer: 23 n/a
   Total: 23 0
   Number of NLRIs in the update sent: max 0, min 0
   Last detected as dynamic slow peer: never
   Dynamic slow peer recovered: never
   Refresh Epoch: 2
   
Address tracking is enabled, the RIB does have a route to 86.191.16.5
Connections established 1; dropped 0
   Last reset never
   Transport(tcp) path-mtu-discovery is enabled
   Graceful-Restart is disabled
   Connection state is ESTAB, I/O status: 1, unread input bytes: 0
   Connection is ECN Disabled, Minimum incoming TTL 0, Outgoing TTL 1
   Local host: 86.191.16.6, Local port: 13336
Foreign host: 86.191.16.5, Foreign port: 179
   Connection tableid (VRF): 0
   Maximum output segment queue size: 50
   
<Output omitted>
Service Provider #3

eBGP

Establish eBGP peering between AS28451 and AS56775 using routers physical interfaces.
Ensure that the following (SP#3) prefixes are advertised as follows:
199.0.0.0/8 origin of IGP – community value of 25458:98
All other prefixes should be advertised by default (eg: Global DNS Server)
Disable IPv4 unicast address family peering capabilities on the routers.
BGP process should NOT log changes to its neighbor adjacencies.
Do not use ACL anywhere in your configuration.

Configuration:

SP98
ip bgp-community new-format
ip prefix-list RedConnBGP_PL seq 5 permit 199.0.0.0/8 le 32
route-map RedConnBGP permit 10
match ip address prefix-list RedConnBGP_PL
set community 25458:98
route-map RedConnBGP permit 20
router bgp 28451
no bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 66.171.14.6 remote-as 56775
address-family ipv4
redistribute connected route-map RedConnBGP
neighbor 66.171.14.6 activate
neighbor 66.171.14.6 send-community
exit-address-family

SP94
ip bgp-community new-format
router bgp 56775
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 66.171.14.5 remote-as 28451
address-family ipv4
neighbor 66.171.14.5 activate
neighbor 66.171.14.5 send-community
exit-address-family
Verification:

R94#show ip bgp 199.53.176.0/20
BGP routing table entry for 199.53.176.0/20, version 14
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1

28451

66.171.14.5 from 66.171.14.5 (199.53.176.150)
Origin incomplete, metric 0, localpref 100, valid, external, best
Community: 25458:98
rx pathid: 0, tx pathid: 0x0

Note: We can that Global DNS prefix 4.2.2.2 is being received without any community values attached to it so again we are looking good!

R94#show ip bgp 4.2.2.2/32
BGP routing table entry for 4.2.2.2/32, version 2
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1

28451

66.171.14.5 from 66.171.14.5 (199.53.176.150)
Origin incomplete, metric 0, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0

R94#sh ip bgp | be Net
Network Next Hop Metric LocPrf Weight Path
>* 4.2.2.2/32 66.171.14.5 0 0 28451 ?
>* 66.171.14.0/30 66.171.14.5 0 0 28451 ?
>* 66.171.14.1/32 66.171.14.5 0 0 28451 ?
r> 66.171.14.4/30 66.171.14.5 0 0 28451 ?
>* 199.45.16.0/20 66.171.14.5 0 0 28451 ?
>* 199.46.32.0/20 66.171.14.5 0 0 28451 ?
>* 199.47.48.0/20 66.171.14.5 0 0 28451 ?
>* 199.48.64.0/20 66.171.14.5 0 0 28451 ?
>* 199.49.96.0/20 66.171.14.5 0 0 28451 ?
>* 199.50.0.0/20 66.171.14.5 0 0 28451 ?
>* 199.51.128.0/20 66.171.14.5 0 0 28451 ?
>* 199.52.160.0/20 66.171.14.5 0 0 28451 ?
>* 199.53.176.0/20 66.171.14.5 0 0 28451 ?
Service Provider #4

eBGP

Establish eBGP peering between AS5771 and AS28451 using routers physical interfaces.
Later in the lab ensure that (SP#4) 59.0.0.0/8 networks are seen by other devices with origin of incomplete and community value of 5771:5771.

Ensure that 60.99.98.0/24 prefix (Internet Prefix) is assigned an "internet" community value.
Do not use redistribution or make any configuration under the neighbor statement.

Your configuration for this task should use two separate route maps.
Disable IPv4 unicast address family peering capabilities on the routers.
BGP process should log changes to its neighbor adjacencies.
You are not allowed to use prefix list.
You can create only a single ACL sequence 10 with a single permit statement.
All other prefixes should be advertised by default.

Configuration:

```
SP98
router bgp 28451
  neighbor 66.171.14.1 remote-as 5771
  address-family ipv4
    neighbor 66.171.14.1 activate
    neighbor 66.171.14.1 send-community
    exit-address-family

SP99
ip bgp-community new-format
  access-list 10 permit 50.0.0.0 0.255.255.255
  route-map IN-COMMUNITY permit 10
    set community internet
  route-map RedConnBGP permit 10
    match ip address 10
    set community 5771:5771
  route-map RedConnBGP permit 20
  router bgp 5771
    bgp log-neighbor-changes
    no bgp default ipv4-unicast
    neighbor 66.171.14.2 remote-as 28451
    address-family ipv4
      network 60.99.98.0 mask 255.255.255.0 route-map IN-COMMUNITY
      redistribute connected route-map RedConnBGP
      neighbor 66.171.14.2 activate
      neighbor 66.171.14.2 send-community
      exit-address-family
```
**Verification:**

**Note:** Great! We are receiving updates from BGP AS 5771

R98#sh ip bgp regexp _5771$

BGP table version is 26, local router ID is 199.53.176.150

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 59.52.0.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.111.27.150/32</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.124.0.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.134.16.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.138.0.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.173.48.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.183.16.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.186.32.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 59.195.80.0/20</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 60.99.98.0/24</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>* 66.171.14.0/30</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>r&gt; 66.171.14.2/32</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.24/30</td>
<td>66.171.14.1</td>
<td>0</td>
<td>0</td>
<td>5771</td>
<td>?</td>
</tr>
</tbody>
</table>

**Note:** also community values match as per the question requirements

R98#sh ip bgp 60.99.98.0/24

BGP routing table entry for 60.99.98.0/24, version 15
Paths: (1 available, best #1, table default)
Advertised to update-groups:

1

Refresh Epoch 1

**5771**

66.171.14.1 from 66.171.14.1 (60.99.98.150)

**Origin IGP**, metric 0, localpref 100, valid, external, best

**Community:** internet

rx pathid: 0, tx pathid: 0x0

R98#sh ip bgp 59.138.0.0/20

BGP routing table entry for 59.138.0.0/20, version 20
Paths: (1 available, best #1, table default)
Advertised to update-groups:

1

Refresh Epoch 1

**5771**

66.171.14.1 from 66.171.14.1 (60.99.98.150)

**Origin incomplete**, metric 0, localpref 100, valid, external, best

**Community:** 5771:5771

rx pathid: 0, tx pathid: 0x0
Service Provider #5

eBGP

Establish eBGP peering between AS15789 and all relevant devices in AS64784

Use routers physical interfaces for the BGP neighbourship

SP#5 must establish all adjacencies **dynamically** based on the 155.84.74.0/27 subnet

Use peer group named eBGP for your solution

SP#5 should only allow maximum of 4 devices to establish eBGP peerings

Ensure that the following (SP#5) prefixes are advertised as follows:
- 117.0.0.0/16 origin of IGP - community value of 15789:91
- 117.1.0.0/16 origin of incomplete - community value of 15789:9191
- 117.3.0.0/16 origin of incomplete and community value of 91:91 (eg: Facebook Web Server)

BGP router ID in AS64784 should be routers Loopback0 interface IP Address

Disable IPv4 unicast address family peering capabilities on all routers

Ensure that communities are advertised between neighbours using a ‘**new format**’

Refer to the BGP Diagram

**Configuration:**

**R10**

```
ip bgp-community new-format

router bgp 64784
 bgp router-id 192.10.10.10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 155.84.74.10 remote-as 15789
 address-family ipv4
 neighbor 155.84.74.10 activate
 neighbor 155.84.74.10 send-community
 exit-address-family
```

**R11**

```
ip bgp-community new-format

router bgp 64784
 bgp router-id 192.11.11.11
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 155.84.74.14 remote-as 15789
 address-family ipv4
 neighbor 155.84.74.14 activate
 neighbor 155.84.74.14 send-community
 exit-address-family
```
R12
ip bgp-community new-format

router bgp 64784
 bgp router-id 192.12.12.12
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 155.84.74.17 remote-as 15789
 address-family ipv4
  neighbor 155.84.74.17 activate
  neighbor 155.84.74.17 send-community
 exit-address-family

R13
ip bgp-community new-format

router bgp 64784
 bgp router-id 192.13.13.13
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 155.84.74.21 remote-as 15789
 address-family ipv4
  neighbor 155.84.74.21 activate
  neighbor 155.84.74.21 send-community
 exit-address-family

SP91
ip bgp-community new-format

access-list 10 permit 117.0.0.0 0.0.255.255
access-list 11 permit 117.1.0.0 0.0.255.255
access-list 12 permit 117.3.0.0 0.0.255.255

route-map RedConnBGP permit 10
 match ip address 10
 set origin igp
 set community 15789:91

route-map RedConnBGP permit 20
 match ip address 11
 set community 15789:9191

route-map RedConnBGP permit 30
 match ip address 12
 set community 91:91

route-map RedConnBGP permit 40

router bgp 15789
 bgp log-neighbor-changes
 bgp listen range 155.84.74.0/27 peer-group EBGP
 bgp listen limit 4
 no bgp default ipv4-unicast
 neighbor EBGP peer-group
 neighbor EBGP remote-as 64784
 address-family ipv4
 redistribute connected route-map RedConnBGP
 neighbor EBGP activate
 neighbor EBGP send-community
 exit-address-family
Note: and quick check on all BGP relevant routers

Dynamically created based on a listen range command
Dynamically created neighbors: 4, Subnet ranges: 1
BGP peergroup EBGP listen range group members:
  155.84.74.0/27
Total dynamically created neighbors: 4/(4 max), Subnet ranges: 1

R10#show ip bgp 117.0.144.0/22
BGP routing table entry for 117.0.144.0/22, version 4
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
15789
  155.84.74.10 from 155.84.74.10 (117.3.64.150)
    Origin IGP, metric 0, localpref 100, valid, external, best
    Community: 15789:91
    rx pathid: 0, tx pathid: 0x0

R10#show ip bgp 117.1.0.0/22
BGP routing table entry for 117.1.0.0/22, version 5
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
15789
  155.84.74.10 from 155.84.74.10 (117.3.64.150)
    Origin incomplete, metric 0, localpref 100, valid, external, best
    Community: 15789:9191
    rx pathid: 0, tx pathid: 0x0

R10#show ip bgp 117.3.16.0/20
BGP routing table entry for 117.3.16.0/20, version 7
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
15789
  155.84.74.10 from 155.84.74.10 (117.3.64.150)
    Origin incomplete, metric 0, localpref 100, valid, external, best
    Community: 91:91
    rx pathid: 0, tx pathid: 0x0
Service Provider #6

iBGP

Establish iBGP peering within AS10001 using routers physical interfaces
Secure iBGP session using password “CCIEBGP” (without quotes)
Disable IPv4 unicast address family peering capabilities on both routers
On SP#6(R92) ensure that prefixes:

- 197.0.0.0/16 are assigned a community value of 0:22222 0:33333 23545:196 before they are advertised towards R93
- 110.0.0.0/16 networks (R92) are seen by other AS’s as per below output on R96:

Configuration:

SP92
access-list 10 permit 110.0.0.0 0.0.255.255
access-list 11 permit 197.0.0.0 0.0.255.255

route-map RedConnBGP permit 10
match ip address 10
set community 9999:10001

route-map RedConnBGP permit 20

route-map AddCommunity permit 10
match ip address 11
set community 0:22222 0:33333 additive

route-map AddCommunity permit 20

router bgp 10001
no bgp default ipv4-unicast
neighbor 86.191.16.9 remote-as 10001
neighbor 86.191.16.9 password CCIEBGP

address-family ipv4
redistribute connected route-map RedConnBGP
neighbor 86.191.16.9 activate
neighbor 86.191.16.9 send-community
neighbor 86.191.16.9 next-hop-self
neighbor 86.191.16.9 route-map AddCommunity out
exit-address-family

SP93
ip bgp-community new-format

router bgp 10001
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor 86.191.16.10 remote-as 10001
neighbor 86.191.16.10 password CCIEBGP

address-family ipv4
neighbor 86.191.16.10 activate
neighbor 86.191.16.10 send-community
exit-address-family
Verification:

**Note:** Example output on R96

R96#sh ip bgp 110.0.48.0/24
BGP routing table entry for 110.0.48.0/24, version 34
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
29737 10001
86.191.16.2 from 86.191.16.2 (63.70.112.150)
  Origin incomplete, localpref 100, valid, external, best
  Community: 9999:10001
  rx pathid: 0, tx pathid: 0x0

**Note:** Brilliant! Our route-map configuration has worked!

R93#sh ip bgp 197.0.32.0/22
BGP routing table entry for 197.0.32.0/22, version 34
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
29737 25432
86.191.16.10 from 86.191.16.10 (110.1.16.150)
  Origin incomplete, metric 0, localpref 100, valid, internal, best
  Community: 0:22222 0:33333 23545:196
  rx pathid: 0, tx pathid: 0x0
R93#deb ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
R93#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R93(config)#int s 5/0
R93(config-if)#no sh
*Dec 20 15:11:14.345: %SYS-5-CONFIG_I: Configured from console by console
*Dec 20 15:11:17.126: %LINK-5-UPDOWN: Line protocol on Interface Serial5/0, changed state to up
*Dec 20 15:11:7.923: %BGP-5-NOTIFICATION: received from neighbor 86.191.16.10 active 6/0 (CEASE: unknown subcode) 0 bytes
*Dec 20 15:11:7.923: %BGP-5-NEIGHBOR_RESET: Neighbor 86.191.16.10 active reset (BGP Notification received)
*Dec 20 15:11:7.923: %BGP_SESSION-5-ADJCHANGE: neighbor 86.191.16.10 Up
BGP(0): 86.191.16.10 rcvd UPDATE w/ attr: nexthop 86.191.16.10, origin ?, localpref 100, metric 0, merged path 29737 25432, AS_PATH , community 29737:0
BGP(0): 86.191.16.10 rcvd 197.0.0.0/22
BGP(0): 86.191.16.10 rcvd 197.0.16.0/20
BGP(0): 86.191.16.10 rcvd 197.0.32.0/22
BGP(0): 86.191.16.10 rcvd 197.0.48.0/22
BGP(0): 86.191.16.10 rcvd 197.0.64.0/22
BGP(0): 86.191.16.10 rcvd 197.0.80.0/22
All possible debugging has been turned off.
Service Provider #6

NLRI Advertisement

Advertise Lo401 – Lo410 of R93 into BGP (Including Google Server) – see BGP Diagram
Do not use redistribution

**Configuration:**

```
SP93
router bgp 10001
  address-family ipv4
  network 124.1.16.0 mask 255.255.255.0
  network 124.3.32.144 mask 255.255.255.248
  network 124.5.64.128 mask 255.255.255.128
  network 124.7.128.0 mask 255.255.255.0
  network 124.9.196.0 mask 255.255.255.0
  network 124.11.224.144 mask 255.255.255.240
  network 124.13.240.150 mask 255.255.255.255
  network 124.15.248.128 mask 255.255.255.224
  network 124.17.252.0 mask 255.255.255.0
  network 124.19.254.128 mask 255.255.255.192
  exit-address-family
```

**Verification:**

```
R92#show ip bgp neighbors 86.191.16.9 routes | be Net
  Network          Next Hop            Metric LocPrf Weight Path
  *>i 124.1.16.0/24  86.191.16.9              0    100      0 i
  *>i 124.3.32.144/29  86.191.16.9              0    100      0 i
  *>i 124.5.64.128/25  86.191.16.9              0    100      0 i
  *>i 124.7.128.0/24  86.191.16.9              0    100      0 i
  *>i 124.9.196.0/24  86.191.16.9              0    100      0 i
  *>i 124.11.224.144/28  86.191.16.9              0    100      0 i
  *>i 124.13.240.150/32  86.191.16.9              0    100      0 i
  *>i 124.15.248.128/27  86.191.16.9              0    100      0 i
  *>i 124.17.252.0/24  86.191.16.9              0    100      0 i
  *>i 124.19.254.128/26  86.191.16.9              0    100      0 i
Total number of prefixes 10
```
Service Provider #6 #7

eBGP

Establish eBGP peering between AS10001 and AS56775 using routers physical interfaces
On R94 redistribute Loopback 1390 – 1402 prefixes into BGP
Ensure that no other prefixes are redistributed by default
Use network statement to advertise prefixes towards R19 and R94
Do not use ACL or prefix list to accomplish this task
At this point SP#1 (R96) should receive lots of prefixes from other BGP Autonomous Systems
Ensure R96 is able send ICMP ping to the following IP Addresses, use TCL script to test:
- SP#4 (R99) 66.171.14.1
- SP#7 (R94) 155.84.74.37
- SP#7 (R94) 66.171.14.13

Configuration:

SP93

```
router bgp 10001
neighbor 66.171.14.9 remote-as 56775
  address-family ipv4
  neighbor 66.171.14.9 activate
  neighbor 66.171.14.9 send-community
  neighbor 86.191.16.10 next-hop-self
  exit-address-family
```

SP94

```
route-map RedConnBGP permit 10
  match interface Loopback1390 Loopback1391 Loopback1392 Loopback1393 Loopback1394 Loopback1395 Loopback1398 Loopback1399 Loopback1401 Loopback1402
router bgp 56775
neighbor 66.171.14.10 remote-as 10001
  address-family ipv4
  network 66.171.14.12 mask 255.255.255.252
  network 155.84.74.36 mask 255.255.255.252
  redistribute connected route-map RedConnBGP
  neighbor 66.171.14.10 activate
  neighbor 66.171.14.10 send-community
  exit-address-family
```

Verification:

```
R96#sh ip bgp summ | be Neigh
Neighbor     V AS  MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
86.191.16.2  4  29737  154  131      130    0    0 01:52:19       76
```
Note: Let’s check reachability between the furthest BGP configured routers till this point in our network. R96 is the best one to go for so we will check if its BGP table has been populated with any prefixes that came from AS 56775.

R96#sh ip bgp regexp _56775
BGP table version is 130, local router ID is 197.0.144.150.
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-path, c RIB-compressed.
RPKI validation codes: V valid, I invalid, N Not found.

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 66.171.14.12/30</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.1.224.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.1.240.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.5.32.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.5.48.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.5.176.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.6.144.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.6.224.150/32</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.6.240.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.12.0.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 75.12.32.0/20</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
<tr>
<td>*&gt; 155.84.74.36/30</td>
<td>86.191.16.2</td>
<td>0</td>
<td>29737</td>
<td>10001</td>
<td>56775</td>
</tr>
</tbody>
</table>

Note: Good and now let’s send some pings.

R96#tclsh
R96(tcl)#foreach ip {155.84.74.37; 66.171.14.1; 66.171.14.13} { ping $ip re 10}
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.37, timeout is 2 seconds: !!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 28/30/38 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 66.171.14.1, timeout is 2 seconds: !!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 34/41/53 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 66.171.14.13, timeout is 2 seconds: !!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/31/46 ms
R96(tcl)#tclquit
BGP Filtering

SP#6 network admins have been notified by SP#1 and SP#2 that the 75.x.x.x prefixes originated from BGP AS56775 (except for the Fictitious Tacacs+ Server prefix) relate to a potential virus. Configure R93 to inform R94 that it does not want to receive these routes. Achieve this in such a manner that R94 does not actually advertise these routes toward R93. Do not use an ACL for this task or filter list for this task.

SP#1 / SP#2 and SP#2 should only see in their BGP Tables also only be able to reach the three following prefixes coming from AS 56775:
- Tacacs+ Server (75.6.224.150/32)
- R94 / R19 P2P Multilink (155.84.74.36/30)
- R94 / R95 P2P Ethernet (66.171.14.12/30)

Configuration:

**SP93**

```conf
ip prefix-list VIRUS_AS56775 seq 5 deny 75.1.224.0/20
ip prefix-list VIRUS_AS56775 seq 10 deny 75.1.240.0/20
ip prefix-list VIRUS_AS56775 seq 15 deny 75.5.32.0/20
ip prefix-list VIRUS_AS56775 seq 20 deny 75.5.48.0/20
ip prefix-list VIRUS_AS56775 seq 25 deny 75.5.176.0/20
ip prefix-list VIRUS_AS56775 seq 30 deny 75.6.144.0/20
ip prefix-list VIRUS_AS56775 seq 35 deny 75.6.240.0/20
ip prefix-list VIRUS_AS56775 seq 40 deny 75.12.0.0/20
ip prefix-list VIRUS_AS56775 seq 45 deny 75.12.32.0/20
ip prefix-list VIRUS_AS56775 seq 50 permit 0.0.0.0/0 le 32
```

```
router bgp 10001
address-family ipv4
neighbor 66.171.14.9 capability orf prefix-list send
neighbor 66.171.14.9 prefix-list VIRUS_AS56775 in
exit-address-family
```

**SP94**

```
router bgp 56775
address-family ipv4
neighbor 66.171.14.10 capability orf prefix-list receive
exit-address-family
```

Verification:

The BGP Prefix-Based Outbound Route Filtering feature uses the Border Gateway Protocol (BGP) outbound route filter (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the amount of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.

Reference: [BGP Prefix-Based Outbound Route Filtering](#)

**Note:** Example BGP table from R97 before implementation:
R93#sh ip bgp regexp _56775$
BGP table version is 175, local router ID is 63.70.112.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
  r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
  x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 66.171.14.12/30</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>i</td>
</tr>
<tr>
<td>*&gt; 75.1.224.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.1.240.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.5.32.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.5.48.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.5.176.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.6.144.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.6.224.150/32</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.6.240.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.12.0.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 75.12.32.0/20</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.36/30</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>i</td>
</tr>
</tbody>
</table>

**Note:** And now after configuration has been applied we can see the filtering taking place

R93#deb ip bgp up
BGP updates debugging is on for address family: IPv4 Unicast
BGP(0): 66.171.14.9 rcvd 155.84.74.36/30
BGP(0): 66.171.14.9 rcvd UPDATE w/ attr: nexthop 66.171.14.9, origin ?, metric 0, merged path 56775, AS_PATH
BGP(0): 66.171.14.9 rcvd 75.6.224.150/32
BGP(0): Revise route installing 1 of 1 routes for 66.171.14.12/30
  > 66.171.14.9(global) to main IP table
BGP(0): Revise route installing 1 of 1 routes for 75.6.224.150/32
  > 66.171.14.9(global) to main IP table
BGP(0): Revise route installing 1 of 1 routes for 155.84.74.36/30
  > 66.171.14.9(global) to main IP table
BGP(0): 86.191.16.10 NEXT_HOP is set to self for net 66.171.14.12/30,
BGP(0): (base) 86.191.16.10 send UPDATE (format) 66.171.14.12/30, next 86.191.16.9, metric 0, path 56775
BGP(0): 86.191.16.10 NEXT_HOP is set to self for net 75.6.224.150/32,
BGP(0): 86.191.16.10 NEXT_HOP is set to self for net 155.84.74.36/30,
BGP(0): (base) 86.191.16.10 send UPDATE (format) 75.6.224.150/32, next 86.191.16.9, metric 0, path 56775
R93#un all
All possible debugging has been turned off

R94#deb ip bgp up
BGP updates debugging is on for address family: IPv4 Unicast
<Output omitted>
BGP(0): (base) 66.171.14.10 send UPDATE (format) 66.171.14.12/30, next 66.171.14.9, metric 0, path Local
BGP(0): (base) 66.171.14.10 send UPDATE (format) 75.6.224.150/32, next 66.171.14.9, metric 0, path Local
BGP(0): (base) 66.171.14.10 send UPDATE (format) 155.84.74.36/30, next 66.171.14.9, metric 0, path Local
R94#un all
All possible debugging has been turned off

R97#sh ip bgp regexp _56775$
BGP table version is 291, local router ID is 63.70.112.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
  r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
  x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 66.171.14.12/30</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>i</td>
</tr>
<tr>
<td>*&gt; 75.6.224.150/32</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.36/30</td>
<td>86.191.16.6</td>
<td>0</td>
<td>10001</td>
<td>56775</td>
<td>i</td>
</tr>
</tbody>
</table>
Service Provider #7 #8

eBGP

Establish eBGP peering between AS56775 and AS35426 using routers physical interfaces
R95 should generate a log message if it receives more than 90 prefixes from its eBGP neighbour R94
When the threshold reaches 80% router should generate a warning message
Advertise 217.0.0.0/8 (R95) networks with a community value of 35426:95
Ensure that Global NTP server and other connected prefixes are advertised “by default” with no special BGP attributes
Disable IPv4 unicast address family peering capabilities on the routers

Configuration:

```
SP94
router bgp 56775
 neighbor 66.171.14.14 remote-as 35426
    address-family ipv4
       neighbor 66.171.14.14 activate
       neighbor 66.171.14.14 send-community

SP95
ip bgp-community new-format
access-list 10 permit 217.0.0.0 0.255.255.255
route-map RedConnBGP permit 10
   match ip address 10
   set community 35426:95

route-map RedConnBGP permit 20

router bgp 35426
   no bgp default ipv4-unicast
   neighbor 66.171.14.13 remote-as 56775
       address-family ipv4
       redistribute connected route-map RedConnBGP
       neighbor 66.171.14.13 activate
       neighbor 66.171.14.13 send-community
       neighbor 66.171.14.13 maximum-prefix 90 80 warning-only
       exit-address-family
```

Verification:

**Note:** Below syslog should appear as soon as the BGP adjacency between R94 and R95 establishes

```
R95#
*Dec 20 16:13:16.125: %BGP-4-MAXPFX: Number of prefixes received from 66.171.14.13 (afi 0) reaches 73, max 90
```

**Note:** Let’s see if we can reach from SP#1 (R96) and SP#4 (R99) Global NTP Server IP Address 194.35.252.7
**Note:** Later in the lab as the BGP table grows as per one of the previous tasks R95 should begin complaining on the number of prefixes it receives. You should notice the following Syslog message on R95:

*Dec 20 17:27:52.991: %BGP-4-MAXPFX: Number of prefixes received from 66.171.14.13 (afi 0) reaches 88, max 90
*Dec 20 17:27:52.991: %BGP-3-MAXPFDEXCEED: Number of prefixes received from 66.171.14.13 (afi 0): 91 exceeds limit 90
*Dec 20 17:28:24.555: %BGP-3-MAXPFDEXCEED: Number of prefixes received from 66.171.14.13 (afi 0): 100 exceeds limit 90
*Dec 20 18:56:38.637: %BGP-3-MAXPFDEXCEED: Number of prefixes received from 66.171.14.13 (afi 0): 100 exceeds limit 90
Establish eBGP peering between AS64799 / AS35426 and AS56775 using routers physical interfaces

Use Loopback0 IP Address as BGP router ID on R17 and R18

Create a static default route on R16 towards SP#4 (R99)

Do not configure BGP between R16 and SP#4

SP#7 and SP#8 expect the BGP connection to come from AS65527 where R19 and R20 reside

Disable IPv4 unicast address family peering capabilities on all routers

Please refer to the BGP Diagram

**Configuration:**

**R16**

```
ip route 0.0.0.0 0.0.0.0 155.84.74.26
```

**R20**

```
router bgp 64799
neighbor 155.84.74.42 remote-as 35426
neighbor 155.84.74.42 local-as 65527

address-family ipv4
neighbor 155.84.74.42 activate
neighbor 155.84.74.42 send-community
exit-address-family
```

**R19**

```
router bgp 64799
neighbor 155.84.74.37 remote-as 56775
neighbor 155.84.74.37 local-as 65527

address-family ipv4
neighbor 155.84.74.37 activate
neighbor 155.84.74.37 send-community
exit-address-family
```

**R94**

```
router bgp 56775
neighbor 155.84.74.38 remote-as 65527

address-family ipv4
neighbor 155.84.74.38 activate
neighbor 155.84.74.38 send-community
exit-address-family
```

**R95**

```
router bgp 35426
neighbor 155.84.74.30 remote-as 64799
neighbor 155.84.74.34 remote-as 64799
neighbor 155.84.74.41 remote-as 65527

address-family ipv4
neighbor 155.84.74.30 activate
neighbor 155.84.74.30 send-community
neighbor 155.84.74.34 activate
neighbor 155.84.74.34 send-community
neighbor 155.84.74.41 activate
neighbor 155.84.74.41 send-community
exit-address-family
```
R17
router bgp 64799
  bgp router-id 192.17.17.17
  no bgp default ipv4-unicast
  neighbor 155.84.74.29 remote-as 35426
  address-family ipv4
  neighbor 155.84.74.29 activate
  neighbor 155.84.74.29 send-community
  exit-address-family

R18
router bgp 64799
  bgp router-id 192.18.18.18
  no bgp default ipv4-unicast
  neighbor 155.84.74.33 remote-as 35426
  address-family ipv4
  neighbor 155.84.74.33 activate
  neighbor 155.84.74.33 send-community
  exit-address-family

Verification:

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.84.74.29</td>
<td>4</td>
<td>35426</td>
<td>29</td>
<td>8</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>00:04:50</td>
<td>97</td>
</tr>
<tr>
<td>155.84.74.33</td>
<td>4</td>
<td>35426</td>
<td>29</td>
<td>8</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>00:04:37</td>
<td>97</td>
</tr>
<tr>
<td>155.84.74.37</td>
<td>4</td>
<td>56775</td>
<td>26</td>
<td>5</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>00:02:18</td>
<td>97</td>
</tr>
<tr>
<td>155.84.74.42</td>
<td>4</td>
<td>35426</td>
<td>25</td>
<td>4</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>00:01:04</td>
<td>97</td>
</tr>
</tbody>
</table>

Note: Now check R16 RIB (Routing Information Base) routing table and FIB (Forwarding Information Base) CEF table

R16#show route static | beg Gate
Gateway of last resort is 155.84.74.26 to network 0.0.0.0
S* 0.0.0.0.0/0 [1/0] via 155.84.74.26

R16#sh ip cef 0.0.0.0/0
0.0.0.0/0
  nexthop 155.84.74.26 Ethernet0/0
eBGP

R19 should not receive any prefixes from its Internet Service Provider except for the BGP default route. Do not use ACL anywhere in your configuration.

R20 should not receive any prefixes from its Internet Service Provider except for the BGP default route. Do not use ACL, Prefix List or Distribute List anywhere in your configuration. Do not perform any form of redistribution or network advertisement anywhere.

Network Admin on R96 should be able to reach external IP Addresses, see TCL script in verification.

### Configuration:

**R94**

```
ip prefix-list ONLY_DEFAULT deny 0.0.0.0/0 le 32
route-map ONLY_DEFAULT permit 10
  match ip address prefix-list ONLY_DEFAULT
router bgp 56775
  address-family ipv4
  neighbor 155.84.74.38 default-originate
  neighbor 155.84.74.38 route-map ONLY_DEFAULT out
  exit-address-family
```

**R95**

```
ip as-path access-list 1 deny .*
router bgp 35426
  address-family ipv4
  neighbor 155.84.74.41 default-originate
  neighbor 155.84.74.41 filter-list 1 out
  exit-address-family
```

### Verification:

**Note: Let's check BGP table on R19 and R20:**

```
R19#sh ip bgp summ | be Neigh
Neighbor          V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.37      4  56775 26     5       98   0    0 00:02:18 97
```

```
R20#sh ip bgp summ | be Neigh
Neighbor          V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.42      4  35426 25     4       98   0    0 00:01:04 97
```
Note: Now after configuration has been applied on the Service Provider routers:

R19#deb ip bgp up
BGP updates debugging is on for address family: IPv4 Unicast
*Dec 20 16:35:30.937: %BGP-5-ADJCHANGE: neighbor 155.84.74.37 Up
BGP(0): 155.84.74.37 rcvd UPDATE w/ attr: nexthop 155.84.74.37, origin i, merged path 65527 56775, AS_PATH
BGP(0): 155.84.74.37 rcvd 0.0.0.0/0
BGP(0): Revise route installing 1 of 1 routes for 0.0.0.0/0 -> 155.84.74.37(global) to main IP table
R19#un all
All possible debugging has been turned off

R19#sh ip bgp | be Net
Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          155.84.74.37                           0 65527 56775

R19#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer InQ OutQ Up/Down  State/PfxRcd
155.84.74.37    4        56775       5        2    0    0 00:00:37

Note: We are looking good!

R20#deb ip bgp up
BGP updates debugging is on for address family: IPv4 Unicast
*Dec 20 16:40:22.015: %BGP-5-ADJCHANGE: neighbor 155.84.74.42 Up
BGP(0): 155.84.74.42 rcvd UPDATE w/ attr: nexthop 155.84.74.42, origin i, merged path 65527 35426, AS_PATH
BGP(0): 155.84.74.42 rcvd 0.0.0.0/0
BGP(0): Revise route installing 1 of 1 routes for 0.0.0.0/0 -> 155.84.74.42(global) to main IP table
R20#un all
All possible debugging has been turned off

R20#sh ip bgp | be Net
Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          155.84.74.42                           0 65527 35426

R20#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer InQ OutQ Up/Down  State/PfxRcd
155.84.74.42    4        35426       6        5        2    0    0 00:01:18

**Note:** Let's check SP#1 (R96) Network Admin IP Address if we have got the required reachability:

R96(tcl)#foreach ip {
  +>155.84.74.25
  +>155.84.74.30
  +>155.84.74.34
  +>155.84.74.38
  +>155.84.74.41
  +>} { ping $ip sour 197.0.112.150 re 10

Type escape sequence to abort.
 Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
 !!!!!!!!!!
 Success rate is 100 percent (10/10), round-trip min/avg/max = 36/43/65 ms
 Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds:
 !!!!!!!!!!
 Success rate is 100 percent (10/10), round-trip min/avg/max = 27/33/55 ms
 Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 2 seconds:
 !!!!!!!!!!
 Success rate is 100 percent (10/10), round-trip min/avg/max = 26/30/41 ms
 Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
 !!!!!!!!!!
 Success rate is 100 percent (10/10), round-trip min/avg/max = 35/41/55 ms
 Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.41, timeout is 2 seconds:
 !!!!!!!!!!
 Success rate is 100 percent (10/10), round-trip min/avg/max = 33/42/77 ms
 R96(tcl)#tclqui
Service Provider #9

iBGP

All routers in iBGP AS5934 must have only one iBGP neighbor with the exception of R1

Secure all iBGP sessions with authentication using the password "CCIEBGP" (without quotes)
R1 should always initiate the TCP session for the BGP adjacency

Disable IPv4 unicast address family peering capabilities on all routers
All routers in AS5934 must use Loopback0 IP Address as their BGP router ID
Configure all of R1’s BGP peering sessions for fast peering deactivation, make sure that R1 does not rely on BGP dead timers

Make sure that Loopback0 is used as a source to forward packets on TCP port 179 on all routers
Routers R4 and R5 should not be configured for BGP. Refer to the BGP Diagram
Ensure your solution is ready for future MPLS VPNv4 implementation

Configuration:

R2

router bgp 5934
  bgp router-id 172.100.2.2
  no bgp default ipv4-unicast
  neighbor 172.100.1.1 remote-as 5934
  neighbor 172.100.1.1 transport connection-mode passive
  neighbor 172.100.1.1 password CCIEBGP
  neighbor 172.100.1.1 update-source Loopback0

  address-family ipv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community
  exit-address-family

  address-family vpnv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community extended
  exit-address-family

R3

router bgp 5934
  bgp router-id 172.100.3.3
  no bgp default ipv4-unicast
  neighbor 172.100.1.1 remote-as 5934
  neighbor 172.100.1.1 transport connection-mode passive
  neighbor 172.100.1.1 password CCIEBGP
  neighbor 172.100.1.1 update-source Loopback0

  address-family ipv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community
  exit-address-family

  address-family vpnv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community extended
  exit-address-family
R1

gateway bgp 5934
bgp router-id 172.100.1.1
no bgp default ipv4-unicast
neighbor 172.100.2.2 remote-as 5934
genph 172.100.2.2 transport connection-mode active
neighbor 172.100.2.2 password CCIEBGP
neighbor 172.100.2.2 update-source Loopback0
neighbor 172.100.2.2 fail-over
neighbor 172.100.3.3 remote-as 5934
neighbor 172.100.3.3 transport connection-mode active
neighbor 172.100.3.3 password CCIEBGP
neighbor 172.100.3.3 update-source Loopback0
neighbor 172.100.3.3 fail-over
neighbor 172.100.6.6 remote-as 5934
neighbor 172.100.6.6 transport connection-mode active
neighbor 172.100.6.6 password CCIEBGP
neighbor 172.100.6.6 update-source Loopback0
neighbor 172.100.6.6 fail-over
neighbor 172.100.7.7 remote-as 5934
neighbor 172.100.7.7 transport connection-mode active
neighbor 172.100.7.7 password CCIEBGP
neighbor 172.100.7.7 update-source Loopback0
neighbor 172.100.7.7 fail-over

address-family ipv4
neighbor 172.100.2.2 activate
neighbor 172.100.2.2 send-community both
neighbor 172.100.2.2 route-reflector-client
neighbor 172.100.3.3 activate
neighbor 172.100.3.3 send-community both
neighbor 172.100.3.3 route-reflector-client
neighbor 172.100.6.6 activate
neighbor 172.100.6.6 send-community both
neighbor 172.100.6.6 route-reflector-client
neighbor 172.100.7.7 activate
neighbor 172.100.7.7 send-community both
neighbor 172.100.7.7 route-reflector-client
exit-address-family

address-family vpnv4
neighbor 172.100.2.2 activate
neighbor 172.100.2.2 send-community extended
neighbor 172.100.2.2 route-reflector-client
neighbor 172.100.3.3 activate
neighbor 172.100.3.3 send-community extended
neighbor 172.100.3.3 route-reflector-client
neighbor 172.100.6.6 activate
neighbor 172.100.6.6 send-community extended
neighbor 172.100.6.6 route-reflector-client
neighbor 172.100.7.7 activate
neighbor 172.100.7.7 send-community extended
neighbor 172.100.7.7 route-reflector-client
exit-address-family
R6

router bgp 5934
  bgp router-id 172.100.6.6
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 172.100.1.1 remote-as 5934
  neighbor 172.100.1.1 transport connection-mode passive
  neighbor 172.100.1.1 password CCIEBGP
  neighbor 172.100.1.1 update-source Loopback0

  address-family ipv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community extended
  exit-address-family

  address-family vpnv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community both
  exit-address-family

R7

router bgp 5934
  bgp router-id 172.100.7.7
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 172.100.1.1 remote-as 5934
  neighbor 172.100.1.1 transport connection-mode passive
  neighbor 172.100.1.1 password CCIEBGP
  neighbor 172.100.1.1 update-source Loopback0

  address-family ipv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community
  exit-address-family

  address-family vpnv4
    neighbor 172.100.1.1 activate
    neighbor 172.100.1.1 send-community extended
  exit-address-family

Verification:

Note: These are the BGP peering we expect to see on R1

R1#
*Dec 20 17:02:35.613: %BGP-5-ADJCHANGE: neighbor 172.100.2.2 Up
R1#
*Dec 20 17:02:37.462: %BGP-5-ADJCHANGE: neighbor 172.100.7.7 Up
R1#
*Dec 20 17:02:38.481: %BGP-5-ADJCHANGE: neighbor 172.100.3.3 Up
R1#
*Dec 20 17:02:40.602: %BGP-5-ADJCHANGE: neighbor 172.100.6.6 Up
R1#show ip bgp summary
BGP router identifier 172.100.1.1, local AS number 5934
BGP table version is 1, main routing table version 1

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.2.2</td>
<td>4</td>
<td>5934</td>
<td>6</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>00:01:55</td>
<td></td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:01:55</td>
<td></td>
</tr>
<tr>
<td>172.100.6.6</td>
<td>4</td>
<td>5934</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:01:46</td>
<td></td>
</tr>
<tr>
<td>172.100.7.7</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:01:55</td>
<td></td>
</tr>
</tbody>
</table>

Note: We are also ready to accept and send MPLS VPNv4 customer prefixes based on VPNv4 AF(address family)

R1#show bgp vpnv4 unicast all summary
BGP router identifier 172.100.1.1, local AS number 5934
BGP table version is 1, main routing table version 1

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.2.2</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>00:02:03</td>
<td></td>
</tr>
<tr>
<td>172.100.3.3</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:02:03</td>
<td></td>
</tr>
<tr>
<td>172.100.6.6</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:01:54</td>
<td></td>
</tr>
<tr>
<td>172.100.7.7</td>
<td>4</td>
<td>5934</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>00:02:03</td>
<td></td>
</tr>
</tbody>
</table>
San Francisco Group HQ

**iBGP**

All routers in BGP AS64784 must be configured for iBGP in a full mesh fashion. Configure all iBGP using a peer group named ‘PEER-INTERNAL’ without the quotes.

Disable IPv4 unicast address family peering capabilities on all routers.

Use Loopback0 IP Address as their BGP router ID. (R10 and R11 would have been already partially configured from the earlier task.)

Use Loopback0 on all devices to establish iBGP peerings.

Ensure that BGP communities are being received on R8 and R9 in a ‘new format’

Refer to the BGP Diagram for your solution

---

**Configuration:**

**R8**

```plaintext
ip bgp-community new-format

router bgp 64784
  bgp router-id 192.8.8.8
  no bgp default ipv4-unicast
  neighbor PEER-INTERNAL peer-group
  neighbor PEER-INTERNAL remote-as 64784
  neighbor PEER-INTERNAL update-source Loopback0
  neighbor 192.9.9.9 peer-group PEER-INTERNAL
  neighbor 192.10.10.10 peer-group PEER-INTERNAL
  neighbor 192.11.11.11 peer-group PEER-INTERNAL

  address-family ipv4
    neighbor PEER-INTERNAL send-community
    neighbor 192.9.9.9 activate
    neighbor 192.10.10.10 activate
    neighbor 192.11.11.11 activate
    exit-address-family
```

**R9**

```plaintext
ip bgp-community new-format

router bgp 64784
  bgp router-id 192.9.9.9
  no bgp default ipv4-unicast
  neighbor PEER-INTERNAL peer-group
  neighbor PEER-INTERNAL remote-as 64784
  neighbor PEER-INTERNAL update-source Loopback0
  neighbor 192.8.8.8 peer-group PEER-INTERNAL
  neighbor 192.10.10.10 peer-group PEER-INTERNAL
  neighbor 192.11.11.11 peer-group PEER-INTERNAL

  address-family ipv4
    neighbor PEER-INTERNAL send-community
    neighbor 192.8.8.8 activate
    neighbor 192.10.10.10 activate
    neighbor 192.11.11.11 activate
    exit-address-family
```
**R10**

```text
router bgp 64784
neighbor PEER-INTERNAL peer-group
neighbor PEER-INTERNAL remote-as 64784
neighbor PEER-INTERNAL update-source Loopback0
neighbor 192.8.8.8 peer-group PEER-INTERNAL
neighbor 192.9.9.9 peer-group PEER-INTERNAL
neighbor 192.11.11.11 peer-group PEER-INTERNAL

default-family ipv4
neighbor PEER-INTERNAL send-community
neighbor 192.8.8.8 activate
neighbor 192.9.9.9 activate
neighbor 192.11.11.11 activate
exit-address-family
```

**R11**

```text
router bgp 64784
neighbor PEER-INTERNAL peer-group
neighbor PEER-INTERNAL remote-as 64784
neighbor PEER-INTERNAL update-source Loopback0
neighbor 192.8.8.8 peer-group PEER-INTERNAL
neighbor 192.9.9.9 peer-group PEER-INTERNAL
neighbor 192.10.10.10 peer-group PEER-INTERNAL

default-family ipv4
neighbor PEER-INTERNAL send-community
neighbor 192.8.8.8 activate
neighbor 192.9.9.9 activate
neighbor 192.10.10.10 activate
exit-address-family
```

Verification:

```text
R10#sh ip bgp summ | be Neig
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.10    4        15789     158     153       14    0    0 02:17:21       13
192.8.8.8       4        64784       4       8       14    0    0 00:00:54        0
192.9.9.9       4        64784       4       9       14    0    0 00:00:52        0
192.11.11.11    4        64784       9       9       14    0    0 00:00:22       13
```

**Note:** Let's check R10 to see what it thinks what is the best route towards prefixes originated from AS 15789?

```text
R10#sh ip bgp 117.0.144.0/22
BGP routing table entry for 117.0.144.0/22, version 4
Paths: (2 available, best #2, table default)
Advertised to update-groups:
  2
  Refresh Epoch 2
  15789
155.84.74.14 from 192.11.11.11 (192.11.11.11)
  Origin IGP, metric 0, localpref 100, valid, internal
  Community: 15789:91
  rx pathid: 0, tx pathid: 0
  Refresh Epoch 1
  15789
155.84.74.10 from 155.84.74.10 (117.3.64.150)
  Origin IGP, metric 0, localpref 100, valid, best
  Community: 15789:91
  rx pathid: 0, tx pathid: 0x0
```
Note: Prefixes learned from R11 have admin distance of 200 (iBGP) versus distance of 20 (eBGP) so the path towards R91 is considered valid and best, similar result should be visible on R11.

R10#sh ip route 117.0.144.0
Routing entry for 117.0.144.0/22
Known via "bgp 64784", distance 20, metric 0
Tag 15789, type external
Last update from 155.84.74.10 02:20:17 ago
Routing Descriptor Blocks:
  * 155.84.74.10, from 155.84.74.10, 02:20:17 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 15789
    MPLS label: none

Note: Finally we will check R8 and R9.

R8#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.9.9.9       4        64784       5       5        1    0    0 00:02:09        0
192.10.10.10    4        64784       9       5        1    0    0 00:01:19       13
192.11.11.11    4        64784       9       2        1    0    0 00:00:51       13

R9#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.8.8.8       4        64784       5       5        1    0    0 00:02:38        0
192.10.10.10    4        64784       10      5        1    0    0 00:01:45       13
192.11.11.11    4        64784       9       3        1    0    0 00:01:24       13

R8#sh ip bgp | be Net
Network          Next Hop            Metric LocPrf Weight Path
* i 117.0.32.0/22    155.84.74.14             0    100      0 15789 i
* i 117.0.128.0/22   155.84.74.14             0    100      0 15789 i
* i 117.0.144.0/22   155.84.74.14             0    100      0 15789 i
* i 117.1.0.0/22     155.84.74.14             0    100      0 15789 i
* i 117.3.0.0/22     155.84.74.14             0    100      0 15789 ?
* i 117.3.16.0/20    155.84.74.14             0    100      0 15789 ?
* i 117.3.32.0/22    155.84.74.14             0    100      0 15789 ?
* i 117.3.48.150/32  155.84.74.14             0    100      0 15789 ?
* i 117.3.64.0/22    155.84.74.14             0    100      0 15789 ?
* i 155.84.74.8/30   155.84.74.14             0    100      0 15789 ?
<Output omitted>

Note: None of the prefixes is shown as best > on R8 and R9 due to the next hop not being configured yet neither on R10 nor R11 what is clearly seen below:
R8#show ip bgp 117.3.64.0/22
BGP routing table entry for 117.3.64.0/22, version 0
Paths: (2 available, no best path)
Flag: Ox820
 Not advertised to any peer
Refresh Epoch 2
 15789
  155.84.74.14 (inaccessible) from 192.11.11.11 (192.11.11.11)
    Origin incomplete, metric 0, localpref 100, valid, internal
    Community: 91:91
    rx pathid: 0, tx pathid: 0
Refresh Epoch 1
  15789
  155.84.74.10 (inaccessible) from 192.10.10.10 (192.10.10.10)
    Origin incomplete, metric 0, localpref 100, valid, internal
    Community: 91:91
    rx pathid: 0, tx pathid: 0

R8#sh ip route 155.84.74.14
% Subnet not in table

R8#sh ip route 155.84.74.10
% Subnet not in table

Note: Move onto the next question where we will apply the remaining configuration
eBGP – Next Hop Self

Establish eBGP peering between AS64784 / SP#1 and SP#6 using routers physical interfaces
Ensure that BGP next-hop is never marked as unreachable as long as interface Loopback0 of the remote peer is known via IGP
On R8 do not use the “next-hop-self” command to accomplish this task
Ensure R12 and R13 receive all BGP prefixes
Test ICMP reachability from R16 and R20 outside interface IP Addresses towards R12 and R13 outside interface IP Addresses

Configuration:

R10
router bgp 64784
    address-family ipv4
    neighbor PEER-INTERNAL next-hop-self
    exit-address-family

R11
router bgp 64784
    neighbor 140.60.88.13 remote-as 10001
    address-family ipv4
    neighbor PEER-INTERNAL next-hop-self
    neighbor 140.60.88.13 activate
    neighbor 140.60.88.13 send-community
    exit-address-family

R8
route-map NEXT_HOP permit 10
    set ip next-hop self
router bgp 64784
    neighbor 155.84.74.2 remote-as 25432
    address-family ipv4
    neighbor PEER-INTERNAL route-map NEXT_HOP out
    neighbor 155.84.74.2 activate
    neighbor 155.84.74.2 send-community
    exit-address-family

R96
router bgp 25432
    neighbor 155.84.74.1 remote-as 64784
    address-family ipv4
    neighbor 155.84.74.1 activate
    neighbor 155.84.74.1 send-community
    exit-address-family

R93
router bgp 10001
    neighbor 140.60.88.14 remote-as 64784
    address-family ipv4
    neighbor 140.60.88.14 activate
    neighbor 140.60.88.14 send-community
    exit-address-family
R12
router bgp 64784
  address-family ipv4
  neighbor 155.84.74.17 allowas-in
  exit-address-family

R13
router bgp 64784
  address-family ipv4
  neighbor 155.84.74.21 allowas-in
  exit-address-family

Verification: Before allowas-in is applied

R12#debug ip bgp up
BGP updates debugging is on for address family: IPv4 Unicast
R12#clear ip bgp * so i
R12#
BGP: nbr_topo global 155.84.74.17 IPv4 Unicast:base (0x37D7CF0:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 155.84.74.17 IPv4 Unicast:base(0x37D7CF0:1) refresh_epoch is 2
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: next-hop 155.84.74.17, origin ?, metric 0, merged path 15789, AS_PATH, community 15789:9191
BGP(0): 155.84.74.17 rcvd 17.1.0.0/22...duplicate ignored
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: next-hop 155.84.74.17, origin ?, originator 0.0.0.0, merged path 15789 64784 1051 56775
35424, AS_PATH, community, extended community, SSA attribute
BGPSSA ssacount is 0
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: nexthop 155.84.74.17, origin ?, metric 0, merged path 15789, AS_PATH, community 15789:9191
BGP(0): 155.84.74.17 rcvd 17.0.32.0/22...duplicate ignored
BGP(0): 155.84.74.17 rcvd 17.0.128.0/22...duplicate ignored
BGP(0): 155.84.74.17 rcvd 17.0.144.0/22...duplicate ignored
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: nexthop 155.84.74.17, origin ?, originator 0.0.0.0, merged path 15789 64784 25432, AS_PATH, community 23545:196, extended community, SSA attribute
BGPSSA ssacount is 0
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.0.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.16.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.32.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.48.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.64.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.80.0/22...DENIED due to: AS_PATH contains our own AS;
BGP(0): 155.84.74.17 rcvd UPDATE about 17.0.96.0/22...DENIED due to: AS_PATH contains our own AS;
<Output omitted>...
R12#un all
All possible debugging has been turned off

R12#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.17    4        15789     247     184       14    0    0 02:43:56 13

R13#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.21    4        15789     223     184       14    0    0 02:44:13 13
Verification: After allowas-in is applied

R12#dev ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
BGP: nbr_topo global 155.84.74.17 IPv4 Unicast:base (0x37D7CF0:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 155.84.74.17 IPv4 Unicast:base (0x37D7CF0:1) refresh_epoch is 3
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: nexthop 155.84.74.17, origin I, metric 0, merged path 15789, AS_PATH , community 15789:9191
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: nexthop 155.84.74.17, origin I, metric 0, merged path 15789, AS_PATH , community 15789:9191
BGP(0): 155.84.74.17 rcvd UPDATE w/ attr: nexthop 155.84.74.17, origin I, metric 0, merged path 15789, AS_PATH , community 23545:196

R12#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.17  4        15789     284     196      102    0    0 02:54:47 101

R13#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.21  4        15789     260     196      102    0    0 02:54:55 101

Note: Ok allow-as did the trick so now let’s see if we can reach outside interface IP Address of R12 and R13 from R16 and R20

R16#ping 155.84.74.18 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 6/11/16 ms

R16#traceroute 155.84.74.18 probe 1
Type escape sequence to abort.
Tracing the route to 155.84.74.18
VRF info: (vrf in name/id, vrf out name/id)
1 155.84.74.26 1 msec
2 66.171.14.2 10 msec
3 66.171.14.6 10 msec
4 66.171.14.10 10 msec
5 140.60.88.14 14 msec
6 155.84.74.14 9 msec
7 155.84.74.18 10 msec
R20#ping 155.84.74.22 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 8/11/15 ms

R20#traceroute 155.84.74.22 probe 1
Type escape sequence to abort.
Tracing the route to 155.84.74.22
VRF info: (vrf in name/id, vrf out name/id)
1 155.84.74.42 [AS 35426] 9 msec
3 66.171.14.10 [AS 35426] 10 msec
4 140.60.88.14 [AS 35426] 6 msec
5 155.84.74.14 [AS 35426] 4 msec
6 155.84.74.22 [AS 35426] 12 msec

Note: We can see that the traffic traverses from SP#6 towards to R11 (AS 64784) and then to the final destination which is OK as there was no requirement to manipulate routing path...yet 😊

R10#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.10    4        15789     218     215      206    0    0 02:40:13       13
192.9.9.9       4        64784     64      64      206    0    0 00:02:03       13
192.10.10.10    4        64784     40      64      206    0    0 00:02:03       13
192.11.11.11    4        64784     56      64      206    0    0 00:02:03       13

R10#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.2     4        25432     36       26      181    0    0 00:23:37       89
192.9.9.9       4        64784     30      64      181    0    0 00:24:06       13
192.10.10.10    4        64784     40      64      181    0    0 00:24:06       13
192.11.11.11    4        64784     56      62      181    0    0 00:23:37       89

R8#sh ip bgp summ | be Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
155.84.74.2     4        25432     36       26      181    0    0 00:23:37       88
192.9.9.9       4        64784     30      64      181    0    0 00:24:06       13
192.10.10.10    4        64784     40      64      181    0    0 00:24:06       13
192.11.11.11    4        64784     56      62      181    0    0 00:23:37       89

R8#sh ip bgp | be Netw
Network          Next Hop          Metric LocPrf Weight Path
*              4.2.2.2/32 192.11.11.11 0 100 0 10001 56775 28451 ?
*              59.52.0.0/20 192.11.11.11 0 100 0 10001 56775 28451 5771 ?
*              59.111.27.150/32 192.11.11.11 0 100 0 10001 56775 28451 5771 ?
*              59.124.0.0/20 192.11.11.11 0 100 0 10001 56775 28451 5771 ?
*              59.134.16.0/20 192.11.11.11 0 100 0 10001 56775 28451 5771 ?
<Output omitted>
Route Preference

Inbound and outbound traffic destined to/from AS64784 should always enter via R8 then R11 in case of R8’s failure.

After successful implementation R93 should always route via its P2P neighbour R92 and R11 only when its connection to R92 goes down.

At the end of this task each office external interface in Sydney should be able to reach external internet interfaces of every Office/Data Center in San Francisco.

Configuration:

R8
route-map BGP_PREF permit 10
set local-preference 555
router bgp 64784
address-family ipv4
neighbor 155.84.74.2 route-map BGP_PREF in
exit-address-family

R11
router bgp 64784
address-family ipv4
neighbor 140.60.88.13 route-map BGP_PREF in
neighbor 140.60.88.13 route-map BGP_PATH out
exit-address-family
route-map BGP_PATH permit 10
set as-path prepend 64784 64784 64784 64784 64784
route-map BGP_PREF permit 10
set local-preference 554

R10
router bgp 64784
address-family ipv4
neighbor 155.84.74.10 route-map BGP_PATH out
exit-address-family
route-map BGP_PATH permit 10
set as-path prepend 64784 64784 64784 64784 64784
Verification:

**Note:** Let's check one more time how the traffic is being routed outbound from AS64784.

*We will pick the Global DNS Server IP Address 4.2.2.2 as our destination target prefix.*

```plaintext
R8#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 116
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
    3
  Refresh Epoch 3
    10001 56775 28451
       192.11.11.11 (metric 857215) from 192.11.11.11 (192.11.11.11)
       Origin incomplete, metric 0, localpref 100, valid, internal, best
       rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 2
    25432 29737 10001 56775 28451
       155.84.74.2 from 155.84.74.2 (197.0.144.150)
       Origin incomplete, localpref 100, valid, external
       rx pathid: 0, tx pathid: 0

R8#sh ip route 4.2.2.2
Routing entry for 4.2.2.2/32
Known via "bgp 64784", distance 200, metric 0
  Tag 0.0.39.17, type internal
  Last update from 192.11.11.11 00:59:17 ago
Routing Descriptor Blocks:
  * 192.11.11.11, from 192.11.11.11, 00:59:17 ago
  Route metric is 0, traffic share count is 1
  AS Hops 3
  Route tag 0.0.39.17
  MPLS label: none

**Note:** Looks like R8 prefers R11 as its exit point out of the AS 64784 due to shorter AS path 3 hops vs 5 hops.

*And the same goes for R11 which prefers its eBGP neighbor SP#6 (R93) as the next hop so let's begin making changes.*

```plaintext
R11#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 107
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    1
  Refresh Epoch 2
    10001 56775 28451
       140.60.88.13 from 140.60.88.13 (124.19.254.150)
       Origin incomplete, localpref 100, valid, external, best
       rx pathid: 0, tx pathid: 0x0
```
**Note:** After configuring Local Preference on R8 we can see that R10 and R11 are now using R8 as the next hop but strangely R12 and R13 are now no longer able to reach Global DNS IP Address 4.2.2.2?

R11#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 250
Paths: (2 available, best #1, table default)
Flag: Ox820
    Advertised to update-groups: (Pending Update Generation)
        1
    Refresh Epoch 1
        25432 29737 10001 56775 28451
            192.8.8.8 (metric 857215) from 192.8.8.8 (192.8.8.8)
            Origin incomplete, metric 0, localpref 555, valid, internal, **best**
            rx pathid: 0, tx pathid: 0x0
    Refresh Epoch 2
        10001 56775 28451
            140.60.88.13 from 140.60.88.13 (124.19.254.150)
            Origin incomplete, localpref 100, valid, external
            rx pathid: 0, tx pathid: 0

R12#ping 4.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
......
Success rate is 0 percent (0/5)

R12#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 165
Paths: (1 available, best #1, table default)
    Not advertised to any peer
    Refresh Epoch 3
        15789 64784 25432 29737 10001 56775 28451
            155.84.74.17 from 155.84.74.17 (117.3.64.150)
            Origin incomplete, localpref 100, valid, external, **best**
            rx pathid: 0, tx pathid: 0x0

R13#ping 4.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
......
Success rate is 0 percent (0/5)

R13#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 165
Paths: (1 available, best #1, table default)
    Not advertised to any peer
    Refresh Epoch 2
        15789 64784 25432 29737 10001 56775 28451
            155.84.74.21 from 155.84.74.21 (117.3.64.150)
            Origin incomplete, localpref 100, valid, external, **best**
            rx pathid: 0, tx pathid: 0x0
R91#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 255
Paths: (2 available, best #2, table default)
   Advertised to update-groups: 1
   Refresh Epoch 1
64784 25432 29737 10001 56775 28451
   155.84.74.13 from *155.84.74.13 (192.11.11.11)
      Origin incomplete, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
   Refresh Epoch 1
64784 25432 29737 10001 56775 28451
   155.84.74.9 from *155.84.74.9 (192.10.10.10)
      Origin incomplete, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0

Note: R91 points towards R10

R10#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 294
Paths: (1 available, best #1, table default)
   Advertised to update-groups: 1
   Refresh Epoch 1
25432 29737 10001 56775 28451
   192.8.8.8 (metric 861498) from 192.8.8.8 (192.8.8.8)
      Origin incomplete, metric 0, localpref 555, valid, internal, best
      rx pathid: 0, tx pathid: 0x0

Note: R8 points towards R96

R8#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 263
Paths: (1 available, best #1, table default)
   Advertised to update-groups: 2
   Refresh Epoch 5
25432 29737 10001 56775 28451
   155.84.74.2 from 155.84.74.2 (197.0.144.150)
      Origin incomplete, localpref 555, valid, external, best
      rx pathid: 0, tx pathid: 0x0

Note: What if we check the reverse path towards R12 and R13. They both are using external Ethernet interfaces. We'll jump directly on R93

R93#sh ip bgp 155.84.74.16
BGP routing table entry for 155.84.74.16/30, version 119
Paths: (1 available, best #1, table default)
   Advertised to update-groups: 8
   Refresh Epoch 2
64784 15789
   140.60.88.14 from 140.60.88.14 (192.11.11.11)
      Origin incomplete, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
R93#sh ip bgp 155.84.74.20
BGP routing table entry for 155.84.74.20/30, version 120
Paths: (1 available, best #1, table default)
  Advertised to update-groups: 8 9
  Refresh Epoch 2
  64784 15789
     140.60.88.14 from 140.60.88.14 (192.11.11.11)
     Origin incomplete, localpref 100, valid, external, best
     rx pathid: 0, tx pathid: 0x0

R98#traceroute 155.84.74.16 source 4.2.2.2 probe 1
Type escape sequence to abort.
Tracing the route to 155.84.74.16
VRF info: (vrf in name/id, vrf out name/id)
  1 66.171.14.6 5 msec
  2 66.171.14.10 6 msec
  3 140.60.88.14 24 msec
  4 *
  5 *
  6 *
  7 *
<Output omitted>

R12#traceroute 4.2.2.2 probe 1
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 155.84.74.17 [AS 15789] 5 msec
  2 155.84.74.9 [AS 15789] 8 msec
  3 *
  4 *
<Output omitted>

Note: and this is our problem - R93 should route via its iBGP neighbour R92 and not via R11. After we have made another configuration change we can see R11 finally prefers R8 instead also R93 prefers R92 however we are still not able to reach 4.2.2.2 from R12 or R13?

R11#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 250
Paths: (2 available, best #1, table default)
  Advertised to update-groups: 1 4
  Refresh Epoch 2
  25432 29737 10001 56775 28451
     192.8.8.8 (metric 857215) from 192.8.8.8 (192.8.8.8)
     Origin incomplete, metric 0, localpref 555, valid, internal, best
     rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 3
  10001 56775 28451
     140.60.88.13 from 140.60.88.13 (124.19.254.150)
     Origin incomplete, localpref 554, valid, external
     rx pathid: 0, tx pathid: 0
R9#sh ip bgp 155.84.74.20
BGP routing table entry for 155.84.74.20/30, version 167
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
    9
Refresh Epoch 1
29737 25432 64784 15789
  86.191.16.10 from 86.191.16.10 (110.1.16.150)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    rx pathid: 0, tx pathid: 0
Refresh Epoch 10
64784 64784 64784 64784 64784 64784 15789
  140.60.88.14 from 140.60.88.14 (192.11.11.11)
    Origin incomplete, localpref 100, valid, external
    rx pathid: 0, tx pathid: 0

Note: If we check R8 BGP table for R12 and R13 external interface 155.84.74.16/30 and 155.84.74.20/30 IP Addresses we will notice that R8 wants to route via R11 then in the opposite direction R91 prefers R10 to reach 4.2.2.2 so let's fix it by adjusting as path outbound on R10 so that R91 prefers R11 instead
Let’s get the ping going in all directions:

R12#ping 4.2.2.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
..............................................................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                         !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 74 percent (74/100), round-trip min/avg/max = 22/31/44 ms

R13#ping 4.2.2.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
..............................................................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                         !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 81 percent (81/100), round-trip min/avg/max = 17/30/40 ms

R98#ping 155.84.74.18 source 4.2.2.2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
Packet sent with a source address of 4.2.2.2
..............................................................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                         !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 57 percent (57/100), round-trip min/avg/max = 25/31/44 ms

R9#sh ip bgp 4.2.2.2
BGP routing table entry for 4.2.2.2/32, version 301
Paths: (2 available, best #1, table default)
  Advertised to update-groups:
    1
Refresh Epoch 10
64784 25432 29737 10001 56775 28451
  155.84.74.13 from *155.84.74.13 (192.11.11.11)
    Origin incomplete, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0
Refresh Epoch 6
64784 64784 64784 64784 64784 64784 28451
  155.84.74.9 from *155.84.74.9 (192.10.10.10)
    Origin incomplete, localpref 100, valid, external
    rx pathid: 0, tx pathid: 0
R12#traceroute 4.2.2.2 pr 1
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 155.84.74.17 [AS 15789] 7 msec
2 155.84.74.13 [AS 15789] 14 msec
3 192.168.10.21 11 msec
4 155.84.74.2 [AS 25432] 1 msec
5 86.191.16.2 [AS 25432] 7 msec
6 86.191.16.6 [AS 29737] 22 msec
7 86.191.16.9 [AS 10001] 28 msec
8 66.171.14.9 28 msec
9 66.171.14.5 [AS 28451] 29 msec

R13#traceroute 4.2.2.2 pr 1
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 155.84.74.21 [AS 15789] 5 msec
2 155.84.74.13 [AS 15789] 5 msec
3 192.168.10.21 12 msec
4 155.84.74.2 [AS 25432] 1 msec
5 86.191.16.2 [AS 25432] 11 msec
6 86.191.16.6 [AS 29737] 21 msec
7 86.191.16.9 [AS 10001] 38 msec
8 66.171.14.9 26 msec
9 66.171.14.5 [AS 28451] 39 msec

R98#traceroute 155.84.74.18 to 4.2.2.2 pr 1
Type escape sequence to abort.
Tracing the route to 155.84.74.18
VRF info: (vrf in name/id, vrf out name/id)
1 66.171.14.6 4 msec
2 66.171.14.10 1 msec
3 86.191.16.10 [AS 10001] 11 msec
4 86.191.16.5 [AS 10001] 21 msec
5 86.191.16.1 [AS 29737] 33 msec
6 155.84.74.1 [AS 25432] 36 msec
7 192.168.10.22 30 msec
8 155.84.74.14 [AS 15789] 64 msec
9 155.84.74.18 [AS 15789] 53 msec

R98#traceroute 155.84.74.22 to 4.2.2.2 pr 1
Type escape sequence to abort.
Tracing the route to 155.84.74.22
VRF info: (vrf in name/id, vrf out name/id)
1 66.171.14.6 7 msec
2 66.171.14.10 1 msec
3 86.191.16.10 [AS 10001] 13 msec
4 86.191.16.5 [AS 10001] 20 msec
5 86.191.16.1 [AS 29737] 18 msec
6 155.84.74.1 [AS 25432] 26 msec
7 192.168.10.22 33 msec
8 155.84.74.14 [AS 15789] 33 msec
9 155.84.74.22 [AS 15789] 28 msec
Note: Looking good now so the final test is to see if R12 and R13 have ICMP reachability to each external interface IP Address across the BGP topology we have set up so far:

R12(tcl)#foreach CCIE {
  +>155.84.74.25
  +>155.84.74.30
  +>155.84.74.34
  +>155.84.74.38
  +>155.84.74.41
  +} { ping $CCIE time 5 re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 34/45/61 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 25/35/49 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 22/34/50 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 34/39/46 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.41, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 38/41/48 ms
R12(tcl)#tclquit

R13#tclsh
R13(tcl)#foreach CCIE {
  +>155.84.74.25
  +>155.84.74.30
  +>155.84.74.34
  +>155.84.74.38
  +>155.84.74.41
  +} { ping $CCIE time 5 re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 38/41/46 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 28/32/37 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 28/34/49 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 28/34/49 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.41, timeout is 5 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 37/42/53 ms
R13(tcl)#tclquit
R13#tclsh
R13(tcl)#foreach CCIE {
+>155.84.74.25 
+>155.84.74.30 
+>155.84.74.34 
+>155.84.74.38 
+>} { traceroute $CCIE pro 1 } 
Type escape sequence to abort.
Tracing the route to 155.84.74.25 
VRF info: (vrf in name/id, vrf out name/id)
 1 155.84.74.21 [AS 15789] 1 msec 
 2 155.84.74.13 [AS 15789] 5 msec 
 3 192.168.10.21 7 msec 
 4 155.84.74.2 [AS 25432] 11 msec 
 5 86.191.16.2 [AS 25432] 11 msec 
 6 86.191.16.6 [AS 29737] 22 msec 
 7 86.191.16.9 [AS 10001] 33 msec 
 8 66.171.14.9 27 msec 
 9 66.171.14.5 [AS 28451] 29 msec 
 10 66.171.14.1 [AS 28451] 44 msec 
 11 155.84.74.25 [AS 5771] 51 msec 
Type escape sequence to abort. 
Tracing the route to 155.84.74.30 
VRF info: (vrf in name/id, vrf out name/id)
 1 155.84.74.21 [AS 15789] 5 msec 
 2 155.84.74.13 [AS 15789] 9 msec 
 3 192.168.10.21 8 msec 
 4 155.84.74.2 [AS 25432] 9 msec 
 5 86.191.16.2 [AS 25432] 9 msec 
 6 86.191.16.6 [AS 29737] 21 msec 
 7 86.191.16.9 [AS 10001] 25 msec 
 8 66.171.14.9 32 msec 
 10 155.84.74.30 [AS 35426] 37 msec 
Type escape sequence to abort. 
Tracing the route to 155.84.74.34 
VRF info: (vrf in name/id, vrf out name/id)
 1 155.84.74.21 [AS 15789] 20 msec 
 2 155.84.74.13 [AS 15789] 5 msec 
 3 192.168.10.21 7 msec 
 4 155.84.74.2 [AS 25432] 4 msec 
 5 86.191.16.2 [AS 25432] 10 msec 
 6 86.191.16.6 [AS 29737] 21 msec 
 7 86.191.16.9 [AS 10001] 35 msec 
 8 66.171.14.9 32 msec 
10 155.84.74.34 [AS 35426] 29 msec 
Type escape sequence to abort. 
Tracing the route to 155.84.74.41 
VRF info: (vrf in name/id, vrf out name/id)
 1 155.84.74.21 [AS 15789] 6 msec 
 2 155.84.74.13 [AS 15789] 1 msec 
 3 192.168.10.21 13 msec 
 4 155.84.74.2 [AS 25432] 6 msec 
 5 86.191.16.2 [AS 25432] 10 msec 
 6 86.191.16.6 [AS 29737] 22 msec 
 7 86.191.16.9 [AS 10001] 30 msec 
 8 66.171.14.9 20 msec 
 9 155.84.74.38 [AS 56775] 35 msec 
Type escape sequence to abort. 
Tracing the route to 155.84.74.41 
VRF info: (vrf in name/id, vrf out name/id)
 1 155.84.74.21 [AS 15789] 7 msec 
 2 155.84.74.13 [AS 15789] 1 msec 
 3 192.168.10.21 1 msec 
 4 155.84.74.2 [AS 25432] 1 msec 
 5 86.191.16.2 [AS 25432] 10 msec 
 6 86.191.16.6 [AS 29737] 21 msec 
 7 86.191.16.9 [AS 10001] 31 msec 
 8 66.171.14.9 85 msec 
10 155.84.74.41 [AS 35426] 47 msec 
R12#tclsh
R12(tcl)#foreach CCIE {  
  ->155.84.74.25  
  ->155.84.74.30  
  ->155.84.74.34  
  ->155.84.74.38  
  ->155.84.74.41  
  }  
  ( traceroute $CCIE pro 1 )

Type escape sequence to abort.
Tracing the route to 155.84.74.25
VRF info: (vrf in name/id, vrf out name/id)
  1 155.84.74.17 [AS 15789] 2 msec
  2 155.84.74.13 [AS 15789] 2 msec
  3 192.168.10.21 7 msec
  4 155.84.74.2 [AS 25432] 9 msec
  5 86.191.16.2 [AS 25432] 10 msec
  6 86.191.16.6 [AS 29737] 19 msec
  7 86.191.16.9 [AS 10001] 33 msec
  8 66.171.14.9 33 msec
  9 66.171.14.5 [AS 28451] 29 msec
  10 66.171.14.1 [AS 28451] 45 msec
  11 155.84.74.25 [AS 5771] 40 msec
Type escape sequence to abort.
Tracing the route to 155.84.74.30
VRF info: (vrf in name/id, vrf out name/id)
  1 155.84.74.17 [AS 15789] 5 msec
  2 155.84.74.13 [AS 15789] 1 msec
  3 192.168.10.21 2 msec
  4 155.84.74.2 [AS 25432] 6 msec
  5 86.191.16.2 [AS 25432] 11 msec
  6 86.191.16.6 [AS 29737] 22 msec
  7 86.191.16.9 [AS 10001] 35 msec
  8 66.171.14.9 25 msec
  10 155.84.74.30 [AS 35426] 31 msec
Type escape sequence to abort.
Tracing the route to 155.84.74.34
VRF info: (vrf in name/id, vrf out name/id)
  1 155.84.74.17 [AS 15789] 9 msec
  2 155.84.74.13 [AS 15789] 8 msec
  3 192.168.10.21 8 msec
  4 155.84.74.2 [AS 25432] 4 msec
  5 86.191.16.2 [AS 25432] 10 msec
  6 86.191.16.6 [AS 29737] 19 msec
  7 86.191.16.9 [AS 10001] 30 msec
  8 66.171.14.9 32 msec
Type escape sequence to abort.
Tracing the route to 155.84.74.41
VRF info: (vrf in name/id, vrf out name/id)
  1 155.84.74.17 [AS 15789] 6 msec
  2 155.84.74.13 [AS 15789] 6 msec
  3 192.168.10.21 1 msec
  4 155.84.74.2 [AS 25432] 1 msec
  5 86.191.16.2 [AS 25432] 10 msec
  6 86.191.16.6 [AS 29737] 25 msec
  7 86.191.16.9 [AS 10001] 31 msec
  8 66.171.14.9 34 msec
  10 155.84.74.41 [AS 35426] 45 msec
San Francisco Group Remote Site

Redistribution

Network Admin (Loopback1 of R12) is running an application that requires direct access to the Internet resources such as (DNS, Facebook, Google, NTP servers)
On R12 redistribute EIGRP into BGP
Do not redistribute BGP back into your internal EIGRP domain
Ensure that only Network Admin PC (Lo:1) subnet is allowed to get out to the internet
Finance PC#1 should NOT be able to get out on the internet at this point

Configuration:

R12
access-list 1 permit 192.168.21.0 0.0.0.15
route-map NET_ADMIN permit 10
match ip address 1
router bgp 64784
    address-family ipv4
        redistribute eigrp 150 route-map NET_ADMIN
    exit-address-family

R10
router bgp 64784
    address-family ipv4
        neighbor 155.84.74.10 allowas-in
    exit-address-family

R11
router bgp 64784
    address-family ipv4
        neighbor 155.84.74.14 allowas-in
    exit-address-family

Verification:

R10#deb ip bgp ipv4 unicast updates 155.84.74.10
BGP updates debugging is on for neighbor 155.84.74.10 for address family: IPv4 Unicast
*Dec 13 14:45:44.433: BGP(0): 155.84.74.10 rcv UPDATE about 192.168.21.0/28 -- DENIED due to: AS-PATH contains our own AS;

Note: R11 will experience the same symptoms as seen above

PC1#ping 4.2.2.2 re 5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
......
Success rate is 0 percent (0/5)

R12#ping 4.2.2.2 so loo 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/34 ms
San Francisco Group Data Centre

eBGP

Ensure that SERVER#1 is able to reach Global Internet resources (DNS Google Facebook NTP servers)
Do not use NAT for your solution
Do not perform a **mutual** redistribution anywhere

**Configuration:**

```
R13
  router bgp 64784
  address-family ipv4
    redistribute eigrp 150 metric 10
    exit-address-family
```

**Verification:**

**Note: Simple test:**

SERVER1#ping 4.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/28/34 ms

SERVER1#ping 117.3.48.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms

SERVER1#ping 124.13.240.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/15/18 ms

SERVER1#ping 194.35.252.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/38/74 ms
Sydney Business Model HQ

Network Services – NAT

Ensure that private corporate traffic originated from VLAN10, VLAN20, VLAN50 is able to connect to public server (DNS Google Facebook NTP servers)

Do not configure any internal or external routing protocol between R16 and SP#4

R16 must swap the SRC-IP Address in these packets with the IP Address of its Ethernet0/0

R16 must allow multiple concurrent connections

VLAN10 VLAN20 and VLAN50 should be able to reach any prefix on the internet

Please refer to the diagram

All internal EIGRP devices should have a static default route in their routing tables towards R16, see below example on SW6 and SW7:

Configuration:

```
R16
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
route-map DEFAULT permit 10
  match ip address prefix-list DEFAULT
  set metric 10000 10 255 1 1500
router eigrp 250
  redistribute static route-map DEFAULT
ip access-list standard NAT_INTERNAL
  permit 192.168.120.0 0.0.0.255
  permit 192.168.130.0 0.0.0.255
  permit 192.168.140.0 0.0.0.255
ip nat inside source list NAT_INTERNAL interface Ethernet0/0 overload
interface Ethernet1/0
  ip nat inside

interface Ethernet2/0
  ip nat inside

interface Ethernet0/0
  ip nat outside
```

Verification:

```
Note: Before any changes are made on R16. Let’s focus on the Global DNS prefix 4.2.2.2 for testing

SW6#sh ip route | in 0.0.0
SW6#

SW7#sh ip route | in 0.0.0
SW7#

SW6#ping 4.2.2.2 so vl 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.120.106
.....
Success rate is 0 percent (0/5)
```
SERVER4#ping 4.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Note: After the changes have been made

SW6#sh ip route | in 0.0.0
Gateway of last resort is 192.168.100.16 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/258816] via 192.168.100.16, 00:00:11, Vlan567

SW7#sh ip route | in 0.0.0
Gateway of last resort is 192.168.110.16 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/258816] via 192.168.110.16, 00:01:29, Vlan668

SW6#ping 4.2.2.2 so vl 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.120.106
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/12 ms

SW7#ping 4.2.2.2 so vl 20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.130.107
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/18/37 ms

SERVER4#ping 4.2.2.2 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/11/14 ms

R16#sh ip nat translations
Proto Inside global       Inside local       Outside local       Outside global
icmp 155.84.74.25:3  192.168.120.106:3  4.2.2.2:3          4.2.2.2:3
icmp 155.84.74.25:0  192.168.130.107:0  4.2.2.2:0          4.2.2.2:0
icmp 155.84.74.25:2  192.168.140.100:2  4.2.2.2:2          4.2.2.2:2
Network Services – NAT

Ensure that when R16 and R99 goes down VLAN10, VLAN20, VLAN50 users can still reach internet resources.
R17 and R18 should become redundant internet exit points for the SBM-HQ Office.
R17 and R18 must swap the SRC-IP Internal Addresses of VLAN10, VLAN20, VLAN50 packets with the IP Address of its Ethernet10/0.
Do not use “ip nat inside” or “ip nat outside” anywhere in your configuration.
Both routers must allow multiple concurrent connections.
As soon as the connection is restored between R16 and R99 then R16 should resume its role of the main default gateway.
Do not enable NAT on VLAN 78.
Do not perform redistribution between any actively running protocols anywhere in your network.
On R16 disable time and date usually shown in the console messages

Configuration:

R16
no service timestamps log

R17
ip route 0.0.0.0 0.0.0.0 155.84.74.29
route-map DEFAULT permit 10
match ip address prefix-list DEFAULT
set metric 10000 1000 255 1 1500
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
router eigrp 250
redistribute static route-map DEFAULT
ip access-list standard NAT_INTERNAL
permit 192.168.120.0 0.0.0.255
permit 192.168.130.0 0.0.0.255
permit 192.168.140.0 0.0.0.255
ip nat source list NAT_INTERNAL interface Ethernet0/0 overload
interface Ethernet1/0
ip nat enable
interface Ethernet0/0
ip nat enable

R18
ip route 0.0.0.0 0.0.0.0 155.84.74.33
route-map DEFAULT permit 10
match ip address prefix-list DEFAULT
set metric 10000 1000 255 1 1500
ip prefix-list DEFAULT seq 5 permit 0.0.0.0/0
router eigrp 250
redistribute static route-map DEFAULT
ip access-list standard NAT_INTERNAL
permit 192.168.120.0 0.0.0.255
permit 192.168.130.0 0.0.0.255
permit 192.168.140.0 0.0.0.255

ip nat source list NAT_INTERNAL interface Ethernet0/0 overload

interface Ethernet1/0
ip nat enable

interface Ethernet0/0
ip nat enable

Verification:

Note: We know from the previous tasks that R16 is being used as an exit point out to the internet
We know that at this point SW6 and SW7 point towards R16 for 0.0.0.0/0 network
Once again let's focus on The Global DNS prefix 4.2.2.2 for testing

SW6#sh ip route | in 0.0.0
Gateway of last resort is 192.168.100.16 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/258816] via 192.168.100.16, 00:00:11, Vlan567

SW7#sh ip route | in 0.0.0
Gateway of last resort is 192.168.110.16 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/258816] via 192.168.110.16, 00:01:29, Vlan668

Note: Let's have a link failure between R16 and R99

R16(config)#int et 0/0
R16(config-if)#shu
R16(config-if)#
%LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
R16(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down

Note: SW6 and SW7 have chanegd their gateway of last resort towards R17 and R18 as planned

SW6#sh ip route | in 0.0.0.0
Gateway of last resort is 192.168.100.17 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/512256] via 192.168.100.16, 00:00:40, Vlan567

SW7#sh ip route | in 0.0.0.0
Gateway of last resort is 192.168.110.18 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/512256] via 192.168.110.18, 00:00:38, Vlan668
**Note: We can still get out to the internet!**

SW6#ping 4.2.2.2 so vl 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.120.106
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/12 ms

SW7#ping 4.2.2.2 so vl 20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.130.107
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/18/37 ms

SERVER4#ping 4.2.2.2 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/11/14 ms

R18#sh ip nat nvi translations
Pro Source global        Source local        Destin local       Destin global
icmp 155.84.74.34:1    192.168.130.107:1  4.2.2.2:1          4.2.2.2:1
icmp 155.84.74.34:3    192.168.140.100:3  4.2.2.2:3          4.2.2.2:3

R17#sh ip nat nvi translations
Pro Source global        Source local        Destin local       Destin global
icmp 155.84.74.30:4    192.168.120.106:4  4.2.2.2:4          4.2.2.2:4

**Note: Let’s unshut R16 Ethernet 0/0**

R16(config)#int et 0/0
R16(config-if)#no sh
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R16(config-if)#

**Note: Looking good!**

SW6#sh ip route | in 0.0.0
Gateway of last resort is 192.168.100.16 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/258816] via 192.168.100.16, 00:00:11, Vlan567

SW7#sh ip route | in 0.0.0
Gateway of last resort is 192.168.110.16 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/258816] via 192.168.110.16, 00:01:29, Vlan668
Internet Connectivity – SLA

R16 should monitor every 5 seconds reachability to Service Provider#4
Ensure that if there is an unexpected/expected link failure between R16 and R99 then users from VLAN10, VLAN20, VLAN50 are still able to connect to public server (DNS Google Facebook NTP servers) via their redundant gateways R17 and R18 as per the previous task
Do not configure any SLA instances or route tracking on R17 or R18

Configuration:

R16
  no ip route 0.0.0.0 0.0.0.0 155.84.74.26
  ip sla 1
    icmp-echo 155.84.74.26 source-ip 155.84.74.25
    frequency 5
  ip sla schedule 1 life forever start-time now
  track 1 ip sla 1 reachability
  ip route 0.0.0.0 0.0.0.0 155.84.74.26 track 1

Verification:

R16#sh ip sla statistics
IPSLAs Latest Operation Statistics
IPS LA operation id: 1
  Latest RTT: 1 milliseconds
  Latest operation start time: 15:44:23 CET Sun Dec 21 2014
  Latest operation return code: OK
  Number of successes: 6
  Number of failures: 0
  Operation time to live: Forever

R16#sh track 1
Track 1
  IP SLA 1 reachability
    Reachability is Up
    1 change, last change 00:01:20
    Latest operation return code: OK
    Latest RTT (milliseconds) 1
    Tracked by:
      Static IP Routing 0

R16#sh ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
  Operation timeout (milliseconds): 5000
  Type of operation to perform: icmp-echo
  Target address/Source address: 155.84.74.26/155.84.74.25
  Type Of Service parameter: 0x0
  Request size (ARR data portion): 28
  Verify data: No
Vrf Name:
Schedule:
  Operation frequency (seconds): 5 (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 15
  History Filter Type: None

Note: One more time let's simulate a link failure

R16(config)#int et 0/0
R16(config-if)#shu
  %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
R16(config-if)#
R16(config-if)#
R16#sh ip sla statistics
IPSLAs Latest Operation Statistics
IPSLA operation id: 1
  Latest RTT: NoConnection/Busy/Timeout
  Latest operation start time: 15:48:18 CET Sun Dec 21 2014
  Latest operation return code: Timeout
  Number of successes: 42
  Number of failures: 6
  Operation time to live: Forever

Note: Looks like it's all working as expected

SW6#sh ip route | in 0.0.0.0
Gateway of last resort is 192.168.100.17 to network 0.0.0.0
  D*EX 0.0.0.0/0 [170/512256] via 192.168.100.17, 00:00:40, Vlan567

SW7#sh ip route | in 0.0.0.0
Gateway of last resort is 192.168.110.18 to network 0.0.0.0
  D*EX 0.0.0.0/0 [170/512256] via 192.168.110.18, 00:00:38, Vlan668
Note: and re-enable Ethernet 0/0 on R16

R16(config)#int et 0/0
R16(config-if)#no sh
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R16(config-if)#
%TRACK-6-STATE: 1 ip sla 1 reachability Down -> Up
R16(config-if)#

SW6#sh ip route | in 0.0.0
Gateway of last resort is 192.168.100.16 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/258816] via 192.168.100.16, 00:00:11, Vlan567

SW7#sh ip route | in 0.0.0
Gateway of last resort is 192.168.110.16 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/258816] via 192.168.110.16, 00:01:29, Vlan668
**Service Provider #3**

**BGP Communities**

Cisco has recently announced that the Internet prefixes that contain the community value of **91:91** could lead to many dangerous viruses being injected into various networks. Ensure that prefixes using this community value are not permitted to enter SP#3 (R98) infrastructure. You can only filter based on the community value. Do not configure anything under any device interfaces. Facebook Web Server IP Address 117.3.48.150/32 should not longer be visible in R98 RIB (routing table) or FIB (CEF table).

**Configuration:**

```plaintext
R98
  ip community-list standard VIRUS permit 91:91

  route-map VIRUS deny 10
     match community VIRUS

  route-map VIRUS permit 20

  router bgp 28451
    address-family ipv4
      neighbor 66.171.14.6 route-map VIRUS in
    exit-address-family
```

**Verification:**

**Note:** Check what BGP AS is sending prefixes with the **91:91** community value. We can see that these prefixes are being received from SP#7 (R94) and are originated from BGP AS 15789 SP#5 (R91).

```plaintext
R98#sh ip bgp community 91:91
BGP table version is 128, local router ID is 199.53.176.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
   r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
   x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPF validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt; 117.3.0.6/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 <strong>15789</strong> ?</td>
</tr>
<tr>
<td>* &gt; 117.3.16.8/20</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 <strong>15789</strong> ?</td>
</tr>
<tr>
<td>* &gt; 117.3.32.8/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 <strong>15789</strong> ?</td>
</tr>
<tr>
<td>* &gt; 117.3.48.150/32</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 <strong>15789</strong> ?</td>
</tr>
<tr>
<td>* &gt; 117.3.64.8/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 <strong>15789</strong> ?</td>
</tr>
</tbody>
</table>
```

**Note:** There are more prefixes being originated from BGP AS 15789 but we only care about the ones with ‘.3’ in the second octet of their IPv4 IP Address as they are the ones tagged with the **91:91** community value.
R98#sh ip bgpregexp 15789
BGP routing table entry for 117.0.144.0/22, version 116
Paths: (1 available, best #1, table default)
Advertised to update-groups:

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf Weight Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 117.0.32.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>*&gt; 117.0.128.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>*&gt; 117.0.144.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>*&gt; 117.1.0.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 117.3.0.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 117.3.16.0/20</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 117.3.16.0/20</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 117.3.16.0/20</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 117.3.16.0/20</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
</tbody>
</table>

R98#sh ip bgp 117.0.144.0/22
BGP routing table entry for 117.0.144.0/22, version 116
Paths: (1 available, best #1, table default)
Advertised to update-groups:

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf Weight Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 155.84.74.0/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.12/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.16/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>*&gt; 155.84.74.20/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 ?</td>
</tr>
</tbody>
</table>

Note: Ultimately after successful full implementation we should no longer be able to reach Facebook Web Server IPv4 IP Address but still receive all other 117.x.x.x prefixes as long as the 2nd octet of their IPv4 Address is not '.3'
Before we make any changes let’s test and see if we can reach Facebook IP Address

R98#ping 117.3.48.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/50/75 ms
R98#debug ip bgp updates
BGP updates debugging is on for address family: IPv4 Unicast
R98#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R98(config)#int et 0/0
R98(config-if)#no sh
R98(config-if)#^Z
R98#
*Dec 21 15:17:52.278: %SYS-5-CONFIG_I: Configured from console by console
R98#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BGP(0): 66.171.14.6 rcvd UPDATE w/ attr: nexthop 66.171.14.6, origin i, merged path 56775 10001 29737 25432 64784 15789, AS_PATH , community 15789:91
BGP(0): 66.171.14.6 rcvd 117.0.32.0/22
BGP(0): 66.171.14.6 rcvd 117.0.128.0/22
BGP(0): 66.171.14.6 rcvd 117.0.144.0/22
BGP(0): 66.171.14.6 rcvd UPDATE w/ attr: nexthop 66.171.14.6, origin ?, merged path 56775 10001 29737 25432 64784 15789, AS_PATH , community 91:91
BGP(0): 66.171.14.6 rcvd 117.3.0.0/22
BGP(0): 66.171.14.6 rcvd 117.3.16.0/22 -- DENIED due to: route-map; 
BGP(0): 66.171.14.6 rcvd 117.3.32.0/22 -- DENIED due to: route-map; 
BGP(0): 66.171.14.6 rcvd 117.3.48.150/32 -- DENIED due to: route-map; 
BGP(0): 66.171.14.6 rcvd 117.3.64.0/22 -- DENIED due to: route-map; 
BGP(0): Revise route installing 1 of 1 routes for 117.0.32.0/22 -> 66.171.14.6(global) to main IP table
BGP(0): Revise route installing 1 of 1 routes for 117.0.128.0/22 -> 66.171.14.6(global) to main IP table
BGP(0): Revise route installing 1 of 1 routes for 117.0.144.0/22 -> 66.171.14.6(global) to main IP table
BGP(0): Revise route installing 1 of 1 routes for 117.1.0.0/22 -> 66.171.14.6(global) to main IP table
R98#un all
All possible debugging has been turned off

Note: Exactly what we want!

R98#sh ip bgp regexp _15789$
BGP table version is 327, local router ID is 199.53.176.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-path, c RIB-compressed, 
Origin codes: i - IGP, e - BGP, ? - incomplete 
RPKI validation codes: V valid, I invalid, N Not found 
Network          Next Hop            Metric LocPrf Weight Path
*>  117.0.32.0/22    66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  117.0.128.0/22   66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  117.0.144.0/22   66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  117.1.0.0/22     66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  155.84.74.8/30   66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  155.84.74.12/30  66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  155.84.74.16/30  66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i
*>  155.84.74.20/30  66.171.14.6                            0 56775 10001 29737 25432 64784 15789 i

R98#ping 117.3.48.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
.......
Success rate is 0 percent (0/5)

R98#ping 117.0.32.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.0.32.150, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/30/37 ms
Service Provider#6

BGP Communities

Google Server BGP Global prefix must have an "Internet" community value assigned to it
Do not make any configuration changes under any neighbor statement or perform redistribution anywhere in your configuration

Configuration:

```
R93
route-map GOOGLE permit 10
  set community internet
router bgp 10001
  address-family ipv4
    network 124.13.240.150 mask 255.255.255.255 route-map GOOGLE
```

Verification:

**Note:** Let's first check how the Google Server prefix is seen at the moment..... no community value at all

```
R93#sh ip bgp 124.13.240.150/32
BGP routing table entry for 124.13.240.150/32, version 8
  Paths: (1 available, best #1, table default)
    Advertised to update-groups:
      1          2
    Refresh Epoch 1
    Local
      0.0.0.0 from 0.0.0.0 (124.19.254.150)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local, best
      rx pathid: 0, tx pathid: 0x0

R91#sh ip bgp 124.13.240.150/32
BGP routing table entry for 124.13.240.150/32, version 17
  Paths: (2 available, best #2, table default)
    Advertised to update-groups:
      1
    Refresh Epoch 1
      64784 64784 64784 64784 64784 64784 10001
      155.84.74.9 from *155.84.74.9 (192.10.10.10)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

```
**Note:** and after the changes are made

R93#sh ip bgp 124.13.240.150/32
BGP routing table entry for 124.13.240.150/32, version 170
Paths: (1 available, best #1, table default)
   Advertised to update-groups:
     1 2
   Refresh Epoch 1
Local
  0.0.0.0 from 0.0.0.0 (124.19.254.150)
     Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local, best
Community: internet
   rx pathid: 0, tx pathid: 0x0

R91#sh ip bgp 124.13.240.150/32
BGP routing table entry for 124.13.240.150/32, version 255
Paths: (2 available, best #2, table default)
   Advertised to update-groups:
     1
   Refresh Epoch 1
64784 64784 64784 64784 64784 64784 64784 10001
155.84.74.9 from *155.84.74.9 (192.10.10.10)
     Origin IGP, localpref 100, valid, external
Community: internet
   rx pathid: 0, tx pathid: 0
Refresh Epoch 1
64784 10001
155.84.74.13 from *155.84.74.13 (192.11.11.11)
     Origin IGP, localpref 100, valid, external, best
Community: internet
   rx pathid: 0, tx pathid: 0x0
Service provider #5

BGP Aggregation Summary Only

SP#5 must advertise an aggregate prefix 197.0.0.0/17 and must suppress all component prefixes
No other devices but R96 should see the specific prefixes that make up the summary
Do not use suppress or unsuppress map for your solution
Ping the Network Admin IP Address 197.0.112.150/32 to test

Configuration:

```
R96
router bgp 25432
    address-family ipv4
        aggregate-address 197.0.0.0 255.255.128.0 summary-only
        exit-address-family
```

Verification:

```
Note: Based on the subnet mask prefixes 197.0.128.0/22 and 197.0.144.0/22 will not fall into aggregation which is perfectly fine
```

```
R96#sh ip bgp regexp ^$ 
BGP table version is 186, local router ID is 197.0.144.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, 
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, 
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network          Next Hop            Metric LocPrf Weight Path
*>  86.191.16.0/30   0.0.0.0                  0         32768 ?
*>  155.84.74.0/30   0.0.0.0                  0         32768 ?
s>  197.0.0.0/22    0.0.0.0                  0         32768 i
*>  197.0.0.0/17     0.0.0.0                  0         32768 ?
s>  197.0.0.16/20    0.0.0.0                  0         32768 ?
s>  197.0.0.32/22    0.0.0.0                  0         32768 ?
s>  197.0.0.48/22    0.0.0.0                  0         32768 ?
s>  197.0.0.64/22    0.0.0.0                  0         32768 ?
s>  197.0.0.80/22    0.0.0.0                  0         32768 ?
s>  197.0.0.96/22    0.0.0.0                  0         32768 ?
s>  197.0.0.112.150/32  0.0.0.0                  0         32768 ?
*>  197.0.128.0/22   0.0.0.0                  0         32768 ?
*>  197.0.144.0/22   0.0.0.0                  0         32768 ?
```

```
R92#sh ip bgp regexp _25432$
BGP table version is 206, local router ID is 110.1.16.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, 
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, 
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network          Next Hop          Metric LocPrf Weight Path
*>  155.84.74.0/30   86.191.16.5                  0 29737 25432 ?
*>  197.0.0.0/17     86.191.16.5                  0 29737 25432 i
*>  197.0.0.128.0/22 86.191.16.5                  0 29737 25432 ?
*>  197.0.144.0/22   86.191.16.5                  0 29737 25432 ?
```
**Note:** Now test if we can still get to places for example Network Admin IP Address.... Good!

R92#ping 197.0.112.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/21/25 ms

R16#ping 197.0.112.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/40/46 ms

R20#ping 197.0.112.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/49/84 ms

R12#ping 197.0.112.150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds: 
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10 ms
Service provider #6

BGP Aggregation Suppress Map

On R93 advertise an aggregate route for 124.0.0.0/11 prefixes so that Google Server prefix is separately advertised in addition to the summary route
Do not use ACL to accomplish this task

**Configuration:**

```
R93
ip prefix-list NOTAGG seq 5 permit 124.13.240.150/32
route-map NOTAGG deny 10
  match ip address prefix-list NOTAGG
route-map NOTAGG permit 20
router bgp 10001
  address-family ipv4
    aggregate-address 124.0.0.0 255.224.0.0 summary-only suppress-map NOTAGG
  exit-address-family
```

**Verification:**

```
Note: This time we will go for R95 to test from .... Below is before the changes:

R95#sh ip bgp regexp _10001$
BGP table version is 205, local router ID is 217.0.128.150
Status codes: s suppressed, d damp ed, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter, x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPF validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &gt; 86.13.117.119/32</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 86.191.16.4/30</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 86.191.16.8/30</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.16.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.48.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.64.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.80.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.96.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.112.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.128.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.0.144.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.1.0.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 110.1.16.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.1.16.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.3.32.144/29</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.5.64.128/25</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.7.128.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.9.196.8/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.11.224.144/28</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>* &gt; 124.13.240.150/32</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
</tbody>
</table>
```

<Output omitted>
R93#sh ip bgp regexp ^$  
BGP table version is 212, local router ID is 124.19.254.150  
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,  
x best-external, a additional-path, c RIB-compressed,  
Origin codes: i - IGP, e - RGP, ? - incomplete  
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 86.13.117.119/32</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 86.191.16.4/30</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>r&gt; 86.191.16.8/30</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.16.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.48.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.64.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.80.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.96.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.112.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.128.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.0.144.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.1.0.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 110.1.16.0/24</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 124.0.0.0/11</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.3.32.144/29</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.5.64.128/25</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.7.128.0/24</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.9.196.0/24</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.11.224.144/28</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.13.240.150/32</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.15.248.128/27</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.17.252.0/24</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s&gt; 124.19.254.128/26</td>
<td>0.0.0.0</td>
<td>32768</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** and after the change...Great, the summary is there along with the Google Server prefix

R95#sh ip bgp regexp _10001_  
BGP table version is 215, local router ID is 217.0.128.150  
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,  
x best-external, a additional-path, c RIB-compressed,  
Origin codes: i - IGP, e - RGP, ? - incomplete  
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 86.13.117.119/32</td>
<td>86.191.16.10</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 86.191.16.4/30</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 86.191.16.8/30</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.16.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.48.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.64.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.80.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.96.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.112.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.128.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.0.144.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.1.0.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 110.1.16.0/24</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
<tr>
<td>*&gt; 124.0.0.0/11</td>
<td>66.171.14.13</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>7</td>
</tr>
</tbody>
</table>

*Output omitted*...
Redistribution – Internet Connectivity

R14 must be able to access Internet resources via its Ethernet outside connection to SP#6 (R93)
Do not configure any routing protocol between R14 and R92 or R14 and R93
Prefix 140.60.88.28/30 should be redistributed into BGP on R93
Do not use ACL or prefix list for this task
Ensure no other prefix is redistributed by default into BGP
R14 except for its Local and Connected routes should have the following entry in its routing table:
S* 0.0.0.0/0 [1/0] via 140.60.88.30

Configuration:

R93
route-map CONNECTED permit 10
match interface Ethernet1/0
router bgp 10001
  address-family ipv4
    redistribute connected route-map CONNECTED
    exit-address-family

R14
ip route 0.0.0.0 0.0.0.0 140.60.88.30

Verification:

R14(tcl)#tclsh
R14(tcl)#foreach CCIE {+>117.3.48.150
+>63.69.0.150
+>124.13.240.150
+>75.6.224.150
+>194.35.252.7
+>4.2.2.2
+>} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 14/16/22 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 63.69.0.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/21/28 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 124.13.240.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/4/9 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 75.6.224.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/5/9 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/5 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/5 ms
R14(tcl)#tclquit

232 | Page
R14(tcl)#foreach CCIE {
  ->117.3.48.150
  ->63.69.0.150
  ->124.13.240.150
  ->75.6.224.150
  ->194.35.252.7
  ->4.2.2.2
  ->} { traceroute $CCIE probe 1 }
Type escape sequence to abort.

**Tracing the route to 117.3.48.150**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 0 msec
2 86.191.16.10 9 msec
3 86.191.16.5 47 msec
4 86.191.16.1 15 msec
5 155.84.74.1 23 msec
6 192.168.102.22 87 msec
7 155.84.74.45 45 msec
Type escape sequence to abort.

**Tracing the route to 63.69.0.150**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 1 msec
2 86.191.16.10 62 msec
3 86.191.16.5 142 msec
Type escape sequence to abort.

**Tracing the route to 124.13.240.150**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 10 msec
Type escape sequence to abort.

**Tracing the route to 75.6.224.150**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 7 msec
2 66.171.14.9 1 msec
Type escape sequence to abort.

**Tracing the route to 194.35.252.7**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 3 msec
2 66.171.14.9 5 msec
3 66.171.14.14 2 msec
Type escape sequence to abort.

**Tracing the route to 4.2.2.2**
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.30 7 msec
2 66.171.14.9 9 msec
3 66.171.14.5 1 msec
R14(tcl)#tclquit
IPv6 Table

**Note:**

CIDR Prefixes[edit]

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/128</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/127</td>
<td>Point-to-point links (inter-router)</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/124</td>
<td>Point-to-point links (inter-router)</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/120</td>
<td>Point-to-point links (inter-router)</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/116</td>
<td>Point-to-point links (inter-router)</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/112</td>
<td>Point-to-point links (inter-router)</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/104</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/100</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/96</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/92</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/88</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/84</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/80</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/76</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/72</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/68</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/64</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/60</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/56</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/52</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/44</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/40</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/36</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/32</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/28</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/24</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/20</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/16</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/12</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/8</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/4</td>
<td>Single end-points and loopback</td>
</tr>
<tr>
<td>2001:0db8:0123:4567:89ab:cdef:1234:5678/0</td>
<td>Single end-points and loopback</td>
</tr>
</tbody>
</table>
**Note:**

**EIGRP IPv6 VRF-Lite**

The EIGRP IPv6 VRF Lite feature:
- provides EIGRP IPv6 support for multiple VRFs. EIGRP for IPv6 can operate in the context of a VRF.
- provides separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless it is explicitly configured.
- simplifies the management and troubleshooting of traffic belonging to a specific VRF.
- is available only in EIGRP named configurations.

**IPv6 Enable command**

`interface X/Y ipv6 enable end`

Issuing this simple command on a default configured interface starts a few things. Firstly the router boots up its process for associating the link-local address to the physical interface. Secondly it boots up the IPv6 database and a few other processes.

**Router not running IPv6:**

```
R4#show processes inc v6
  88 Wwe 61412A40 0 1 0 5696/6000 0 IPv6 ping proc
  165 Wve 614141FC 0 1 0 8624/9000 0 IPv6 RIB Clean up
  165 Wve 61403618 0 1 0 8576/6000 0 IPv6 RIB Event H
  202 Wve 63A82668 0 1 0 5612/6000 0 IPSECv6 PS Proc
```

**Router running IPv6 enable command:**

```
R4#show processes inc v6
  88 Wve 6141A2A0 0 1 0 5696/6000 0 IPv6 ping proc
  93 Wve 616D0038 0 1 4 3000 7520/9000 0 IPv6 IDB
  134 Lve 6130D017C 4 35 114 8220/9000 0 IPv6 background
  165 Wve 614141FC 0 1 0 8624/9000 0 IPv6 RIB Clean up
  166 Wve 61403618 4 6 666 8388/9000 0 IPv6 RIB Event H
  191 Wve 6162700A 0 1 35 728/6000 0 IPv6 Addr Reg
  202 Wve 63A82668 0 1 0 5612/6000 0 IPSECv6 PS Proc
  230 Wve 61C82654 0 9 0 8576/6000 0 IPv6 Input
  252 Wve 6130D220 80 4 20000 6652/9000 0 IPv6 ND
```

Thirdly it sets up the MTU for the interface that just came up/up. Fourthly it adds the Multicast group FF02::1

These steps can be followed via debugs:

```
DEBUG IPv6 Enable Command
Jan 21 20:01:23.279: %EXEC:IPv6ADVR: Adding default link-local on FastEthernet0/0
Jan 21 20:01:23.279: %EXEC:IPv6ADVR: Adding operating owner default link-local on FastEthernet0/0
Jan 21 20:01:23.237: %EXEC:IPv6ADVR: IPv6 Address DB initialized on FastEthernet0/0
Jan 21 20:01:31.236: %EXEC:IPv6IFF: F00/12 L3 dwn, L3 dwn/dis: set opp state to enabled: default link-local
Jan 21 20:01:31.236: %EXEC:IPv6IFF: F00/12 L3 dwn, L3 dwn/dis: set opp state to enabled: default link-local
Jan 21 20:01:31.236: %EXEC:IPv6IFF: F00/12 L3 dwn, L3 dwn/dis: set opp state to enabled: default link-local
Jan 21 20:01:31.236: %EXEC:IPv6IFF: F00/12 L3 dwn, L3 dwn/dis: set opp state to enabled: default link-local
```

The interface transitions into fully operational state, and starts sending packets.
It attempts to do a neighbor discovery with its link-local address via Neighbor solicitation.
It sends multiple Multicast listeners to the well-known FF02::1 address
It sends a packet advertisement notifying everyone on the link at which MAC address it can be found.
The `ipv6 enable` command as seen above has a quite a few steps behind it.
San Francisco Group HQ

OSPFv3

Configure AREA0 OSPFv3 process ID 100
Use Loopback0 address as the OSPFv6 router ID
Advertise Loopback 0 interfaces of all devices into OSPFv3
Ensure Loopback0 of R8 and R9 is never able send any OSPF packets
Ensure R8 is a DR and R9 BDR on its P2P link
On R8 and R9 do not use "ipv6 ospf" statement anywhere in your configuration
Refer to IPv6 Topology #1

**Configuration:**

**R8**

```
ipv6 unicast-routing
ipv6 cef
ipv6 router ospf 100
    router-id 192.8.8.8
    passive-interface Loopback0

interface Loopback0
    ospfv3 100 ipv6 area 0

interface Ethernet1/0
    ospfv3 100 ipv6 area 0
    ospfv3 100 priority 255

interface Ethernet3/0
    ospfv3 100 ipv6 area 0
```

**R9**

```
ipv6 unicast-routing
ipv6 cef

router ospfv3 100
    router-id 192.9.9.9
    passive-interface Loopback0

interface Loopback0
    ospfv3 100 ipv6 area 0

interface Ethernet1/0
    ospfv3 100 ipv6 area 0
    ospfv3 100 priority 254

interface Ethernet2/0
    ospfv3 100 ipv6 area 0
```
R10
ipv6 unicast-routing
ipv6 cef

ipv6 router ospf 100
  router-id 192.10.10.10

interface Loopback0
  ipv6 ospf 100 area 0

interface Ethernet1/0
  ipv6 ospf 100 area 0

R11
ipv6 unicast-routing
ipv6 cef

ipv6 router ospf 100
  router-id 192.11.11.11

interface Loopback0
  ipv6 ospf 100 area 0

interface Ethernet3/0
  ipv6 ospf 100 area 0

SW1
ipv6 unicast-routing
ipv6 cef

ipv6 router ospf 100
  router-id 192.101.101.101

interface Loopback0
  ipv6 ospf 100 area 0

interface Ethernet0/0
  ipv6 ospf 100 area 0

interface Vlan118
  ipv6 ospf 100 area 0

SW2
ipv6 unicast-routing
ipv6 cef

ipv6 router ospf 100
  router-id 192.102.102.102

interface Loopback0
  ipv6 ospf 100 area 0

interface Ethernet0/0
  ipv6 ospf 100 area 0

interface Vlan119
  ipv6 ospf 100 area 0
Verification:

R8#sh ipv6 protocols
IPv6 Routing Protocol is "ospf 100"
   Router ID 192.8.8.8
   Number of areas: 1 normal, 0 stub, 0 nssa
   Interfaces (Area 0):
      Loopback0
      Ethernet3/0
      Ethernet1/0
   Redistribution:
      None

R8#show ipv6 ospf neighbor
OSPFv3 Router with ID (192.8.8.8) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.101.101.101   1   FULL/BDR        00:00:31    16              Ethernet3/0
192.9.9.9       254   FULL/BDR        00:00:34    7               Ethernet1/0

R8#show ipv6 ospf interface eth1/0
Ethernet1/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:801, Interface ID 7
   Area 0, Process ID 100, Instance ID 0, Router ID 192.8.8.8
   Network Type BROADCAST, Cost: 10
   Transmit Delay is 1 sec,
   State DR, Priority 255
   Designated Router (ID) 192.8.8.8, local address FE80::A8BB:CCFF:FE00:801
   Backup Designated router (ID) 192.9.9.9, local address FE80::A8BB:CCFF:FE00:901
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:08
   Graceful restart helper support enabled
   Index 1/2/2, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 6
   Last flood scan time is 0 msec, maximum is 1 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
   Supress hello for 0 neighbor(s)

R9#show ipv6 ospf neighbor
OSPFv3 Router with ID (192.9.9.9) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.102.102.102   1   FULL/DR        00:00:37    16              Ethernet2/0
192.8.8.8       255   FULL/DR        00:00:32    7               Ethernet1/0
R9#show ipv6 ospf interface eth1/0

Ethernet1/0 is up, line protocol is up
Link Local Address FE80::A8BB:CCFF:FE00:901, Interface ID 7
Area 0, Process ID 100, Instance ID 0, Router ID 192.9.9.9
Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 254

Designated Router (ID) 192.8.8.8, local address FE80::A8BB:CCFF:FE00:801
Backup Designated router (ID) 192.9.9.9, local address FE80::A8BB:CCFF:FE00:901

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Graceful restart helper support enabled
Index 1/2/2, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 4
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1

Adjacent with neighbor 192.8.8.8 (Designated Router)

Note: Test reachability between two furthest prefixes, R10 and R11 Loopback0 IPv6 Addresses

R10#ping ipv6 2010:CAFE:11::11 so 2010:CAFE:10::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:CAFE:11::11, timeout is 2 seconds:
Packet sent with a source address of 2010:CAFE:10::10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
**RIP/OSPFv3/Redistribution**

Configure RIPng between R8 and R96
Advertise Loopback 307 (Network Admin) of R96 into RIP
Mutually redistribute between both protocols on R8 including connected interfaces
Network Admin (2001:197:150::150/128) within the SP#1 network should be able to reach San Francisco Group HQ internal DNS Lo:0 of R11 (2010:CAFE:11::11/128) and the Finance User Lo:0 of R10 (2010:CAFE:10::10/128)

**Configuration:**

**R8**
ipv6 router rip RIPng
interface Ethernet0/0
ipv6 rip RIPng enable
router ospfv3 100
   address-family ipv6 unicast
      redistribute rip RIPng include-connected
      exit-address-family
ipv6 router rip RIPng
redistribute ospf 100 metric 5 include-connected

**R96**
ipv6 unicast-routing
ipv6 cef
ipv6 router rip RIPng
interface Loopback307
ipv6 rip RIPng enable
interface Ethernet0/0
ipv6 rip RIPng enable

**Verification:**

R8#sh ipv6 route rip
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDP - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, ls - LISP site
ld - LISP dyn-EID, a - Application
R   2001:197:150::150/128 [120/2]
   via FE80::A8BB:CCFF:FE00:6000, Ethernet0/0
R8#ping ipv6 2001:197:150::150
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:197:150::150, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/21 ms

R8#sh ipv6 rip database
RIP process "RIPng", local RIB
  2001:197:150::150/128, metric 2, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:6000, expires in 169 secs
  2001:CC00:CCCC:CAFE::/126, metric 2
    Ethernet0/0/FE80::A8BB:CCFF:FE00:6000, expires in 169 secs

Note: Prior to redistribution

R96#show ipv6 rip database
RIP process "RIPng", local RIB
  2001:CCCC:CAFE::/126, metric 2
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 167 secs

Note: After redistribution R96 has received all relevant IPv6 OSPFv3 prefixes from R8

R96#sh ipv6 rip database
RIP process "RIPng", local RIB
  2001:CC1E:CAFE::/126, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2001:CCCC:CAFE::/126, metric 2
    Ethernet0/0/FE80::A8BB:CCFF:FE00:6000, expires in 160 secs
  2010:CAFE:8::8/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2010:CAFE:9::9/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2010:CAFE:10::10/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2010:CAFE:11::11/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2010:CAFE:101::101/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
  2010:CAFE:102::102/128, metric 6, installed
    Ethernet0/0/FE80::A8BB:CCFF:FE00:800, expires in 160 secs
```
R96#sh ipv6 route rip
IPv6 Routing Table - default - 16 entries
Codes: C - Connected, L - Local1, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1s - LISP site
1d - LISP dyn-EID, a - Application
R  2001:CC1E:CAFE::/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2001:CC1E:CAFE::4/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2001:CC1E:CAFE::8/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2001:CC1E:CAFE::10/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2001:CC1E:CAFE::14/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2001:CC1E:CAFE::18/126 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:8::8/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:9::9/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:10::10/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:11::11/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:101::101/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
R  2010:CAFE:102::102/128 [120/6] via FE80::A8BB:CCFF:FE00:800, Ethernet0/0
```

```
R96#sh ipv6 protocols
IPv6 Routing Protocol is "ospf 100"
Router ID 192.8.8.8
Autonomous system boundary router
Number of areas: 1 normal, 0 stub, 0 nssa
Interfaces (Area 0):
  Loopback0
  Ethernet3/0
  Ethernet1/0
Redistribution:
  Redirecting protocol rip RIPng include-connected
IPv6 Routing Protocol is "rip RIPng"
Interfaces:
  Ethernet0/0
Redistribution:
  Redirecting protocol ospf 100 with metric 5 (internal, external 1 & 2, nssa-external 1 & 2)
  include-connected

Note: And vice versa OSPFv3 domain should now be able to reach RIPng networks

R10#show ipv6 route ospf
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
OE2 2001:197:150::150/128 [110/20]
OE2 2001:CCCC:CAFE::/126 [110/20]
```
R1#show ipv6 route ospf | in OE2
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
OE2  2001:197:150::150/128 [110/20]
OE2  2001:CCCC:CAFE::126 [110/20]

R1#sh ipv6 ospf database | be Type-5

<table>
<thead>
<tr>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.8.8.8</td>
<td>596</td>
<td>0x80000001</td>
<td>2001:197:150::150/128</td>
</tr>
<tr>
<td>192.8.8.8</td>
<td>596</td>
<td>0x80000001</td>
<td>2001:CCCC:CAFE::126</td>
</tr>
</tbody>
</table>

R8#sh ipv6 ospf 100
Routing Process "ospfv3 100" with ID 192.8.8.8
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
\[It is an autonomous system boundary router\]
\[Rip RIPng include-connected\]
\(<Output omitted>\)

**Note:** We will check if we can get to RIPng prefixes from R10 and R11

R10#ping 2001:197:150::150 so loo 0 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:197:150::150, timeout is 2 seconds:
Packet sent with a source address of 2010:CAFE:10::10
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/6 ms

R11#ping 2001:197:150::150 so 2010:CAFE:11::11 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:197:150::150, timeout is 2 seconds:
Packet sent with a source address of 2010:CAFE:11::11
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/4/6 ms
OSPFv3 Metric

R8 is often taken for maintenance
Make sure that when R8 is brought back from the maintenance and put back on the network then it will advertise the following metric values to its neighbours for 60 seconds during the boot up process and thus become the least preferred routing path
- Inter-area LSAs metric 700000
- External LSAs metric 800000

Configuration:

R8
router ospfv3 100
max-metric router-lsa inter-area-lsas 700000 external-lsa 800000 on-startup 60

Verification:

Note: As we do not have any other OSPF areas except for Area0 we will not be able to test ‘inter-area-lsas’ however we have got an external Type 2 LSA coming from RIPng domain

R1#show ipv6 route 2001:197:150::150/128
Routing entry for 2001:197:150::150/128
Known via "ospf 100", distance 110, metric 20, type extern 2
Route count is 1/1, share count 0
Routing paths:
FE80::A8BB:CCFF:FE00:3400, Ethernet3/0
Last updated 00:07:20 ago

Note: Below output shows R8 after changes have been applied locally

R8#show ipv6 ospf 100
Routing Process "ospfv3 100" with ID 192.8.8.8
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Originating router-LSAs with maximum metric
  Condition: on startup for 60 seconds, State: inactive
  Advertise inter-area LSAs with metric 700000
  Advertise external LSAs with metric 800000
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
<Output omitted>

Note: and R9 with defaults

R9#show ipv6 ospf 100
Routing Process "ospfv3 100" with ID 192.9.9.9
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
<Output omitted>
**Note:** Let’s save and reload R8 and see what happens....

R8#wr
R8#reload
Proceed with reload? [confirm]Y

<br/>

**Note:** While R8 is rebooting let’s pick R11 and check IPv6 Network Admin Prefix coming from the RIPng domain

R11#show ipv6 route 2001:197:150::150/128
Routing entry for 2001:197:150::150/128
Known via “ospf 100”, distance 110, metric 800000, type extern 2
Route count is 1/1, share count 0
Routing paths:
    FE80::A8BB:CCFF:FE00:3400, Ethernet3/0
        Last updated 00:00:00 ago

R11#show ipv6 route 2001:197:150::150/128
Routing entry for 2001:197:150::150/128
Known via “ospf 100”, distance 110, metric 800000, type extern 2
Route count is 1/1, share count 0
Routing paths:
    FE80::A8BB:CCFF:FE00:3400, Ethernet3/0
        Last updated 00:00:58 ago

**Note:** As expected, it took 60 seconds for R8 to start advertising correct metric to its OSPFv3 neighbours

R11#show ipv6 route 2001:197:150::150/128
Routing entry for 2001:197:150::150/128
Known via “ospf 100”, distance 110, metric 20, type extern 2
Route count is 1/1, share count 0
Routing paths:
    FE80::A8BB:CCFF:FE00:3400, Ethernet3/0
        Last updated 00:00:00 ago
Note:

OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. OSPFv3 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPFv3.

When OSPFv3 runs on IPv6, OSPFv3 requires the IPv6 authentication header (AH) or IPv6 ESP header to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH and ESP extension headers can be used to provide authentication and confidentiality to OSPFv3.

To use the IPsec AH, you must enable the `ipv6 ospf authentication` command.

To use the IPsec ESP header, you must enable the `ipv6 ospf encryption` command.

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value).

IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area.

For higher security, you should configure a different policy on each interface configured with IPsec.

If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

*directly from Cisco website*
**OSPFv3 Authentication**

Configure Area0 with IPsec authentication
Use message digest 5, a security policy index of 300 with the key of
**DEC0DECC1E0DBA11B0B0BBEDB00B00**
Do not use interface level command on R8 and R9
For increased security an SPI policy index between SW1 – R10 and SW2 – R11 should be **301** and **302** respectively

Configuration:

```
R8
router ospfv3 100
  area 0 authentication ipsec spi 300 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00

R9
router ospfv3 100
  area 0 authentication ipsec spi 300 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00

R10
  interface Ethernet1/0
    ipv6 ospf authentication ipsec spi 301 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00

R11
  interface Ethernet3/0
    ipv6 ospf authentication ipsec spi 302 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00

SW1
  interface Ethernet0/0
    ipv6 ospf authentication ipsec spi 301 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00
    interface Vlan118
      ipv6 ospf authentication ipsec spi 300 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00

SW2
  interface Ethernet0/0
    ipv6 ospf authentication ipsec spi 302 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00
    interface Vlan119
      ipv6 ospf authentication ipsec spi 300 md5 DEC0DECC1E0DBA11B0B0BBEDB00B00
```

Verification:
R8#show ipv6 ospf 100
Routing Process "ospfv3 100" with ID 192.8.8.8
<br>Area BACKBONE(0)
Number of interfaces in this area is 3
  MD5 Authentication, SPI 300
  SPF algorithm executed 14 times
Number of LSA 26, Checksum Sum 0x0BF490
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

SW1#show ipv6 ospf interface ethernet 0/0
Ethernet0/0 is up, line protocol is up (connected)
  Link Local Address FE80::A8BB:CCFF:FE00:3300, Interface ID 15
  Area 0, Process ID 100, Instance ID 0, Router ID 192.101.101.101
  Network Type BROADCAST, Cost: 10
  MD5 authentication SPI 301, secure socket UP (errors: 0)
<br>
R10#show crypto ipsec policy
Crypto IPSec client security policy data
  Policy name: OSPFFv3-301
  Policy refcount: 1
  Inbound AH SPI: 301 (0x12D)
  Outbound AH SPI: 301 (0x12D)
  Inbound AH Key: DECODECC1E00DBA11B0BBEDB00B00
  Outbound AH Key: DECODECC1E00DBA11B0BBEDB00B00
  Transform set: ah-md5-hmac

Note: Similar output should be seen between SW2 and R11
OSPFv3 HSRP

R8 should be the active device for the group 101 and R9 should be the active device for the group 201. Use a value of 120 for the priority.

Track interface Ethernet3/0 IPv6 routing of R8 and ensure that when it goes down R9 will take over HSRP active – use any value for tracking as long as it meets the criteria stated in the question. If Loopback0 "Internal DNS" of R11 becomes unreachable on R9 then ensure R8 will take over HSRP active role – use any value for tracking as long as it meets the criteria stated in the question.

R8 and R9 will take over back their active roles for their respective groups after delay of 30 seconds. Authenticate both devices using a password of "ese" – without the quotes. Do not use any form of encryption.

You are not allowed to create any new IPv6 addresses for this task.

Configuration:

```
R8
interface Ethernet1/0
  standby version 2
  standby 101 ipv6 autoconfig
  standby 101 priority 120
  standby 101 preempt delay minimum 30
  standby 101 authentication ese
  standby 101 track 1 decrement 90
  standby 201 ipv6 autoconfig
  standby 201 preempt
  standby 201 authentication ese

track 1 interface Ethernet3/0 ipv6 routing
```

```
R9
interface Ethernet1/0
  standby version 2
  standby 101 ipv6 autoconfig
  standby 101 preempt
  standby 101 authentication ese
  standby 201 ipv6 autoconfig
  standby 201 priority 120
  standby 201 preempt delay minimum 30
  standby 201 authentication ese
  /standby 201 track 1 decrement 90

track 1 ipv6 route 2010:CAFE:11::11/128 reachability
```
**Verification:**

R8#show standby brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>P</th>
<th>State</th>
<th>Active</th>
<th>Standby</th>
<th>Virtual IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>101</td>
<td>120</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>FE80::A8BB:CCFF:FE00:901</td>
<td>FE80::5:73FF:FEA0:65</td>
</tr>
<tr>
<td>Et1/0</td>
<td>201</td>
<td>100</td>
<td>P</td>
<td>Standby</td>
<td>FE80::A8BB:CCFF:FE00:801</td>
<td>local</td>
<td>FE80::5:73FF:FEA0:65</td>
</tr>
</tbody>
</table>

R9#show standby brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>P</th>
<th>State</th>
<th>Active</th>
<th>Standby</th>
<th>Virtual IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>101</td>
<td>100</td>
<td>P</td>
<td>Standby</td>
<td>FE80::A8BB:CCFF:FE00:801</td>
<td>local</td>
<td>FE80::5:73FF:FEA0:65</td>
</tr>
<tr>
<td>Et1/0</td>
<td>201</td>
<td>120</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>FE80::A8BB:CCFF:FE00:801</td>
<td>FE80::5:73FF:FEA0:C9</td>
</tr>
</tbody>
</table>

R9#show track 1

**IPv6 route 2010:CAFE:11::11/128 reachability**

Reachability is Up (OSPF)

1 change, last change 00:01:42
First-hop interface is Ethernet2/0
Tracked by:

**Note:** Let's begin testing: Track 1

R8#show track 1

**Interface Ethernet3/0 ipv6 routing**

IPv6 routing is Up
1 change, last change 00:02:23
Tracked by:

**HSRP Ethernet1/0 201**

R8#debug track st

track state debugging enabled for track 1
R8#debug standby events
HSRP Events debugging is on
R8#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#int et 3/0
R8(config-if)#shu
R8(config-if)#

track-sta (1) IPv6 address change on Ethernet3/0
track-sta (1) IPv6 address change on Ethernet3/0
track-sta (1) Change #2 interface Et3/0, ipv6 routing Up->Down
*Dec 22 19:37:19.103: TRACK-6-STATE: 1 interface Et3/0 ipv6 routing Up -> Down
HSRP: Et1/0 Grp 101 Track 1 object changed, state Up -> Down

HSRP: Et1/0 Grp 101 Priority 120 -> 30

*Dec 22 19:37:19.111: %DUAL-5-NBRCHANGE: EIGRP-IPv4 150: Neighbor 192.168.10.6 (Ethernet3/0) is down: interface down

HSRP: Et1/0 Grp 101 Active: j/Coup rcvd from higher pri router (10D::ABBB:CCFF:FE00:901)

HSRP: Et1/0 Grp 101 Active router is FE80::ABBB:CCFF:FE00:901, was local

*Dec 22 19:37:19.956: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 101 state Active -> Speak

HSRP: Et1/0 Grp 101 MAC addr update Delete from SMF 0005.73a0.0065

HSRP: Et1/0 Grp 101 Deactivating MAC 0005.73a0.0065

*Dec 22 19:37:31.497: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 101 state Speak -> Standby

R9(config-if)#do u all
All possible debugging has been turned off

R9#debug track state 1
track state debugging enabled for track 1

*Dec 22 19:38:45.203: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 101 state Active -> Speak

R9#debug standby events

*Dec 22 19:39:00.828: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 101 state Standby -> Active

R9#un all
All possible debugging has been turned off
**Note:** and now Track 2

R11>en
R11>conf t
Enter configuration commands, one per line. End with CNTL/Z.
R11(config)#int lo0 0
R11(config-if)#shu
R11(config-if)#
*Dec 22 19:42:59.902: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
*Dec 22 19:43:00.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down

R9#debug track state 1
track state debugging enabled for track 1
R9#debug standby events
HSRP Events debugging is on
R9#
 track-sta (1) Change #2 IPv6 route 2010:CAFE:11::11/128, OSPF->no ipv6 route, reachability Up->Down
track-sta (1) ipv6 route 2010:CAFE:11::11/128 reachability Up -> Down
HSRP: Et1/0 Grp 201 Track 1 object changed, state Up -> Down
HSRP: Et1/0 Grp 201 Priority 120 -> 30
HSRP: Et1/0 Grp 201 Active: j/Coup rcvd from higher pri router (100/FE80::ABB:CCFF:FE00:801)
HSRP: Et1/0 Grp 201 Active router is FE80::ABB:CCFF:FE00:801, was local
HSRP: Et1/0 Nbr FE80::ABB:CCFF:FE00:801 active for group 201
HSRP: Et1/0 Grp 201 Standby router is unknown, was FE80::ABB:CCFF:FE00:801
HSRP: Et1/0 Nbr FE80::ABB:CCFF:FE00:801 no longer standby for group 201 (Active)
HSRP: Et1/0 Grp 201 Active -> Speak
*Dec 22 19:43:14:028: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 201 state Active -> Speak
HSRP: Et1/0 Grp 201 MAC addr update Delete from SMF 0005.73a0.0065
HSRP: Et1/0 Grp 201 MAC addr update Delete from SMF 0005.73a0.00c9
HSRP: Et1/0 Grp 201 Deactivating MAC 0005.73a0.00c9
HSRP: Et1/0 Grp 201 Removing 0005.73a0.00c9 from MAC address filter
HSRP: Et1/0 Grp 101 MAC addr update Delete from SMF 0005.73a0.0065
HSRP: Et1/0 Grp 201 MAC addr update Delete from SMF 0005.73a0.00c9
R9#
HSRP: Et1/0 Grp 201 Speak: d/Standby timer expired (unknown)
HSRP: Et1/0 Grp 201 **Standby router is local**
HSRP: Et1/0 Grp 201 Speak -> Standby
*Dec 22 19:43:26.051: %HSRP-5-STATECHANGE: Ethernet1/0 Grp 201 state Speak -> Standby
R8#debug track state 1
track state debugging enabled for track 1
R8#debug standby events
HSRP: Et1/0 Grp 201 Standby: h/Hello rcvd from lower pri Active router (30/FE80::A8BB:CCFF:FE00:901)
HSRP: Et1/0 Grp 201 Active router is local, was FE80::A8BB:CCFF:FE00:901
HSRP: Et1/0 Nbr FE80::A8BB:CCFF:FE00:901 no longer active for group 201 (Standby)
HSRP: Et1/0 Grp 201 Standby router is unknown, was local
HSRP: Et1/0 Grp 201 Standby -> Active
HSRP: Et1/0 Grp 201 Activating MAC 0005.73a0.00c9
HSRP: Et1/0 Grp 201 Adding 0005.73a0.00c9 to MAC address filter
HSRP: Et1/0 Grp 201 Standby router is FE80::A8BB:CCFF:FE00:901
HSRP: Et1/0 Nbr FE80::A8BB:CCFF:FE00:901 standby for group 201

R8#sh standby brief
<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>P</th>
<th>State</th>
<th>Active</th>
<th>Standby</th>
<th>Virtual IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>101</td>
<td>120</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>FE80::A8BB:CCFF:FE00:901</td>
<td>FE80::5:73FF:FEA0:65</td>
</tr>
<tr>
<td>Et1/0</td>
<td>201</td>
<td>100</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>FE80::A8BB:CCFF:FE00:901</td>
<td>/FE80::5:73FF:FEA0:C9</td>
</tr>
</tbody>
</table>
IPv6 Generic Prefix

You have been assigned a prefix 2001:DB8::/48 and 2001:DB8:1::/48 to R10 and R11 respectively by your ISP SP#5

Ensure that R10 and R11 have their IPv6 Addresses assigned as per diagram based on that prefix

Use "general-prefix" for your solution

Do not explicitly configure IPv6 address on R10 or R11 outside interfaces

**Configuration:**

**R10**

ipv6 general-prefix GLOBAL 2001:DB8:0::/48

interface Ethernet0/0
ipv6 address GLOBAL ::AA00:0:0:0:9/64

**R11**

ipv6 general-prefix GLOBAL 2001:DB8:1::/48

interface Ethernet0/0
ipv6 address GLOBAL ::BB00:0:0:0:13/64

**Verification:**

R10#sh ipv6 int et 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:A00
No Virtual link-local address(es):
General-prefix in use for addressing
Global unicast address(es):

2001:DB8:0:AA00::9, subnet is 2001:DB8:0:AA00::/64

<Output omitted>

R11#show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:B00
No Virtual link-local address(es):
General-prefix in use for addressing
Global unicast address(es):

2001:DB8:1:BB00::13, subnet is 2001:DB8:1:BB00::/64

<Output omitted>
Note: Similar debug messages should be seen on R10

R11#debug ipv6 interface
IPv6 interface all debugging is on

[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/dis]: set opr state to enabled: general prefix
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: Notifying Enabling
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: MTU Changed 1500
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: Notified Enabling
IPv6-IDB: Ethernet0/0 is down, no IPv6 subblock: ipv6_idb_alloc
IPv6-IDB: Ethernet0/0 is down, no IPv6 subblock: ipv6sb linked
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: Notified Enabled

[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: L2 transition down->up (general prefix)
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: Notifying L2 Comingup
[B,Exec]IPv6-INTF Et0/0[L2 dwn, L3 dwn/en]: Notified L2 Comingup
[B,Exec]IPv6-INTF Et0/0[L2 up, L3 dwn/en]: Notifying L2 Init
[B,Exec]IPv6-INTF Et0/0[L2 up, L3 dwn/en]: Notified L2 Init
[B,Exec]IPv6-INTF Et0/0[L2 up, L3 dwn/en]: Notifying L2 Cameup
[B,Exec]IPv6-INTF Et0/0[L2 up, L3 dwn/en]: Notified L2 Cameup

[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 dwn/en]: set l3 state to up: Link-local state changed
[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 up/en]: Notifying L3 Cameup
[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 up/en]: Notified L3 Cameup
[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 up/en]: Ignored L3 event (Route Adjust)
[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 up/en]: Ignored L3 event (Route Adjust)
[B,IPv6 ND]IPv6-INTF Et0/0[L2 up, L3 up/en]: Ignored L3 event (Route Adjust)

[B,Net Background]IPv6-INTF: route-adjust msg enqueued for Ethernet0/0(3-0xA212D1D0) - Qsize 1
[B,IPv6 IDB]IPv6-INTF Et0/0[L2 up, L3 up/en]: ipv6_idb_route_adjust >> Lock Semaphore
[B,IPv6 IDB]IPv6-INTF Et0/0[L2 up, L3 up/en]: Ignore duplicate L2 event up (Route Adjust)
[B,IPv6 IDB]IPv6-INTF Et0/0[L2 up, L3 up/en]: ipv6_idb_route_adjust << Unlock Semaphore

R11#un all
All possible debugging has been turned off
San Francisco Group HQ – Service Provider#5

eBGP

Configure IPv6 eBGP between AS64784 R10 R11 and AS15789 ISP
On R91 advertise into BGP first 64 bits for the prefix pointing towards R10 and R11
Ensure IPv6 community values are also advertised
SP#5 router must establish eBGP session using the peer group named GROUP1

Configuration:

R10
router bgp 64784
neighbor 2001:DB8:0:AA00::10 remote-as 15789

address-family ipv6
  neighbor 2001:DB8:0:AA00::10 activate
  neighbor 2001:DB8:0:AA00::10 send-community
exit-address-family

R11
router bgp 64784
neighbor 2001:DB8:1:BB00::14 remote-as 15789

address-family ipv6
  neighbor 2001:DB8:1:BB00::14 activate
  neighbor 2001:DB8:1:BB00::14 send-community
exit-address-family

R91
ipv6 unicast-routing
ipv6 cef

router bgp 15789
neighbor GROUP1 peer-group
neighbor GROUP1 remote-as 64784
neighbor 2001:DB8:0:AA00::9 peer-group GROUP1
neighbor 2001:DB8:1:BB00::13 peer-group GROUP1

address-family ipv6
  network 2001:DB8:0:AA00::/64
  network 2001:DB8:1:BB00::/64
  neighbor GROUP1 send-community
  neighbor 2001:DB8:0:AA00::9 activate
  neighbor 2001:DB8:1:BB00::13 activate
exit-address-family
Verification:

R91#show bgp ipv6 unicast summary | beg Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:0:AA00::9 4        64784       2       2        1    0    0 00:00:19        0
2001:DB8:1:BB00::13 4        64784       2       2        1    0    0 00:00:13        0
Total dynamically created neighbors: 4/(4 max), Subnet ranges: 1

R10#show bgp ipv6 unicast summary | beg Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:0:AA00::10 4        15789       5       4        3    0    0 00:01:25        2

Note: Similar to IPv4 we get RIB-Failure on R10 and R11 due to AD

R10#sh bgp ipv6 unicast rib-failure
Network            Next Hop                      RIB-failure   RIB-NH Matches
2001:DB8:0:AA00::/64 2001:DB8:0:AA00::10 IPv6 Higher admin distanc  n/a

R10#sh ipv6 route 2001:DB8:0:AA00::/64
Routing entry for 2001:DB8:0:AA00::/64
Known via "connected", distance 0, metric 0, type connected
Backup from "bgp 64784 [20]"
Route count is 1/1, share count 0
Routing paths:
  directly connected via Ethernet0/0
    Last updated 00:10:50 ago

R10#sh bgp ipv6 unicast 2001:DB8:0:AA00::/64
BGP routing table entry for 2001:DB8:0:AA00::/64, version 2
Paths: (1 available, best #1, table default, RIB-failure(145))
Not advertised to any peer
Refresh Epoch 1
15789
2001:DB8:0:AA00::10 (FE80::A8BB:CCFF:FE00:5B01) from 2001:DB8:0:AA00::10 (117.3.64.150)
  Origin IGP, metric 0, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: Ox0
**Note: ICMP reachability check from R10 towards outside interface of R11 IPv6 Address**

R10#show bgp ipv6 unicast 2001:DB8:1:BB00::/64
BGP routing table entry for 2001:DB8:1:BB00::/64, version 3
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   Refresh Epoch 1
   15789
   2001:DB8:0:AA00::10 (FE80::A8BB:CCFF:FE00:5B01) from 2001:DB8:0:AA00::10 (117.3.64.150)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0

R10#ping ipv6 2001:DB8:1:BB00::13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1:BB00::13, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms
San Francisco Group Remote Site

EIGRPv6

Configure EIGRPv6 on R12
Use interface Loopback0 address as EIGRPv6 router ID
PC#1 and R12 should both match below respective outputs
Advertise interface Ethernet1/0 of R12 in EIGRPv6 domain – match IPv4 EIGRP AS number
PC#1 should be able to ping R12

Configuration:

R12
ipv6 unicast-routing
ipv6 cef

router eigrp San_Francisco_Group
  address-family ipv6 unicast autonomous-system 150
  topology base
    metric maximum-hops 20
    distance eigrp 91 171
  exit-as-topology
  maximum-prefix 20
  eigrp router-id 192.12.12.12
  exit-address-family

interface Ethernet1/0
ipv6 eigrp 150

PC1
ipv6 route ::/0 2001:CC1E:BADE::12

Verification:

PC1#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1s - LISP site
  id - LISP dyn-EID, a - Application
S ::/0 [1/0]
  via 2001:CC1E:BADE::12
C 2001:CC1E:BADE::/64 [0/0]
    via Ethernet0/0, directly connected
L 2001:CC1E:BADE::100/128 [0/0]
    via Ethernet0/0, receive
L FF00::/8 [0/0]
    via Null0, receive
PC1#ping ipv6 2001:CC1E:BADE::12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:CC1E:BADE::12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/24 ms

R12#sh ipv6 protocols
IPv6 Routing Protocol is "eigrp 150"
EIGRP-IPv6 VR(San_Francisco_Group) Address-Family Protocol for AS(150)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
Metric rib-scale 128
Metric version 64bit
NSF-aware route hold timer is 240
Maximum-Prefix: 20, threshold: Inherited(15)
Distance: Internal 91 external 171
Active Timer: 3 min
Maximum path: 16
Maximum hopcount 20
Maximum metric variance 1
Total Prefix Count: 2
Total Redist Count: 0
Interfaces:
Ethernet0/0
Ethernet1/0
Redistribution:
None
Default Route

Do not configure eBGP between R12 and R91
R12 should have an IPv6 static default route pointing towards R91 relevant IPv6 Address
Ensure R12 is able to reach outside IPv6 Addresses of R10 and R11

Configuration:

R12
ipv6 route ::/0 2001:DB8:2:CC00::17

R91
router bgp 15789
   address-family ipv6
     network 2001:DB8:2:CC00::/64
     exit-address-family

Verification:

R12#ping ipv6 2001:DB8:1:BB00::13 repeat 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2001:DB8:1:BB00::13, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/2/5 ms

R12#ping ipv6 2001:DB8:0:AA00::9 repeat 50
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 2001:DB8:0:AA00::9, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/1/5 ms

R91#sh bgp ipv6 unicast | be Net
Network          Next Hop            Metric LocPrf Weight Path
*>  2001:DB8:0:AA00::/64
   ::                      0         32768 i
*>  2001:DB8:1:BB00::/64
   ::                      0         32768 i
*>  2001:DB8:2:CC00::/64
   ::                      0         32768 i

R91#sh ipv6 route 2001:DB8:2:CC00::/64
Routing entry for 2001:DB8:2:CC00::/64
Known via "connected", distance 0, metric 0, type connected
Route count is 1/1, share count 0
Routing paths:
   directly connected via Ethernet0/0
   Last updated 00:30:10 ago
San Francisco Group Data Centre

EIGRPv6 – DHCP

Configure EIGRPv6 AS111 on R13 using AS 150
Use the interface Loopback0 IPv4 address as the EIGRPv6 router ID
Ensure Server#1 obtains its IPv6 Address (2001:CC1E:FAFF::/64) via DHCP
R13 should set a flag in IPv6 router advertisements which generally indicates to hosts that they should use administered (stateful) protocol to obtain autoconfiguration information other than addresses DNS server should be configured for Loopback111 of R91 and domain name set to data.co.uk
At the end of this task Server#1 should be able to ping R13 Ethernet1/0 IPv6 Address

Configuration:

R13

ipv6 unicast-routing
ipv6 cef

router eigrp San_Francisco_Group
    address-family ipv6 unicast autonomous-system 150
topology base
exit-af-topology
eigrp router-id 192.13.13.13
exit-address-family

interface Ethernet1/0
    ipv6 eigrp 150

ipv6 dhcp pool dhcp-pool
    address prefix 2001:CC1E:FAFF::/64 lifetime infinite infinite
    dns-server 2001:CDBA::3257:9652
domain-name data.co.uk

interface Ethernet1/0
    ipv6 nd managed-config-flag
ipv6 dhcp server dhcp-pool

Note:

DHCPv6 SLAAC (Stateless Address Autoconfiguration)
Reason to use DHCPv6 on a network that uses SLAAC is to push DNS and other information to the clients

SLAAC is by far the easiest way to configure IPv6 addresses, simply because you don’t have to configure any IPv6 address. With SLAAC, a host uses the IPv6 Neighbor Discovery Protocol (NDP) to determine its IP address and default routers. Using SLAAC, a host requests and listens for Router Advertisements (RA) messages, and then taking the prefix that is advertised to form a unique address that can be used on the network. For this to work, the prefix that is advertised must advertise a prefix length of 64 bits (i.e., /64). But the most significant of Stateless Address Autoconfiguration (SLAAC) is it provided no mechanism for configuring DNS resolver information.

Therefore SLAAC can be used along with DHCPv6 (Stateless) to push DNS and other information to the clients.

*directly from Cisco website –
SERVER1

interface Ethernet0/0
ipv6 address dhcp
ipv6 enable
ipv6 nd autoconfig default-route

Verification:

R13#debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
IPv6 DHCP: Received REQUEST from FE80::ABBB:CCFF:FE00:5100 on Ethernet1/0
IPv6 DHCP: detailed packet contents
src FE80::ABBB:CCFF:FE00:5100 (Ethernet1/0)
dst FF02::1:2
type REQUEST(3), mid 15487166
option ELAPSED-TIME(8), len 2
  elapsed-time 0
option CLIENTID(1), len 10
  00030001AABBCC005100
option ORO(6), len 4
DNS-SERVERS,DOMAIN-LIST
option SERVERID(2), len 10
  00030001AABBCC000D00
option IA-NA(3), len 40
  IAID 0x00030001, T1 0, T2 0
  option IAADDR(5), len 24
    IPv6 address 2001:CC1E:FAFF:0:EC3C:E7E6:73E:C465
preferred INF, INFINITY
valid INF, INFINITY
IPv6 DHCP: Using interface pool dhcp-pool
IPv6 DHCP: Looking up pool 2001:CC1E:FAFF::/64 entry with username '00030001AABBCC00510000030001'
IPv6 DHCP: Poolentry for user found
IPv6 DHCP: Found address 2001:CC1E:FAFF:0:EC3C:E7E6:73E:C465 in binding for FE80::ABBB:CCFF:FE00:5100, IAID 00030001
IPv6 DHCP: Source Address from SAS FE80::ABBB:CCFF:FE00:5100
IPv6 DHCP: Using interface pool dhcp-pool
src FE80::ABBB:CCFF:FE00:5100 (Ethernet1/0)
dst FE80::ABBB:CCFF:FE00:5100 (Ethernet1/0)
type REP(7), mid 15487166
option SERVERID(2), len 10
  00030001AABBCC000D00
option CLIENTID(1), len 10
  00030001AABBCC005100
option IA-NA(3), len 40
  IAID 0x00030001, T1 43200, T2 69120
  option IAADDR(5), len 24
    IPv6 address 2001:CC1E:FAFF:0:EC3C:E7E6:73E:C465
preferred INF, INFINITY
valid INF, INFINITY
option DNS-SERVERS(23), len 16
  2001:CDBA::3257:9652
option DOMAIN-LIST(24), len 12
data.co.uk
IPv6 DHCP: Sending REPLY to FE80::ABBB:CCFF:FE00:5100 on Ethernet1/0
R13#un all
All possible debugging has been turned off

R13#show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  Address allocation prefix: 2001:CC1E:FAFF::/64 valid 4294967295 preferred 4294967295 (1 in use, 0 conflicts)
  DNS server: 2001:CDBA::3257:9652
  Domain name: data.co.uk
  Active clients: 1
WEBSERVER#1#sh ipv6 route
IPv6 Routing Table - default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, ls - LISP site
ld - LISP dyn-EID, a - Application

ND ::/0 [2/0]
  via FE80::A8BB:CCFF:FE00:D01, Ethernet0/0
LC 2001:CC1E:FAFF:0:EC3C:E7E6:73E:C465/128 [0/0]
    via Ethernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
eBGP

Configure eBGP between R13 and R91
SP#5 router must establish eBGP session using already existing peer group
On R91 advertise first 64bit of the IPv6 connection Address towards R13 into BGP

Configuration:

R13
router bgp 64784
neighbor 2001:DB8:3:DD00::21 remote-as 15789
address-family ipv6
neighbor 2001:DB8:3:DD00::21 activate
neighbor 2001:DB8:3:DD00::21 send-community
exit-address-family

R91
router bgp 15789
neighbor 2001:DB8:3:DD00::22 peer-group GROUP1
address-family ipv6
network 2001:DB8:3:DD00::/64
neighbor 2001:DB8:3:DD00::22 activate
exit-address-family

Verification:

R13#show bgp ipv6 unicast | be Net
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 2001:DB8:0:AA00::/64</td>
<td>2001:DB8:3:DD00::21</td>
<td>0</td>
<td>0</td>
<td>15789</td>
<td>i</td>
</tr>
<tr>
<td>* 2001:DB8:1:BB00::/64</td>
<td>2001:DB8:3:DD00::21</td>
<td>0</td>
<td>0</td>
<td>15789</td>
<td>i</td>
</tr>
<tr>
<td>* 2001:DB8:2:CC00::/64</td>
<td>2001:DB8:3:DD00::21</td>
<td>0</td>
<td>0</td>
<td>15789</td>
<td>i</td>
</tr>
<tr>
<td>2001:DB8:3:DD00::/64</td>
<td>2001:DB8:3:DD00::21</td>
<td>0</td>
<td>0</td>
<td>15789</td>
<td>i</td>
</tr>
</tbody>
</table>

R13#show bgp ipv6 unicast summary | be Neigh
<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8:3:DD00::21</td>
<td>4</td>
<td>15789</td>
<td>9</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>00:01:58</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
Route Advertisement

On SP#5 advertise Global DNS and Facebook prefixes using two separate network statements
Ensure that verification output on R11 is a match (same for R10 and R13)
IPv6 users from each office should be able to reach Global IPv6 DNS server and Facebook website by their respective IPv6 addresses
Do not use ACL or Prefix List anywhere in your configuration
Do not perform redistribution anywhere in your configuration

Configuration:

R91
route-map IPV6_METRIC permit 10
  match interface Loopback111 Loopback133
  set metric 50
  set origin incomplete
router bgp 15789
  address-family ipv6
    network 2001:DB8:1A:1111::131/128 route-map IPV6_METRIC
    network 2001:CDBA::3257:9652/128 route-map IPV6_METRIC
  exit-address-family

Verification:

R11# show bgp ipv6 unicast | be Net
Network Next Hop Metric LocPrf Weight Path
*> 2001:DB8:0:AA00::/64 2001:DB8:1:BB00::14 0 0 15789 i
r> 2001:DB8:1:BB00::/64 2001:DB8:1:BB00::14 0 0 15789 i
*> 2001:DB8:2:CC00::/64 2001:DB8:1:BB00::14 0 0 15789 i
*> 2001:DB8:3:DD00::/64 2001:DB8:1:BB00::14 0 0 15789 i
*> 2001:DB8:1A:1111:131/128 2001:DB8:1:BB00::14 50 0 15789 ?
*> 2001:CDBA::3257:9652/128 2001:DB8:1:BB00::14 50 0 15789 ?

R11# show bgp ipv6 unicast 2001:CDBA::3257:9652/128
BGP routing table entry for 2001:CDBA::3257:9652/128, version 7
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  15789
  2001:DB8:1:BB00::14 (FE80::A8BB:CCFF:FE00:5B02) from 2001:DB8:1:BB00::14 (117.3.64.150)
    Origin incomplete, metric 50, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0x0
R11# show bgp ipv6 unicast 2001:DB8:1A:1111::131/128
BGP routing table entry for 2001:DB8:1A:1111::131/128, version 6
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1

15789
  2001:DB8:1:BB00::14 (FE80::A8BB:CCFF:FE00:5B02) from 2001:DB8:1:BB00::14 (117.3.64.150)
    Origin incomplete, metric 50, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0x0

Note: ICMP reachability check from R11 towards Facebook and Global DNS IPv6 Address

R11(tcl)#foreach CCIE {
  +>2001:DB8:1A:1111::131
  +>2001:CDBA::3257:9652
  +>}{ ping $CCIE source eth 0/0 }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1A:1111::131, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1:BB00::13
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:CDBA::3257:9652, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1:BB00::13
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R11(tcl)#tclquit
R11#
IPv6 Global DNS Service

IPv6 San Francisco routers R10 R11 R12 R13 should be able to reach IPv6 www.facebook.com by its website name FQDN.
R91 must be configured as a Global DNS Server – please refer to the diagram.

**Configuration:**

R10
```bash
ip name-server 2001:CDBA::3257:9652
```

R11
```bash
ip name-server 2001:CDBA::3257:9652
```

R12
```bash
ip name-server 2001:CDBA::3257:9652
```

R13
```bash
ip name-server 2001:CDBA::3257:9652
```

R91
```bash
ip dns server
ip host www.facebook.com 2001:DB8:1A:1111::131
```

**Verification:**

R10#ping www.facebook.com

Translating "www.facebook.com"...domain server (2001:CDBA::3257:9652) [OK]

Sending 5, 100-byte ICMP Echos to 2001:DB8:1A:1111::131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms

R10#debug domain replies detail
Domain Name System Reply debugging is on (detailed)
search_nametype_index: www.facebook.com
search_nametype_index: www.facebook.com
Domain: query for www.facebook.com type 28 to 2001:CDBA::3257:9652
DOM: dom2cache: hostname is www.facebook.com, RR type=28, class=1, ttl=10, n=16
search_nametype_index: www.facebook.com
delete_nametype_from_index: searching www.facebook.com to delete
delete_nametype_from_index: name www.facebook.com not found to del
delete_nametype_from_index: also found 0 entries to delete directly
add_nametype_to_index: added www.facebook.com
delete_nametype_from_index: searching www.facebook.com to delete
delete_nametype_from_index: www.facebook.com found & deleted
delete_nametype_from_index: also found 0 entries to delete directly
add_nametype_to_index: added www.facebook.com
Reply received ok

search_nametype_index: www.facebook.com
search_nametype_index: found www.facebook.com for www.facebook.com
search_nametype_index: www.facebook.com
search_nametype_index: found www.facebook.com for www.facebook.com
R10#un all
All possible debugging has been turned off
R91#debug domain replies detail
Domain Name System Reply debugging is on (detailed)
DNS: Send reply from internal information:
  id=43039, response, opcode=0, aa=0, tc=0, rd=1, ra=1
  rcode=0, qdcount=1, ancount=1, nscount=0, arcount=0
  query name is www.facebook.com, qtype=28, class=1
Answer section:
  Name='www.facebook.com'
  RR type=28, class=1, ttl=10, data length=16
  IPv6=2001:DB8:1A:1111::131
Authority section:
Additional record section:
DNS: Finished processing query (id#43039) in 0.000 secs
R91#un all
All possible debugging has been turned off
GRE Tunnel

Implement GRE Tunnel between R11 R12 and R13. The tunnel must use the IPv6 address space as seen in the IPv6 diagram where X is the router number. Use internet interface to source all packets from and establish Tunnel reachability. Tunnel packets should carry the ID key 1112 for R11-R12 and 1113 for R11-R13. Extend OSPFv3 domain across the Tunnel. Static default route should only exist on R12. At the end of this task all San Francisco offices, DR site and Service Provider#1 Network Admin should be able to establish connectivity with each other’s IPv6 Addresses.

Configuration:

R13

interface Tunnel1113
no ip address
ipv6 address 3001::13/112
ipv6 ospf 100 area 0
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 155.84.74.13
tunnel key 1113

router eigrp San_Francisco_Group
address-family ipv6 unicast autonomous-system 150
topology base
redistribute ospf 100 include-connected
exit-address-family

ipv6 route ospf 100
redistribute eigrp 150 include-connected

R11

interface Tunnel1113
no ip address
ipv6 address 3001::11/112
ipv6 ospf 100 area 0
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 155.84.74.22
tunnel key 1113

interface Tunnel1112
no ip address
ipv6 address 3000::11/112
ipv6 ospf 100 area 0
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 155.84.74.18
tunnel key 1112
**R12**

interface Tunnel1112
no ip address
ipv6 address 3000::12/112
ipv6 ospf 100 area 0
tunnel source Ethernet0/0
tunnel mode ipv6ip
tunnel destination 155.84.74.13
tunnel key 1112

ipv6 ospf 10
redistribute eigrp 150 include-connected

**Verification:**

```
R12#sh ipv6 osp ne
OSPFv3 Router with ID (192.11.11.11) (Process ID 100)
 Neighbor ID Pri State Dead Time Interface ID Interface
192.168.21.12 0 FULL/ - 00:00:30 16 Tunnel1112
192.168.35.100 0 FULL/ - 00:00:32 20 Tunnel1113
192.102.102.102 1 FULL/DR 00:00:36 15 Ethernet3/0
```

**Note:** We should now be able to reach Network Admin IPv6 user inside of RIPng domain

WEBSERVER# ping ipv6 2001:197:150::150 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:197:150::150, timeout is 2 seconds:
!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/23 ms

WEBSERVER# traceroute ipv6 2001:197:150::150
Type escape sequence to abort.
Tracing the route to 2001:197:150::150
   1 2001:CC1E:FAFF::13 4 msec 2 msec 1 msec
    2 3001::11 1 msec 1 msec 9 msec
    3 2001:CC1E:CAFE::19 15 msec 9 msec 2 msec
    4 2001:CC1E:CAFE::9 2 msec 2 msec 6 msec
    5 2001:CC1E:CAFE::1 6 msec 2 msec 1 msec
    6 2001:CCCC:CAFE::2 2 msec 2 msec 1 msec

PCI# ping 2001:197:150::150 repeat 10 so et 0/0
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:197:150::150, timeout is 2 seconds:
Packet sent with a source address of 2001:CC1E:BADE::100
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/22/113 ms
traceroute ipv6 2001:197:150::150
Type escape sequence to abort.
Tracing the route to 2001:197:150::150
1 2001:CC1E:BADE::12 5 msec 17 msec 1 msec
2 3000::11 0 msec 4 msec 1 msec
3 2001:CC1E:CAFE::19 2 msec 3 msec 1 msec
4 2001:CC1E:CAFE::9 2 msec 1 msec 1 msec
5 2001:CC1E:CAFE::1 1 msec 2 msec 5 msec
6 2001:CCCC:CAFE::2 1 msec 2 msec 1 msec

Note: Routing table check on R11 and we can see our newly created tunnel interfaces in use!
DNS & SSH

Configure R13 to only allow SSH connections from R9 VLAN19 IPv6 Address in the HQ
HQ internal DNS server R11 Loopback0 holds an entry “R13SSH”
No other devices should be able to SSH to R13
R13 should log all SSH attempts
Use a local username of DATA and a password of CISCO
Do not configure AAA for this task
Configure a domain as ‘SanFran.co.uk’ without the quotes

Configuration:

R13
ip domain name SanFran.co.uk
username DATA privilege 15 password 0 CISCO
ipv6 access-list SSH_ACCESS
   permit tcp host 2001:CC1E:CAFE::9 any eq 22 log
deny ipv6 any any log
line vty 0 4
   ipv6 access-class SSH_ACCESS in
   login local
   transport input ssh
   crypto key generate rsa general-keys modulus 1024

R11
ip dns server
ip host R13SSH 3001::13

R8
ip name-server 2010:CAFE:11::11

R9
ip name-server 2010:CAFE:11::11

R10
ip name-server 2010:CAFE:11::11

Verification:

R9#ssh -l DATA R13SSH
Translating "R13SSH"...domain server (2010:CAFE:11::11)
Translating "R13SSH"...domain server (2010:CAFE:11::11) [OK]
Password:
R13#exit
[Connection to R13SSH closed by foreign host]
**Note:** We will enable debug on R13 and R11

R13#debug ip ssh detail

```
ssh detail messages debugging is on
```

```
* Dec 25 12:30:53.674: %IPV6_ACL-6-ACCESSLOGP: list SSH_ACCESS/10 permitted tcp 2001:CC1E:CAFE::9(38209) -> ::(22), 1 packet
```

```
* Dec 25 12:30:53.687: %IPV6_ACL-6-ACCESSLOGP: list SSH_ACCESS/10 permitted tcp 2001:CC1E:CAFE::9(38209) -> 3001::13(22), 1 packet
```

```
SSH0: starting SSH control process
```

```
SSH01: sent protocol version id SSH-1.99-Cisco-1.25
SSH0: protocol version id is - SSH-1.99-Cisco-1.25
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2 0: kex: client->server enc:aes128-cbc mac:hmac-sha1
SSH2 0: kex: server->client enc:aes128-cbc mac:hmac-sha1
SSH2 0: Using kex_algo = diffie-hellman-group-exchange-sha1
SSH2 0: SSH2_MSG_KEX_DH_GEX_REQUEST received
SSH2 0: Range sent by client is - 1024 < 2048 < 4096
SSH2 0: expecting SSH2_MSG_KEX_DH_GEX_INIT
SSH2 0: SSH2_MSG_KEX_DH_GEX_INIT received
SSH2: kexderive_keys complete
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: SSH2_MSG_NEWKEYS received
SSH2 0: Using method = none
SSH2 0: Authentications that can continue = publickey,keyboard-interactive,password
SSH2 0: Using method = keyboard-interactive
SSH2 0: authentication successful for DATA
SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
SSH2 0: shell request
SSH2 0: shell message received
SSH2 0: starting shell for vty
SSH0: Session terminated normally

R11#debug domain replies detail

Domain Name System Reply debugging is on (detailed)

DNS: Forwarding reply:
```
DOM: id=37307, response, opcode=0, aa=0, tc=0, rd=1, ra=1
   rcode=2, qdcount=1, ancount=0, ncount=0, arcount=0
   query name is R13SSH, qtype=1, class=1
```

Answer section:

Authority section:

Additional record section:

DNS: Send reply from internal information:
```
DOM: id=33824, response, opcode=0, aa=0, tc=0, rd=1, ra=1
   rcode=0, qdcount=1, ancount=1, ncount=0, arcount=0
   query name is R13SSH, qtype=28, class=1
```

Answer section:

```
Name='R13SSH'
   RR type=28, class=1, ttl=10, data length=16
```

IPv6=3001::13

Authority section:

Additional record section:

DNS: Finished processing query (id#33824) in 0.000 secs
R8#ssh -l DATA R13SSH
Translating "R13SSH"...domain server (2010:CAFE:11::11)
Translating "R13SSH"...domain server (2010:CAFE:11::11) [OK]
% Connection refused by remote host

R13#
*Dec 25 12:31:43.634: %IPV6_ACL-6-ACCESSLOGP: list SSH_ACCESS/20 denied tcp
2001:CC1E:CAFE::1(59167) --> ::(22), 1 packet

R11#debug domain replies detail
Domain Name System Reply debugging is on (detailed)
DNS: Forwarding reply:
  DOM: id=7815, response, opcode=0, aa=0, tc=0, rd=1, ra=1
      rcode=2, qdcount=1, ancount=0, ncount=0, arcount=0
      query name is R13SSH, qtype=1, class=1
Answer section:
Authority section:
Additional record section:
DNS: Send reply from internal information:
  DOM: id=14714, response, opcode=0, aa=0, tc=0, rd=1, ra=1
      rcode=0, qdcount=1, ancount=1, ncount=0, arcount=0
      query name is R13SSH, qtype=28, class=1
Answer section:
  Name='R13SSH'
    RR type=28, class=1, ttl=10, data length=16
    IPv6=3001::13
Authority section:
Additional record section:
DNS: Finished processing query (id#14714) in 0.000 secs
Configure OSPFv3 in the SP#9 Office as per the following requirements:
Configure OSPF Process Id 1
Configure Loopback 0 as OSPF router id
R3 must be elected as DR for VLAN 23
R2 must be BDR and ready to take over R3
You are not allowed to use `ipv6 ospf 1 area`
You are not allowed to use `ipv6 ospf 1 priority`

**Configuration:**

R2
```
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.2.2

interface Ethernet1/0.24
  ospfv3 1 ipv6 area 0

interface Ethernet1/0.23
  ospfv3 1 priority 254
  ospfv3 1 ipv6 area 0
```

R3
```
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.3.3

interface Ethernet2/0
  ospfv3 1 priority 255
  ospfv3 1 ipv6 area 0

interface Ethernet0/0.35
  ospfv3 1 ipv6 area 0
```

R4
```
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.4.4

interface Ethernet0/0.46
  ospfv3 1 ipv6 area 0

interface Ethernet0/0.24
  ospfv3 1 ipv6 area 0
```
R5
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.5.5
interface Ethernet1/0
ospfv3 1 ipv6 area 0
interface Ethernet0/0.57
ospfv3 1 ipv6 area 0

R6
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.6.6
interface Ethernet0/0.46
ospfv3 1 ipv6 area 0

R7
ipv6 unicast-routing
ipv6 cef
router ospfv3 1
router-id 172.100.7.7
interface Ethernet2/0
ospfv3 1 ipv6 area 0

Verification:

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Interface ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.3.3</td>
<td>255</td>
<td>FULL/DR</td>
<td>00:00:39</td>
<td>11</td>
<td>Ethernet1/0.23</td>
</tr>
<tr>
<td>172.100.4.4</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:36</td>
<td>15</td>
<td>Ethernet1/0.24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Interface ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.100.5.5</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:38</td>
<td>7</td>
<td>Ethernet0/0.35</td>
</tr>
<tr>
<td>172.100.2.2</td>
<td>254</td>
<td>FULL/BDR</td>
<td>00:00:30</td>
<td>20</td>
<td>Ethernet2/0</td>
</tr>
</tbody>
</table>

Note: Check reachability between R6 and R7 LAN IPv6 Addresses

R6#ping 2001:CC1E:BEF:57:172:31:10:38 so set 0/0.46 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:CC1E:BEF:57:172:31:10:38, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/9 ms

Type escape sequence to abort.
IPv6 Part II

Establish the four eBGP peering as indicated on “diagram IPv6 routing”
Do not use the network command under the BGP IPv6 address-family on neither R6 or R7
Advertise the IPv6 prefix on WAN interfaces into BGP on R6, R7, R13, and R15 respectively
Advertise the IPv6 prefix of both Loopback 100 interfaces of R13 and R15 into BGP
Do not configure any prefix advertisement into BGP on SP#6 routers
Configure your network such that R13 Network Admin Loopback 100 IPv6 Address can communicate
with R15 File Server Loopback 100 IPv6 Address
Do not use any static route or default route anywhere

Configuration:

R6
router bgp 5934
address-family ipv6
  redistribute ospf 1 match internal external 1 external 2 network 2001:CC1E:BEF:20::/64
exit-address-family
router ospfv3 1
  address-family ipv6 unicast
  redistribute bgp 5934
  exit-address-family

R7
router bgp 5934
address-family ipv6
  redistribute ospf 1 match internal external 1 external 2 network 2001:CC1E:BEF:25::/64
exit-address-family
router ospfv3 1
  address-family ipv6 unicast
  redistribute bgp 5934
  exit-address-family

R92
ipv6 unicast-routing
ipv6 cef

router bgp 10001
  neighbor 2001:CC1E:BEF:20:140:60:88:2 remote-as 5934
  address-family ipv6
  exit-address-family
R93
ipv6 unicast-routing
ipv6 cef
router bgp 10001
neighbor 2001:CC1E:BEF:30:140:60:88:33 remote-as 65001
address-family ipv6
exit-address-family

R13
router bgp 64784
address-family ipv6
network 2001:CC1E:BEF:15::/64
network 2001:CC1E:BEF:192::13/128
exit-address-family

Note: In case IPv4 Unicast Address Family is not disabled by default using 'no bgp default ipv4-unicast' command then output on R15 should look like this:

R15
ipv6 unicast-routing
ipv6 cef
router bgp 65001
neighbor 2001:CC1E:BEF:30:140:60:88:34 remote-as 10001
address-family ipv6
network 2001:CC1E:BEF:30::/64
network 2001:CC1E:BEF:172::15/128
neighbor 2001:CC1E:BEF:30:140:60:88:34 activate
exit-address-family

Verification:

Note: Let's see if we now have desired reachability between Network Admin and the File Server

R13#ping ipv6 2001:CC1E:BEF:172::15 so 2001:CC1E:BEF:192::13 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2001:CC1E:BEF:172::15, timeout is 2 seconds:
Packet sent with a source address of 2001:CC1E:BEF:192::13
..................................................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/10/244 ms

R13#traceroute ipv6 2001:CC1E:BEF:172::15
Tracing the route to 2001:CC1E:BEF:172::15
1 2001:CC1E:BEF:15:140:60:88:22 4 msec 0 msec 1 msec

R7#sh bgp ipv6 unicast 2001:CC1E:BEF:172::15/128
BGP routing table entry for 2001:CC1E:BEF:172::15/128, version 6
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
10001 65001
  (124.19.254.150)
  Origin IGP, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0

R13#sh bgp ipv6 unicast 2001:CC1E:BEF:172::15/128
BGP routing table entry for 2001:CC1E:BEF:172::15/128, version 16
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    1
  Refresh Epoch 1
10001 5934
  (110.1.16.150)
  Origin incomplete, localpref 100, valid, external, best
CCIEv5 R&S IPv6 Topology #3

IPv4/IPv6 Core
BGP AS 64784
San Francisco Group Data Centre

RIPng
BGP AS 25432
Service Provider #1

INTERNET

Redistribution

IPv4/IPv6 Core
BGP AS 65001
Berlin HQ Data Centre

File Server
Loopback 100
2001:CC1E:BEF:172::15/128

Loopback 307
SP#1 Network Admin
2001:197:150:150/128

Copyright © 2015 CCIE4ALL. All rights reserved
IPv6 Redistribution

Network Admin Loopback 307 IPv6 Address inside SP#1 should be able to connect to R15 the File Server Loopback 100 IPv6 Address
On R13 ensure that no other prefix is advertised into the relevant IGB/BGP domains

**Configuration:**

```
R13
ipv6 prefix-list BGPv6 seq 5 permit 2001:CC1E:BEF:172::15/128
ipv6 prefix-list OSPFv3 seq 5 permit 2001:197:150::150/128
route-map BGPv6 permit 10
  match ipv6 address prefix-list BGPv6
route-map OSPFv3 permit 10
  match ipv6 address prefix-list OSPFv3
router bgp 64784
  address-family ipv6
    redistribute ospf 100 route-map OSPFv3
  exit-address-family
ipv6 router ospf 100
  redistribute bgp 64784 route-map BGPv6
```

**Verification:**

```
R96#sh ipv6 route 2001:CC1E:BEF:172::15/128
Routing entry for 2001:CC1E:BEF:172::15/128
  Known via "rip RIPng", distance 120, metric 6
  Route count is 1/1, share count 0
  Routing paths:
    FE80::A8BB:CCFF:FE00:800, Ethernet0/0
    Last updated 00:15:34 ago

R15#sh ipv6 route 2001:197:150::150/128
Routing entry for 2001:197:150::150/128
  Known via "bgp 65001", distance 20, metric 0, type external
  Route count is 1/1, share count 0
  Routing paths:
    FE80::A8BB:CCFF:FE00:5D00, Ethernet0/0
    MPLS label: nolabel
    Last updated 00:17:20 ago

R96#ping 2001:CC1E:BEF:172::15 so loo 307 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:CC1E:BEF:172::15, timeout is 2 seconds:
Packet sent with a source address of 2001:197:150::150
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/6/12 ms

R13#sh ipv6 prefix-list
ipv6 prefix-list BGPv6: 1 entries
  seq 5 permit 2001:CC1E:BEF:172::15/128
ipv6 prefix-list OSPFv3: 1 entries
  seq 5 permit 2001:197:150::150/128
```
IPv6 Routing Protocol is "bgp 64784"
IGP synchronization is disabled
Redistribution:
  - Redistributing protocol ospf 100 (internal) route-map OSPFv3
Neighbor(s):
  Address                  FiltIn FiltOut Weight RoutemapIn RoutemapOut
  2001:DB8:3:DD00::21     

IPv6 Routing Protocol is "ospf 100"
Router ID 192.168.35.100
Autonomous system boundary router
Number of areas: 1 normal, 0 stub, 0 nssa
Interfaces (Area 0):
  Tunnel1113
Redistribution:
  - Redistributing protocol eigrp 150 include-connected
  - Redistributing protocol bgp 64784 route-map BGPv6
Service Provider #6 – Service Provider #9

LDP Authentication

Configure authentication between R2-R3 using password of “MPLS23” (without the quotes)
You must not use “mpls ldp neighbor” command to accomplish this task

Configure authentication between R6-R7 using password of “MPLS67” (without the quotes)
You must not use an ACL for this task

Configuration:

R2

access-list 23 permit 172.100.3.3

mpls ldp password required for 23
mpls ldp password option 1 for 23 MPLS23

R3

access-list 23 permit 172.100.2.2

mpls ldp password required for 23
mpls ldp password option 1 for 23 MPLS23

R6

mpls ldp neighbor 172.100.7.7 password MPLS67

R7

mpls ldp neighbor 172.100.6.6 password MPLS67

Verification: Before Implementation

R2#show mpls ldp neighbor 172.100.3.3 detail
Peer LDP Ident: 172.100.3.3:0; Local LDP Ident 172.100.2.2:0
TCP connection: 172.100.3.3.61261 - 172.100.2.2.646
Password: not required, none, in use
State: Oper; Msgs sent/rcvd: 200/201; Downstream; Last TIB rev sent 68
Up time: 02:28:01; UID: 3; Peer Id 2;
LDP discovery sources:
    Ethernet1/0.23; Src IP addr: 172.31.10.2
    holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
    172.31.10.5     172.100.3.3     172.100.33.33   172.100.133.133
    140.60.88.17    140.60.88.69    140.60.88.73    172.31.10.9
    172.31.10.2
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

<Output omitted>

R2#
*Dec 25 14:22:21.593: %LDP-5-NBRCHG: LDP Neighbor 172.100.3.3:0 (1) is DOWN (Session’s MD5 password changed)
R2#
*Dec 25 14:22:23.159: %TCP-6-BADAUTH: No MD5 digest from 172.100.3.3(43897) to 172.100.2.2(646) tableid - 0
R2#
Verification: After Implementation

R2#show mpls ldp neighbor 172.100.3.3 detail
Peer LDP Ident: 172.100.3.3:0; Local LDP Ident 172.100.2.2:0
TCP connection: 172.100.3.3.29412 - 172.100.2.2.646; MD5 on

Password: required, option 1, in use
State: Oper; Msgs sent/rcvd: 33/33; Downstream; Last TIB rev sent 71
Up time: 00:00:51; UID: 4; Peer Id 2;
LDP discovery sources:
   Ethernet1/0.23; Src IP addr: 172.31.10.2
   holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
   172.31.10.5 172.100.3.3 172.100.33.33 172.100.133.133
   140.60.88.37 140.60.88.69 140.60.88.73 172.31.10.9
   172.31.10.2
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

Note: R3 and R3 LDP adjacency is now up
R2#
*Dec 25 14:22:45.305: %LDP-5-NBRCHG: LDP Neighbor 172.100.3.3:0 (1) is UP

Note: Now R6 and R7 before
R6#show mpls ldp neighbor 172.100.7.7 detail
Peer LDP Ident: 172.100.7.7:0; Local LDP Ident 172.100.6.6:0
TCP connection: 172.100.7.7.34319 - 172.100.6.6.646

Password: not required, none, in use
State: Oper; Msgs sent/rcvd: 205/203; Downstream; Last TIB rev sent 68
Up time: 02:30:45; UID: 1; Peer Id 0;
LDP discovery sources:
   Ethernet2/0; Src IP addr: 172.31.10.46
   holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
   140.60.88.66 140.60.88.62 140.60.88.58 172.31.10.34
   172.100.7.7 172.100.177.177 172.31.10.38
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

Note: And after
R6#show mpls ldp neighbor 172.100.7.7 detail
Peer LDP Ident: 172.100.7.7:0; Local LDP Ident 172.100.6.6:0
TCP connection: 172.100.7.7.34319 - 172.100.6.6.646

Password: not required, neighbor, stale
State: Oper; Msgs sent/rcvd: 206/204; Downstream; Last TIB rev sent 68
Up time: 02:31:41; UID: 1; Peer Id 0;
LDP discovery sources:
   Ethernet2/0; Src IP addr: 172.31.10.46
   holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
   140.60.88.66 140.60.88.62 140.60.88.58 172.31.10.34
   172.100.7.7 172.100.177.177 172.31.10.38
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

Note: Stale - indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale)
LDP Session Protection

The network administrator of AS5934 is concerned about MPLS re-convergence time if the link between any of the MPLS enabled routers flaps – R1 R2 R3 R6 and R7. Ensure that when the link between these devices goes down for maximum of 30 seconds then LDP sessions and LDP bindings do not need to be re-established or relearned.

Configuration:

<table>
<thead>
<tr>
<th>Device</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>mpls ldp session protection duration 30</td>
</tr>
<tr>
<td>R2</td>
<td>mpls ldp session protection duration 30</td>
</tr>
<tr>
<td>R3</td>
<td>mpls ldp session protection duration 30</td>
</tr>
<tr>
<td>R6</td>
<td>mpls ldp session protection duration 30</td>
</tr>
<tr>
<td>R7</td>
<td>mpls ldp session protection duration 30</td>
</tr>
</tbody>
</table>

Verification Before and After

R6#show mpls ldp neighbor 172.100.1.1 detail
   Peer LDP Ident: 172.100.1.1:0; Local LDP Ident 172.100.6.6:0
   TCP connection: 172.100.1.1.646 - 172.100.6.6.11819
   Password: not required, none, in use
   State: Oper; Mqs sent/rcvd: 61/59; Downstream; Last TIB rev sent 89
   Up time: 00:07:13; UID: 4; Peer Id 3;
   LDP discovery sources:
   Ethernet1/0; Src IP addr: 172.31.10.25
   holdtime: 15000 ms, hello interval: 5000 ms
   Targeted Hello 172.100.6.6 -> 172.100.1.1, active, passive;
   holdtime: infinite, hello interval: 10000 ms
   Addresses bound to peer LDP Ident:
   172.31.10.25  172.31.10.30  172.31.10.41  172.31.10.33
   172.31.10.14  172.31.10.10  172.31.100.100  172.100.1.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
<Output omitted>...

R6#show mpls ldp neighbor 172.100.1.1 detail
   Peer LDP Ident: 172.100.1.1:0; Local LDP Ident 172.100.6.6:0
   TCP connection: 172.100.1.1.646 - 172.100.6.6.11819
   Password: not required, none, in use
   State: Oper; Mqs sent/rcvd: 61/59; Downstream; Last TIB rev sent 89
   Up time: 00:07:13; UID: 4; Peer Id 3;
   LDP discovery sources:
   Ethernet1/0; Src IP addr: 172.31.10.25
   holdtime: 15000 ms, hello interval: 5000 ms
   Targeted Hello 172.100.6.6 -> 172.100.1.1, active, passive;
   holdtime: infinite, hello interval: 10000 ms
   Addresses bound to peer LDP Ident:
   172.31.10.25  172.31.10.30  172.31.10.41  172.31.10.33
   172.31.10.14  172.31.10.10  172.31.100.100  172.100.1.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
LDP Session Protection enabled, state: Ready
duration: 30 seconds
<Output omitted>...
Note:

The route distinguisher RD is used to create a unique 96 bit address called the VPNv4 address. It has only one purpose, to make IPv4 prefixes globally unique. It is used by the PE routers to identify which VPN a packet belongs to, e.g. to enable a router to distinguish between 10.0.0.1/8 for Customer A and 10.0.0.1/8 for Customer B. The route distinguisher is made up of an 8 octet field prefixed to the customer IPv4 address, the resulting 12 octet field make a unique VPNv4 address. On this please refer to RFC 4364.

![Route Distinguisher and IPv4 Address Diagram](image)

The RD value used in the network is entirely the choice of the network admin. There are best practices but the number chosen can be any value to make sure the VPNv4 address is unique. Some engineers choose to use the AS number followed by a site ID, e.g. 65335:10 Where 65335 is the AS number for the site and 10 is a site ID.

The route target on the other hand is an 8 byte field which is a BGP extended Communities Attribute defined in RFC 4360. It defines which prefixes are exported and imported on the PE routers.

The route distinguisher makes a unique VPNv4 address across the MPLS network. The route target defines which prefixes get imported and exported on the PE routers.

The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature introduces the `vrf upgrade-cli multi-af-mode {common-policies | non-common-policies} [vrf vrf-name]` command that forces VRF configuration migration from a single-protocol VRF model to a multiprotocol VRF model:

- If the route-target policies apply to all address families configured in the multi-AF VRF, select the common-policies keyword.
- If the route-target policies apply only to the IPv4 address family that you are migrating, select the non-common-policies keyword.

After you enter the `vrf upgrade-cli` command and save the configuration to NVRAM, the single-protocol VRF configuration is saved as a multiprotocol VRF configuration. In the upgrade process, the `ip vrf` command is converted to the `vrf definition` command (global configuration commands) and the `ip vrf forwarding` command is converted to the `vrf forwarding` command (interface configuration command). The `vrf upgrade-cli` command has a one-time immediate effect.

*directly from Cisco website*
VRF Berlin-HQRO

Configure VRF Berlin-HQRO on all relevant devices – refer to the MPLS VPN Topology
PC#4 and Sales#1 PC are simulating two distant customer sites in EIGRP AS200 that are connected
with a L3VPN provided by your core network.
BGP AS5934 and AS10001 must exchange VPN prefixes via BGP using rd:300:300 and the same value
for both route targets.
R2 R3 R6 R7 R92 R93 must be configured as PE routers
R1 must be configured as P router
R14 and R21 must be configured as CE routers.
Configure ‘mpls ldp explicit-null’ on all PEs.
At the end of this task user in Berlin HQ PC#4 should be able to establish ICMP connectivity with the
Sales#1 PC in Berlin Remote Office over the MPLS Infrastructure.
Use relevant IGP routing protocol between PE-CE routers – refer to the MPLS VPN Topology.
Use Option 1 ‘Back to Back VRF’ to establish MPLS connectivity.

In case one of the PE router failure ensure there is redundancy in place.
R92 and R93 Serial link should be configured for Option 3 ‘mpls bgp forwarding’.

Configuration:

R21
router eigrp 200
  network 140.60.88.46 0.0.0.0
  network 140.60.88.70 0.0.0.0
  no passive-interface Ethernet0/0.222
  no passive-interface Ethernet0/0.322

R2
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

  interface Ethernet0/0.222
  ip vrf forwarding Berlin-HQRO
  ip address 140.60.88.45 255.255.255.252

router eigrp 200
  address-family ipv4 vrf Berlin-HQRO autonomous-system 200
  redistribute bgp 5934 metric 1000 1 255 1 1500
  network 140.60.88.45 0.0.0.0
  exit-address-family

router bgp 5934
  address-family ipv4 vrf Berlin-HQRO
  redistribute eigrp 200
  exit-address-family
R3
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

interface Ethernet0/0.322
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.69 255.255.255.252

router eigrp 200
address-family ipv4 vrf Berlin-HQRO autonomous-system 200
 redistribute bgp 5934 metric 1000 1 255 1 1500
 network 140.60.88.69 0.0.0.0
exit-address-family

router bgp 5934
address-family ipv4 vrf Berlin-HQRO
 redistribute eigrp 200
exit-address-family

R6
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

interface Ethernet0/0.93
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.37 255.255.255.252

router bgp 5934
address-family ipv4 vrf Berlin-HQRO
 neighbor 140.60.88.38 remote-as 10001
neighbor 140.60.88.38 activate
exit-address-family

R7
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

interface Ethernet0/0.96
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.62 255.255.255.252

router bgp 5934
address-family ipv4 vrf Berlin-HQRO
 neighbor 140.60.88.61 remote-as 10001
neighbor 140.60.88.61 activate
exit-address-family
R93
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

interface Ethernet3/0.96
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.61 255.255.255.252

router bgp 10001
address-family ipv4 vrf Berlin-HQRO
neighbor 140.60.88.62 remote-as 5934
neighbor 140.60.88.62 activate

R92
ip vrf Berlin-HQRO
rd 300:300
route-target export 300:300
route-target import 300:300

interface Ethernet0/0
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.26 255.255.255.252

interface Ethernet2/0.93
ip vrf forwarding Berlin-HQRO
ip address 140.60.88.38 255.255.255.252

router eigrp 200
address-family ipv4 vrf Berlin-HQRO autonomous-system 200
redistribute bgp 10001 metric 1000
network 140.60.88.26 0.0.0.0
exit-address-family

router bgp 10001
address-family ipv4 vrf Berlin-HQRO
redistribute eigrp 200
neighbor 140.60.88.37 remote-as 5934
neighbor 140.60.88.37 activate

R14
router eigrp 200
network 140.60.88.25 0.0.0.0
no passive-interface Ethernet0/0

Verification:

Note: Check R21 PE Eigrp neighbours

R21#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS (200)
H Address Interface Hold Uptime SRTT RTO Q Seq
  (sec) (ms) Cnt Num
1 140.60.88.69 EtD/0.322 12 00:00:23 5 100 0 3
0 140.60.88.45 EtD/0.222 12 00:01:23 13 100 0 3

Note: Check routing table for VRF Berlin-HQRO on both CE routers R2 and R3
Note: Check connectivity from R2 and R3 CE to PC#4

R2#ping vrf Berlin-HQRO 192.168.50.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms

R3#ping vrf Berlin-HQRO 192.168.50.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms

Note: To make it easier to read debug messages we will temporarily shut down the connection between R6 and R92
R6(config)#int et 0/0.93
R6(config-subif)#shu

*Dec 25 15:04:32.099: %BGP-5-NBR_RESET: Neighbor 140.60.88.38 reset (Interface flap)
*Dec 25 15:04:32.100: %BGP-5-ADJCHANGE: neighbor 140.60.88.38 vpn vrf Berlin-HQRO Down Interface flap

R6#debug bgp vpnv4 unicast updates
BGP updates debugging is on for address family: VPNv4 Unicast
R6#clear bgp vpnv4 unicast * so in
BGP: nbr_topo global 172.100.1.1 VPNv4 Unicast:base (0x38F3BB8:1) rcvd Refresh Start-of-RIB

BGP(4): 172.100.1.1 rcvd UPDATE w/ attr: nexthop 172.100.2.2, origin ?, localpref 100, metric 0, originator 172.100.2.2, clusterlist 172.100.1.1, extended community RT:300:300 Cost:pre-bestpath:128:281600 0x8800:32768:0 0x8801:200:25600 0x8802:65280:256000 0x8803:65281:1500 0x8806:0:2352764973

BGP(4): 172.100.1.1 rcvd UPDATE w/ attr: nexthop 172.100.3.3, origin ?, localpref 100, metric 0, originator 172.100.3.3, clusterlist 172.100.1.1, extended community RT:300:300 Cost:pre-bestpath:128:281600 0x8800:32768:0 0x8801:200:153600 0x8802:65281:256000 0x8803:65281:1500 0x8806:0:3222607125

BGP(4): 172.100.1.1 rcvd UPDATE w/ attr: nexthop 192.21.21.21, origin ?, localpref 100, metric 0, originator 192.21.21.21, clusterlist 172.100.1.1, extended community RT:300:300 Cost:pre-bestpath:128:409600 0x8800:32768:0 0x8801:200:153600 0x8802:65281:256000 0x8803:65281:1500 0x8806:0:3222607125

BGP(4): 172.100.1.1 rcvd UPDATE w/ attr: nexthop 192.168.50.0, origin ?, localpref 100, metric 0, originator 192.168.50.0, clusterlist 172.100.1.1, extended community RT:300:300 Cost:pre-bestpath:128:409600 0x8800:32768:0 0x8801:200:153600 0x8802:65281:256000 0x8803:65281:1500 0x8806:0:3222607125

R6#show bgp vpnv4 unicast all | beg Net
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 300:300 (default for vrf Berlin-HQRO)
*1 140.60.88.44/30 172.100.2.2 0 100 0 7
*1 140.60.88.68/30 172.100.3.3 0 100 0 7
*1 192.21.21.21/32 172.100.2.2 409600 100 0 7
*1 192.168.50.0 172.100.2.2 307200 100 0 7

R7#show bgp vpnv4 unicast all | beg Net
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 300:300 (default for vrf Berlin-HQRO)
*1 140.60.88.44/30 172.100.2.2 0 100 0 7
*1 140.60.88.68/30 172.100.3.3 0 100 0 7
*1 192.21.21.21/32 172.100.2.2 409600 100 0 7
*1 192.168.50.0 172.100.2.2 307200 100 0 7

R6#show bgp vpnv4 unicast all 192.168.50.0
BGP routing table entry for 300:300:192.168.50.0/24, version 9
Paths: (1 available, best #1, table Berlin-HQRO)
Not advertised to any peer
Refresh Epoch 4
Local
172.100.2.2 (metric 21) from 172.100.1.1 (172.100.1.1)
Origin incomplete, metric 307200, localpref 100, valid, internal, best
Extended Community: RT:300:300 Cost:pre-bestpath:128:307200 0x8800:32768:0 0x8801:200:51200 0x8802:65281:256000 0x8803:65281:1500 0x8806:0:3222607125
Originator: 172.100.2.2, Cluster list: 172.100.1.1
mpls labels in/out nolabel/20
rx pathid: 0, tx pathid: 0x0
R7#show bgp vpnv4 unicast all 192.168.50.0
BGP routing table entry for 300:300:192.168.50.0/24, version 9
Paths: (1 available, best #1, table Berlin-HQRO)
Not advertised to any peer
Refresh Epoch 2
Local

172.100.2.2 (metric 21) from 172.100.1.1 (172.100.1.1)
Origin incomplete, metric 307200, localpref 100, valid, internal, best
Extended Community: RT:300:300 Cost:pre-bestpath:128:307200
0x8800:32768:0 0x8801:200:51200 0x8802:65281:256000 0x8803:65281:1500
Originator: 172.100.2.2, Cluster list: 172.100.1.1
mpls labels in/out nolabel/20
rx pathid: 0, tx pathid: 0x0

Note: Check BGP VPNv4 table for customer prefixes on both CE routers R6 and R7 – please unshut R6 Ethernet0/0.93 ethernet interface

R6#sh bgp vpnv4 unicast all summary | be Neigh
Neighbor | V | AS MsgRcvd MsgSent | TblVer | InQ | OutQ | Up/Down | State/PfxRcd
ger 4 | 140.60.88.38 | 4 | 10001 | 9 | 10 | 147 | 0 | 0 | 00:02:23 | 4
172.100.1.1 | 4 | 5934 | 346 | 251 | 147 | 0 | 0 | 03:27:35 | 4

R6#sh bgp vpnv4 unicast all | be Net
Network | Next Hop | Metric | LocPrf | Weight | Path
Route Distinguisher: 300:300 (default for vrf Berlin-HQRO)
*> 140.60.88.24/30 140.60.88.38 0 10001 ?
*>1 140.60.88.44/30 172.100.2.2 0 100 0 ?
*>1 140.60.88.68/30 172.100.3.3 0 100 0 ?
*> 192.14.14.14/32 140.60.88.38 409600 0 10001 ?
*>1 192.16.60.16/29 140.60.88.38 307200 100 0 ?

Note: We are not receiving any VPNv4 customer prefixes from out BGP neighbour SP#6 R93 ?? and instead the customer prefix for Berlin Remote Office we are reciving from R6 ??

R7#sh bgp vpnv4 unicast all summary | be Neigh
Neighbor | V | AS MsgRcvd MsgSent | TblVer | InQ | OutQ | Up/Down | State/PfxRcd
ger 4 | 140.60.88.61 | 4 | 10001 | 6 | 13 | 173 | 0 | 0 | 00:02:27 | 0
172.100.1.1 | 4 | 5934 | 335 | 233 | 173 | 0 | 0 | 03:29:35 | 8

R7#sh bgp vpnv4 unicast all | be Net
Network | Next Hop | Metric | LocPrf | Weight | Path
Route Distinguisher: 300:300 (default for vrf Berlin-HQRO)
*>1 140.60.88.24/30 140.60.88.61 0 10001 ?
*>1 140.60.88.44/30 172.100.2.2 0 100 0 ?
*>1 140.60.88.68/30 172.100.3.3 0 100 0 ?
*>1 192.14.14.14/32 140.60.88.38 409600 100 0 10001 ?
*>1 192.16.60.16/29 140.60.88.38 307200 100 0 10001 ?
*>1 192.16.60.16/29 172.100.6.6 307200 100 0 10001 ?
*>1 192.16.60.12/30 140.60.88.38 307200 100 0 10001 ?
*>1 192.16.60.12/30 172.100.6.6 307200 100 0 10001 ?
*>1 192.16.60.16/29 172.100.6.6 307200 100 0 10001 ?
Note: In this case let's see what's going on on R93. It seems like we are receiving updates from R7 but then the customer traffic will be blackholed as we have no connectivity with the CE R14 so at the moment there is no redundancy in place meaning that if we lose R6 or R92 then the customer will not be able to establish VPN connectivity between customer both remote locations.

```
R93#show bgp vpnv4 unicast vrf Berlin-HQRO summary | beg Neigh
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
140.60.88.62    4           5934      26      19       31    0    0 00:14:04       4
```

```
R93#show bgp vpnv4 unicast vrf Berlin-HQRO | be Net
Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 300:300 (default for vrf Berlin-HQRO)
*>  140.60.88.44/30  140.60.88.62                           0 5934 ?
*>  140.60.88.68/30  140.60.88.62                           0 5934 ?
*>  192.21.21.21/32  140.60.88.62                           0 5934 ?
*>  192.168.50.0     140.60.88.62                           0 5934 ?
```

Note: As per the question requirements let's use Option 3 in order to pass VPNv4 traffic between R92 and R93.

**Configuration:**

```
R92
router bgp 10001
  address-family vpnv4
    neighbor 86.191.16.9 activate
    neighbor 86.191.16.9 send-community extended
    exit-address-family
    interface Serial4/0
    mpls ldp discovery transport-address interface
    mpls bgp forwarding

R93
router bgp 10001
  address-family vpnv4
    neighbor 86.191.16.10 activate
    neighbor 86.191.16.10 send-community extended
    exit-address-family
    interface Serial5/0
    mpls ldp discovery transport-address interface
    mpls bgp forwarding
```

```
R92#sh mpls interfaces serial 4/0 detail
Interface Serial4/0:
  Type Unknown
  IP labeling not enabled
  LSP Tunnel labeling not enabled
  IP FRR labeling not enabled
  BGP labeling enabled
  MPLS Operational
  MTU = 1500
```
R93#sh mpls interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP</th>
<th>Tunnel</th>
<th>BGP Static</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial5/0</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

R93#sh mpls interfaces serial 5/0 detail

Interface Serial5/0:
- Type Unknown
- IP labeling not enabled
- LSP Tunnel labeling not enabled
- IP FRR labeling not enabled
- **BGP labeling enabled**
- **MPLS operational**
- MTU = 1500

**Note: And finally let’s do some testing:**

PC4#ping 192.14.14.14 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.14.14.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
PC4#ping 192.14.14.14 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.14.14.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 92 percent (92/100), round-trip min/avg/max = 5/10/27 ms

Type escape sequence to abort.
Tracing the route to 192.14.14.14
VRF info: (vrf in name/id, vrf out name/id)
   1 192.168.50.21 0 msec 5 msec 1 msec
   2 140.60.88.69 1 msec 0 msec 0 msec
   3 172.31.10.10 [MPLS: Labels 17/21 Exp 0] 3 msec 4 msec 6 msec
   4 140.60.88.62 [MPLS: Label 21 Exp 0] 9 msec 8 msec 10 msec
   5 140.60.88.61 6 msec 11 msec 5 msec
   6 140.60.88.26 [MPLS: Label 18 Exp 0] 11 msec 7 msec 8 msec
   7 140.60.88.25 7 msec * 13 msec

Note: And we're up and running choosing R3 140.60.88.69 as our exit point :

R2(config-subif)#no sh
R2(config-subif)#
*Dec 25 15:49:06.400: %DUAL-5-NBRCHANGE: EIGRP-IPv4 200: Neighbor 140.60.88.46 (Ethernet0/0.222) is up: new adjacency

Note: Let's now shutdown the link between R93 and R7:

PC4#ping 192.14.14.14 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.14.14.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 51 percent (51/100), round-trip min/avg/max = 1/13/137 ms

R93(config)#int et3/0.96
R93(config-subif)#sh
R93(config-subif)#
*Dec 25 16:00:32.997: %BGP-5-NBR_RESET: Neighbor 140.60.88.62 reset (Interface flap)
*Dec 25 16:00:32.998: %BGP-5-ADJCHANGE: neighbor 140.60.88.62 vpn vrf Berlin-HQRO Down Interface flap
*Dec 25 16:00:32.998: %BGP_SESSION-5-ADJCHANGE: neighbor 140.60.88.62 IPv4 Unicast vpn vrf Berlin-HQRO topology base removed from session Interface flap

Note: The reason why we lost this many packets is because when we shut down Ethernet3/0.96 on R93 then R7 had to wait 180 seconds by default to bring down the connection entirely.
We can see in the below output that R6 still thinks R7 is the best path for 192.14.14.14 prefix before R7 BGP has expired and the router has begun to reconverge.
Note: And this is after the reconvergence.

PC4#ping 192.14.14.14 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.14.14.14, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/62 ms

Type escape sequence to abort.
Tracing the route to 192.14.14.14
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec 5 msec 7 msec
2 140.60.88.45 9 msec 5 msec 2 msec
3 172.31.10.14 [MPLS: Labels 30/58 Exp 0] 4 msec 7 msec 2 msec
4 140.60.88.37 [MPLS: Label 58 Exp 0] 7 msec 26 msec 7 msec
5 140.60.88.38 3 msec 3 msec 3 msec
6 140.60.88.25 4 msec * 2 msec
R3(config)# int et3/0.96
R3(config-subif)# no sh
R3(config-subif)#

*Dec 25 16:09:28.342: %BGP-5-NBR_RESET: Neighbor 140.60.88.62 active reset (BGP Notification sent)
*Dec 25 16:09:28.342: %BGP-5-ADJCHANGE: neighbor 140.60.88.62 vpn vrf Berlin-HQRO Up

Type escape sequence to abort.
Tracing the route to 192.14.14.14
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.50.21 5 msec 5 msec 1 msec
  2 140.60.88.45 1 msec 5 msec 6 msec
  3 172.31.10.14 [MPLS: Labels 17/20 Exp 0] 2 msec 12 msec 3 msec
  4 140.60.88.62 [MPLS: Label 20 Exp 0] 1 msec 3 msec 1 msec
  5 140.60.88.61 2 msec 5 msec 3 msec
  6 140.60.88.26 [MPLS: Label 18 Exp 0] 15 msec 12 msec 7 msec
  7 140.60.88.25 11 msec * 8 msec
**Note:** Configuration of the following MPLS connection will break the previously created IPv6 topology as soon as we assign relevant interfaces into their respective VRFs. The Lab was designed this way on purpose!

**VRF SFG-WHDC**

Warehouse Manager (R21 - Loopback2) need to access files from the File Server (R13 - Loopback1).

Both Customer sites are attached to different MPLS VPN Service Providers.

Both customer sites in BGP AS65001 and AS64784 should be able to establish connectivity over the MPLS VPN.

Use rd:200:200 where appropriate for exchanging clients prefixes over the MPLS VPN.

Ensure your VRF solution is ready for future 6VPE deployment.

Configure eBGP peerings between PE and CE routers using their direct P2P connections.

Use Option 1 back to back VRF between all relevant Service Provider devices.

**Configuration:**

```plaintext
R21
vrf definition SFG-WHDC
    rd 200:200

    address-family ipv4
        route-target export 200:200
        route-target import 200:200
        exit-address-family

    address-family ipv6
        exit-address-family

interface Ethernet0/0.221
    vrf forwarding SFG-WHDC
    ip address 140.60.88.54 255.255.255.252

interface Ethernet0/0.321
    vrf forwarding SFG-WHDC
    ip address 140.60.88.18 255.255.255.252

interface Loopback2
    vrf forwarding SFG-WHDC
    ip address 192.168.199.21 255.255.255.255

router bgp 65001
    address-family ipv4 vrf SFG-WHDC
        network 192.168.199.21 mask 255.255.255.255
        neighbor 140.60.88.17 remote-as 5934
        neighbor 140.60.88.17 activate
        neighbor 140.60.88.53 remote-as 5934
        neighbor 140.60.88.53 activate
        exit-address-family
```
R2
vrf definition SFG-WHDC
rd 200:200

address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet0/0.221
  vrf forwarding SFG-WHDC
  ip address 140.60.88.53 255.255.255.252

router bgp 5934
  address-family ipv4 vrf SFG-WHDC
    neighbor 140.60.88.54 remote-as 65001
    neighbor 140.60.88.54 activate
  exit-address-family

R3
vrf definition SFG-WHDC
rd 200:200

address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet0/0.321
  vrf forwarding SFG-WHDC
  ip address 140.60.88.17 255.255.255.252

router bgp 5934
  address-family ipv4 vrf SFG-WHDC
    neighbor 140.60.88.18 remote-as 65001
    neighbor 140.60.88.18 activate
  exit-address-family
R6
vrf definition SFG-WHDC
rd 200:200

address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet0/0.92
  vrf forwarding SFG-WHDC
  ip address 140.60.88.10 255.255.255.252
  ipv6 address 2001:CC1E:BEF:20:140:60:88:2/64

router bgp 5934
  address-family ipv4 vrf SFG-WHDC
  neighbor 140.60.88.9 remote-as 10001
  neighbor 140.60.88.9 activate
  exit-address-family

R7
vrf definition SFG-WHDC
rd 200:200

address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet0/0.95
  vrf forwarding SFG-WHDC
  ip address 140.60.88.66 255.255.255.252

router bgp 5934
  address-family ipv4 vrf SFG-WHDC
  neighbor 140.60.88.65 remote-as 10001
  neighbor 140.60.88.65 activate
  exit-address-family
R92
vrf definition SFG-WHDC
rd 200:200
address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet2/0.92
vrf forwarding SFG-WHDC
  ip address 140.60.88.9 255.255.255.252
  ipv6 address 2001:CC1E:BEF:20:140:60:88:9/64

interface Ethernet1/0
vrf forwarding SFG-WHDC
  ip address 140.60.88.22 255.255.255.252
  ipv6 address 2001:CC1E:BEF:15:140:60:88:22/64

router bgp 10001
address-family ipv4 vrf SFG-WHDC
  neighbor 140.60.88.10 remote-as 5934
  neighbor 140.60.88.10 activate
  neighbor 140.60.88.21 remote-as 64784
  neighbor 140.60.88.21 activate
  exit-address-family

R93
vrf definition SFG-WHDC
rd 200:200
address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family

address-family ipv6
  exit-address-family

interface Ethernet3/0.95
vrf forwarding SFG-WHDC
  ip address 140.60.88.65 255.255.255.252

router bgp 10001
address-family ipv4 vrf SFG-WHDC
  neighbor 140.60.88.66 remote-as 5934
  neighbor 140.60.88.66 activate
  exit-address-family
R13
vrf definition SFG-WHDC
rd 200:200
  address-family ipv4
  route-target export 200:200
  route-target import 200:200
  exit-address-family
  address-family ipv6
  exit-address-family

interface Ethernet2/0
vrf forwarding SFG-WHDC
ip address 140.60.88.21 255.255.255.252
ipv6 address 2001:CC1E:BEF:15:140:60:88:21/64

interface Loopback1
vrf forwarding SFG-WHDC
ip address 192.168.35.100 255.255.255.255

router bgp 64784
  address-family ipv4 vrf SFG-WHDC
  network 192.168.35.100 mask 255.255.255.255
  neighbor 140.60.88.22 remote-as 10001
  neighbor 140.60.88.22 activate
  exit-address-family

Verification:

R21#sh_ip vrf detail SFG-WHDC
VRF SFG-WHDC (VRF Id = 1);
  default RD 200:200; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x10C
  Interfaces:
    Et0/0.221                Et0/0.321                Lo2
  VRF Table ID = 1
  Flags: 0x0

Export VPN route-target communities
  RT:200:200
Import VPN route-target communities
  RT:200:200
No import route-map
No global export route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix

R21#sh bgp vpnv4 unicast all summary | be Neigh
Neighbor       V  AS MagRcvd MagSent TblVer InQ OutQ Up/Down State/PfxRcd
140.60.88.17   4  5934  15  16  3  0  0 00:10:15 1
140.60.88.53   4  5934  16  16  3  0  0 00:10:50 1
R2#sh bgp vpnv4 unicast rd 200:200 neighbors 140.60.88.17 advertised-routes | be Net
Network     Next Hop     Metric LocPrf Weight Path
Route Distinguisher: 200:200 (default for vrf SFG-WHDC)
*> 192.168.35.100/32
   140.60.88.17     0 5934 10001 64784 i
*> 192.168.199.21/32
   0.0.0.0           0 32768 i
Total number of prefixes 2

R2#sh bgp vpnv4 unicast rd 200:200 neighbors 140.60.88.53 advertised-routes | be Net
Network     Next Hop     Metric LocPrf Weight Path
Route Distinguisher: 200:200 (default for vrf SFG-WHDC)
*> 192.168.35.100/32
   140.60.88.17     0 5934 10001 64784 i
*> 192.168.199.21/32
   0.0.0.0           0 32768 i
Total number of prefixes 2

**Note:** Our VRF configuration looks good!

R2#sh ip vrf detail SFG-WHDC
VRF SFG-WHDC (VRF Id = 2); default RD 200:200; default VPNID <not set>
New CLI format, supports multiple address-families
Flags: 0x180C
Interfaces:
   Et0/0.221
VRF Table ID = 2
Flags: 0x0
**Export VPN route-target communities**
   RT:200:200
**Import VPN route-target communities**
   RT:200:200
No import route-map
No global export route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix

**Note:** And we are also receiving relevant customer prefixes!

R2#sh bgp vpnv4 unicast rd 200:200 neighbors 140.60.88.17 advertised-routes | be Net
Network     Next Hop     Metric LocPrf Weight Path
Route Distinguisher: 200:200 (default for vrf SFG-WHDC)
*> 192.168.35.100/32
   172.100.6.6     0 100 0 10001 64784 i
*> 192.168.199.21/32
   140.60.88.54     0 0 65001 i
R21>ping vrf SFG-WHDC 192.168.35.100 so loo 2 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.35.100, timeout is 2 seconds:
Packet sent with a source address of 192.168.199.21
!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/5/17 ms

R21>traceroute vrf SFG-WHDC ip 192.168.35.100 source loo 2 probe 1
Type escape sequence to abort.
Tracing the route to 192.168.35.100
VRF info: (vrf in name/id, vrf out name/id)

1 140.60.88.53 5 msec
2 172.31.10.14 [MPLS: Labels 30/16 Exp 0] 3 msec
3 140.60.88.10 [MPLS: Label 16 Exp 0] 8 msec
4 140.60.88.9 8 msec
5 140.60.88.21 12 msec

Note: R92 points towards R6 and R13 which is what we expect

R92#sh bgp vpnv4 un rd 200:2
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 200:200 (default for vrf SFG-WHDC)
*
192.168.35.100/32 140.60.88.21 0 0 64784 i
*
192.168.199.21/32 86.191.16.9 0 100 0 5934 65001 i
*>
140.60.88.10

Note: R93 points towards R7 and R92 which is also what we expect due to previously enabled mpls bgp forwarding on R92 and R93 Serial interfaces

R93#sh bgp vpnv4 un rd 200:200 192.168.199.21/32
BGP routing table entry for 200:200:192.168.199.21/32, version 66
Paths: (2 available, best #1, table SFG-WHDC)
Advertised to update-groups:
4
Refresh Epoch 1
5934 65001
140.60.88.66 from 140.60.88.66 (172.100.7.7)
Origin IGP, localpref 100, valid, external, best
Extended Community: RT:200:200
mpls labels in/out 19/nolabel
rx pathid: 0, tx pathid: 0x0
Refresh Epoch 9
5934 65001
86.191.16.10 from 86.191.16.10 (110.1.16.150)
Origin IGP, metric 0, localpref 100, valid, internal
Extended Community: RT:200:200
mpls labels in/out 19/26
rx pathid: 0, tx pathid: 0
R92#sh bgp vpnv4 un rd 200:200 | be Net

Route Distinguisher: 200:200 (default for vrf SFG-WHDC)

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*i 192.168.35.100/32</td>
<td>86.191.16.10</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>64784 i</td>
</tr>
<tr>
<td>*&gt; 192.168.199.21/32</td>
<td>140.60.88.66</td>
<td>0</td>
<td>5934</td>
<td>65001 i</td>
<td></td>
</tr>
</tbody>
</table>

Note: R21 will now start sending ICMP pings towards the File Server behind R13 and we will again simulate a failure by shutting down R6 and R92 Ethernet connection

R92#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R92(config)#int Et2/0.92
R92(config-subif)#shu

*R Dec 25 16:59:19.484: %BGP-5-NBR_RESET: Neighbor 140.60.88.10 reset (Interface flap)
*R Dec 25 16:59:19.488: %BGP-5-ADJCHANGE: neighbor 140.60.88.10 vpn vrf SFG-WHDC Down Interface flap
*R Dec 25 16:59:19.488: %BGP_SESSION-5-ADJCHANGE: neighbor 140.60.88.10 IPv4 Unicast vpn vrf SFG-WHDC topology base removed from session Interface flap

R21#ping vrf SFG-WHDC 192.168.35.100 so loo 2 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.35.100, timeout is 2 seconds:
Packet sent with a source address of 192.168.199.21

.........................!!!!!!!
.................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
.................!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 75 percent (75/100), round-trip min/avg/max = 6/43/326 ms

R21#traceroute vrf SFG-WHDC ip 192.168.35.100 source loo 2 probe 1
Type escape sequence to abort.
Tracing the route to 192.168.35.100
VRF info: (vrf in name/id, vrf out name/id)
1 140.60.88.53 14 msec
2 172.31.10.14 [MPLS: Labels 21/21 Exp 0] 2 msec
3 140.60.88.66 [MPLS: Label 21 Exp 0] 9 msec
4 140.60.88.65 6 msec
5 140.60.88.22 [MPLS: Label 24 Exp 0] 27 msec
6 140.60.88.21 39 msec

R92#sh ip vrf
Name Default RD Interfaces
Berlin-HQRO 300:300 Et0/0
SFG-WHDC 200:200 Et1/0 Et2/0.92

Note: All is well!
**Note:**

Using Multiprotocol Label Switching (MPLS) VPN ID you can identify virtual private networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates.

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

Use the `vpn id` command and specify the VPN ID in the following format:

```
vpn id oui:vpn-index
```

A colon separates the OUI from the VPN index. See the `vpn id` command reference page for more information.

- **oui**—An organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets.
- **vpn-index**—This value identifies the VPN within the company. This VPN index is restricted to four octets.

Each VRF configured in a PE router can have a VPN ID. Use the same VPN ID for the PE routers that belong to the same VPN. Make sure the VPN ID is unique for each VPN in the Service Provider network.

*directly from Cisco website*
According to RFC 4577, OSPF for BGP/MPLS IP VPNs, when must the down bit be set when an OSPF route is distributed from the PE to the CE, for Type 3 and Type 5 LSAs

If an OSPF route is advertised from a PE router into an OSPF area, the Down bit (DN) is set. Another PE router in the same area does not redistribute this route into iBGP of the MPLS VPN network if down is set. When a type 3 LSA is sent from a PE router to a CE router, the DN bit in the LSA Options field MUST be set. This is used to ensure that if any CE router sends this type 3 LSA to a PE router, the PE router will not redistribute it further. When a PE router needs to distribute to a CE router a route that comes from a site outside the latter’s OSPF domain, the PE router presents itself as an ASBR (Autonomous System Border Router), and distributes the route in a type 5 LSA. The DN bit [OSPF-DN] MUST be set in these LSAs to ensure that they will be ignored by any other PE routers that receive them.

The DN Bit

When a type 3 LSA is sent from a PE router to a CE router, the DN bit [OSPF-DN] in the LSA Options field MUST be set. This is used to ensure that if any CE router sends this type 3 LSA to a PE router, the PE router will not redistribute it further.

When a PE router needs to distribute to a CE router a route that comes from a site outside the latter’s OSPF domain, the PE router presents itself as an ASBR (Autonomous System Border Router), and distributes the route in a type 5 LSA. The DN bit [OSPF-DN] MUST be set in these LSAs to ensure that they will be ignored by any other PE routers that receive them.

There are deployed implementations that do not set the DN bit, but instead use OSPF route tagging to ensure that a type 5 LSA generated by a PE router will be ignored by any other PE router that may receive it.

A special OSPF route tag, which we will call the VPN Route Tag, is used for this purpose. To ensure backward compatibility, all implementations adhering to this specification MUST by default support the VPN Route Tag procedures. When it is no longer necessary to use the VPN Route Tag in a particular deployment, its use (both sending and receiving) may be disabled by configuration.

*directly from RFC 4577*
**VRF Berlin-DCWH**

Berlin HQ Warehouse Network Admin (R21 - Loopback1) has to make a few configuration changes to the DNS Server #2 in Berlin HQ Data Centre. R21 is a fairly old 1841 Router lacking in memory resources. Currently the Business does not have enough budget for an upgrade and it has been decided not to implement any routing protocol for Berlin HQ Warehouse and instead use a specific static default route towards R2 and R3 WAN interfaces.

**Note:** It is not the case in Berlin HQ Data Centre where OSPF Pid 100 should be used for the peering with the Service Provider R93 router.

Configure VRF Berlin-DCWH using VPN id of 0000a100003f6 on all relevant devices. Ensure that your VRF configuration output does match on R2, R7 and R93:

```
R2#sh ip vrf detail Berlin-DCWH
VRF Berlin-DCWH (VRF Id = 3); default RD 192.168.210.21:5934; default VPNID A1:3F6C
  Old CLI format, supports IPv4 only
  Flags: 0x1C
  Interfaces:
    Et0/0.23
  VRF Table ID = 3
  Flags: 0x0
    Export VPN route-target communities
      RT:10001:5934
    Import VPN route-target communities
      RT:5934:10001
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

```
R7#sh ip vrf detail Berlin-DCWH
VRF Berlin-DCWH (VRF Id = 3); default RD 192.168.210.21:5934; default VPNID A1:3F6C
  Old CLI format, supports IPv4 only
  Flags: 0x1C
  Interfaces:
    Et0/0.97
  VRF Table ID = 3
  Flags: 0x0
    Export VPN route-target communities
      RT:5934:10001
    Import VPN route-target communities
      RT:10001:5934
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```
Ensure that as soon as interface Ethernet0/0.223 on R2 or R21 goes down Network Admin is still able to connect to Berlin DNS Server#2 using R3 as a backup path.
ICMP should be sent every 5 seconds with the threshold and timeout set to default.
Do not configure any VRF instance on R6 or R92 for this task (see MPLS diagram).

**Configuration:**

**R21**

```plaintext
ip sla 1
  icmp-echo 140.60.88.49
  frequency 5
  ip sla schedule 1 life forever start-time now

track 1 ip sla 1 reachability

ip route 172.31.100.100 255.255.255.255 140.60.88.49 track 1
ip route 172.31.100.100 255.255.255.255 140.60.88.73 5
```

**R2**

```plaintext
ip vrf Berlin-DCWH
  vpn id A1:3F6C
  route-target export 10001:5934
  route-target import 5934:10001

interface Ethernet0/0.223
  ip vrf forwarding Berlin-DCWH
  ip address 140.60.88.49 255.255.255.252

ip route vrf Berlin-DCWH 192.168.210.21 255.255.255.255 140.60.88.50

router bgp 5934
  address-family ipv4 vrf Berlin-DCWH
  redistribute static
  exit-address-family
```
R3
ip vrf Berlin-DCWH
vpn id A1:3F6C
route-target export 10001:5934
route-target import 5934:10001
interface Ethernet0/0.323
ip vrf forwarding Berlin-DCWH
ip address 140.60.88.73 255.255.255.252
ip route vrf Berlin-DCWH 192.168.210.21 255.255.255.255 140.60.88.74
router bgp 5934
  address-family ipv4 vrf Berlin-DCWH
    redistribute static
exit-address-family

R7
ip vrf Berlin-DCWH
vpn id A1:3F6C
route-target export 5934:10001
route-target import 10001:5934
interface Ethernet0/0.97
ip vrf forwarding Berlin-DCWH
ip address 140.60.88.58 255.255.255.252
router bgp 5934
  address-family ipv4 vrf Berlin-DCWH
  neighbor 140.60.88.57 remote-as 10001
  neighbor 140.60.88.57 activate
exit-address-family

R93
ip vrf Berlin-DCWH
rd 172.31.100.100:10001
vpn id A1:3F6C
route-target export 10001:5934
route-target import 5934:10001
interface Ethernet0/0
ip vrf forwarding Berlin-DCWH
ip address 140.60.88.34 255.255.255.252
interface Ethernet3/0.97
ip vrf forwarding Berlin-DCWH
ip address 140.60.88.57 255.255.255.252
router ospf 100 vrf Berlin-DCWH
  router-id 93.93.93.93
  redistribute bgp 10001 subnets
  network 140.60.88.34 0.0.0.0 area 0
router bgp 10001
  address-family ipv4 vrf Berlin-DCWH
  redistribute ospf 100
  neighbor 140.60.88.58 remote-as 5934
  neighbor 140.60.88.58 activate
exit-address-family
R15
router ospf 100
  no passive-interface Ethernet0/0
  network 140.60.88.33 0.0.0.0 area 0

Verification:

SERVER2#ping 192.168.210.21 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.210.21, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 2/5/10 ms

SERVER2#traceroute 192.168.210.21
Type escape sequence to abort.
Tracing the route to 192.168.210.21
VRF info: (vrf in name/id, vrf out name/id)
  1 172.31.100.15 6 msec 11 msec 4 msec
  2 140.60.88.34 7 msec 1 msec 0 msec
  3 140.60.88.58 1 msec 1 msec 1 msec
  4 172.31.10.33 [MPLS: Labels 22/20 Exp 0] 3 msec 6 msec 2 msec
  5 140.60.88.49 [MPLS: Label 20 Exp 0] 6 msec 6 msec 5 msec
  6 140.60.88.50 62 msec * 3 msec

R2#sh ip route vrf Berlin-DCWH 192.168.210.21
Routing Table: Berlin-DCWH
Routing entry for 192.168.210.21/32
  Known via "static", distance 1, metric 0
  Redistributing via bgp 5934
  Advertised by bgp 5934
  Routing Descriptor Blocks:
    * 140.60.88.50
      Route metric is 0, traffic share count is 1

R3#sh ip route vrf Berlin-DCWH 192.168.210.21
Routing Table: Berlin-DCWH
Routing entry for 192.168.210.21/32
  Known via "static", distance 1, metric 0
  Redistributing via bgp 5934
  Advertised by bgp 5934
  Routing Descriptor Blocks:
    * 140.60.88.74
      Route metric is 0, traffic share count is 1

R21#sh ip sla statistics
IPSLAs Latest Operation Statistics
IPSLA operation id: 1
  Latest RTT: 1 milliseconds
Latest operation start time: 18:51:02 CET Thu Dec 25 2014
Latest operation return code: OK
Number of successes: 10
Number of failures: 0
Operation time to live: Forever
R21#sh track
Track 1
IP SLA 1 reachability
Reachability is Up
1 change, last change 00:01:17
Latest operation return code: OK
Latest RTT (milliseconds) 1
Tracked by:
Static IP Routing 0

R21#sh ip route track-table
ip route 172.31.100.100 255.255.255.255 140.60.88.49 track 1 state is [up]

R7#sh bgp vpnv4 un rd 192.168.210.21:5934 | be Net
Network Next Hop Metric LocPrf Weight Path
*> 140.60.88.32/30 140.60.88.57 0 0 10001 ?
*> 172.15.15.15/32 140.60.88.57 11 0 10001 ?
*> 172.31.100.0/24 140.60.88.57 20 0 10001 ?
*>i 192.168.210.21/32 172.100.2.2 0 100 0 ?

Paths: (1 available, best #1, table Berlin-DCWH)
Advertised to update-groups: 9
Refresh Epoch 7
Local
172.100.2.2 (metric 21) from 172.100.1.1 (172.100.1.1)
Origin incomplete, metric 0, localpref 100, valid, internal, best
Extended Community: RT:10001:5934
Originator: 172.100.2.2, Cluster list: 172.100.1.1
mpls labels in/out nolabel/20
rx pathid: 0, tx pathid: 0x0

R7#sh bgp vpnv4 un rd 192.168.210.21:5934 172.31.100.0/24
BGP routing table entry for 192.168.210.21:5934:172.31.100.0/24, version 827
Paths: (1 available, best #1, table Berlin-DCWH)
Advertised to update-groups: 1
Refresh Epoch 1
10001
140.60.88.57 from 140.60.88.57 (124.19.254.150)
Origin incomplete, metric 20, localpref 100, valid, external, best
Extended Community: RT:5934:10001
mpls labels in/out 51/nolabel
rx pathid: 0, tx pathid: 0x0

SERVER2#ping 192.168.210.21 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.210.21, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
....!!!!!!!!!
Success rate is 95 percent (95/100), round-trip min/avg/max = 1/4/42 ms
**Note:** Everything seems to be working fine so let’s one more time break some stuff

```
R2(config)#int Ethernet0/0.223
R2(config-subif)#sh

R21#
*Dec 25 18:01:13.250: %TRACK-6-STATE: 1 ip sla 1 reachability Up -> Down

R21#sh ip sla statistics
IPSLAs Latest Operation Statistics
IPSLA operation id: 1
  Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 19:02:07 CET Thu Dec 25 2014
Latest operation return code: Timeout
Number of successes: 130
Number of failures: 7
Operation time to live: Forever

R21#sh track
Track 1
  IP sla 1 reachability
  Reachability is Down
    2 changes, last change 00:01:22
    Latest operation return code: Timeout
Tracked by:
  Static IP Routing 0
```

**Note:** Routing has changed as planned

```
R21#sh ip route 172.31.100.100
Routing entry for 172.31.100.100/32
  Known via "static", distance 5, metric 0
  Routing Descriptor Blocks:
    * 140.60.88.73
      Route metric is 0, traffic share count is 1

SERVER2#traceroute 192.168.210.21 pro 1
Type escape sequence to abort.
Tracing the route to 192.168.210.21
VRF info: (vrf in name/id, vrf out name/id)
  1 172.31.100.15 5 msec
  2 140.60.88.34 6 msec
  3 140.60.88.58 2 msec
  4 172.31.10.33 [MPLS: Labels 29/43 Exp 0] 3 msec
    5 140.60.88.73 [MPLS: Label 43 Exp 0] 7 msec
    6 140.60.88.74 9 msec
```

**Note:** We will now unshut R2’s Ethernet interface expecting routing on R2 to go back to its original state

```
R2(config)#int et 0/0.223
R2(config-subif)#no sh
R21# %Dec 25 18:06:18.904: %TRACK-6-STATE: 1 ip sla 1 reachability Down -> Up

R21#sh ip route 172.31.100.100
Routing entry for 172.31.100.100/32
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
  * 140.60.88.49
    Route metric is 0, traffic share count is 1

Note: The requirements are not to configure anything on R92 and R6 which means that when `debug bgp vpnv4 unicast updates` on R92 you should receive console messages `DENIED due to: extended community not supported;` as there is no active VRF created on R92 and R6.

This is what we are expecting at this point

R92#debug bgp vpnv4 unicast updates
BGP updates debugging is on for address family: VPNv4 Unicast
R92#clear bgp vpnv4 unicast * so i
BGP: nbr_topo global 86.191.16.9 VPNv4 Unicast:base (0x2DC8008:1) rcvd Refresh Start-of-RIB
BGP: nbr_topo global 86.191.16.9 VPNv4 Unicast:base (0x2DC8008:1) refresh_epoch is 12
BGP(4): 86.191.16.9 rcvd UPDATE w/ attr: nexthop 86.191.16.9, origin ?, localpref 100, metric 0, extended community RT:10001:5934 OSPF DOMAIN ID:0x0005:0x000000640200 OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:93.93.93.93
BGP(4): 86.191.16.9 rcvd 172.31.100.100:10001:140.60.88.32/30, label 26 -- DENIED due to: extended community not supported;
BGP(4): 86.191.16.9 rcvd UPDATE w/ attr: nexthop 86.191.16.9, origin ?, localpref 100, metric 11, extended community RT:10001:5934 OSPF DOMAIN ID:0x0005:0x000000640200 OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:93.93.93.93
BGP(4): 86.191.16.9 rcvd 172.31.100.100:10001:172.15.15.15/32, label 27 -- DENIED due to: extended community not supported;
BGP(4): 86.191.16.9 rcvd UPDATE w/ attr: nexthop 86.191.16.9, origin ?, localpref 100, metric 20, extended community RT:10001:5934 OSPF DOMAIN ID:0x0005:0x000000640200 OSPF RT:0.0.0.0:2:0 OSPF ROUTER ID:93.93.93.93
BGP(4): 86.191.16.9 rcvd 172.31.100.100:10001:172.31.100.0/24, label 28 -- DENIED due to: extended community not supported;
<Output omitted>

Note: One way to fix this is to apply `no bgp default route-target filter` under BGP process on R92 and R6.

This is a Service Provider topic – it is introduced in the Troubleshooting Lab.
VRF Filtering

In order to limit a Denial of Service attack based on injecting false information into the internet routing table to consume PE routers memory, limit the number of prefixes that are allowed inbound from Service Provider#6:

- For each active IPv4 VRF R6 should accept maximum of 50 prefixes
- In case this is violated router should generate a warning message

R7 should be configured as follows:

- VRF Berlin–DCWH – 40 prefixes, generate a warning message as soon as 30 prefixes are received
- VRF Berlin–HQRO – 50 prefixes, generate a warning message when less then 40 prefixes are in the VRF routing table
- Routes should be reinstalled when they’re back below the threshold of 35 prefixes
- VRF SFG–WHDC– 40 IPv4 prefixes, generate a warning message if exceeded

**Configuration:**

**R6**

```
ip vrf Berlin-HQRO
   maximum routes 50 warning-only
vrf definition SFG-WHDC
   address-family ipv4
   maximum routes 50 warning-only
   exit-address-family
```

**R7**

```
ip vrf Berlin-DCWH
   maximum routes 40 30

ip vrf Berlin-HQRO
   maximum routes 50 40 reinstall 35

vrf definition SFG-WHDC
   address-family ipv4
   maximum routes 40 warning-only
   exit-address-family
```
### Verification:

<table>
<thead>
<tr>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et0/0.93</td>
</tr>
<tr>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et0/0.92</td>
</tr>
</tbody>
</table>

R6#sh ip vrf detail Berlin-HQRO | in Route
Route warning limit 50, current count 10

R6#sh ip vrf detail SFG-WHDC | in Route
Route warning limit 50, current count 4

### Note: And the same on R7

<table>
<thead>
<tr>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlin-DCNH</td>
<td>192.168.210.21:5934</td>
<td>Et0/0.97</td>
</tr>
<tr>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et0/0.96</td>
</tr>
<tr>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et0/0.95</td>
</tr>
</tbody>
</table>

R7#sh ip vrf detail Berlin-DCNH | in Route
Route limit 40, warning limit 30% (12), current count 6

R7#sh ip vrf detail Berlin-HQRO | in Route
Route limit 50, warning limit 40% (20), current count 10

R7#sh ip vrf detail SFG-WHDC | in Route
Route warning limit 40, current count 4
LDP/TDP Label Protection

There are security reasons around false labels being injected into MPLS network. From the P router R1 perspective, ensure that it only accepts LDP/TDP packets from the following neighbours:

```
R1#sh mpls ldp neighbor | in Peer
   Peer LDP Ident: 172.100.7.7:0; Local LDP Ident 172.100.1.1:0
   Peer LDP Ident: 172.100.5.5:0; Local LDP Ident 172.100.1.1:0
   Peer LDP Ident: 172.100.3.3:0; Local LDP Ident 172.100.1.1:0
   Peer LDP Ident: 172.100.4.4:0; Local LDP Ident 172.100.1.1:0
   Peer LDP Ident: 172.100.2.2:0; Local LDP Ident 172.100.1.1:0
   Peer LDP Ident: 172.100.6.6:0; Local LDP Ident 172.100.1.1:0
```

All other/future TDP/LDP attempts should be denied.
Use an extended ACL called MPLSLDP.
We will only configure only R1 and R2 LAN circuit as the same logic applies to all the remaining connections.

**Configuration:**

**R1**
```
ip access-list extended MPLSLDP
   permit udp host 172.100.2.2 eq 646 host 224.0.0.2 eq 646
   permit tcp host 172.100.2.2 host 172.100.1.1 eq 646
   deny tcp any any eq 646
   deny tcp any eq 646 any
   permit ip any any

interface Ethernet2/0
   ip access-group MPLSLDP in
```

**R2**
```
ip access-list extended MPLSLDP
   permit udp host 172.100.1.1 eq 646 host 224.0.0.2 eq 646
   permit tcp host 172.100.1.1 eq 646 host 172.100.2.2
   deny tcp any any eq 646
   deny tcp any eq 646 any
   permit ip any any

interface Ethernet1/0.12
   ip access-group MPLSLDP in
```
Verification:

R1#sh mpl ld ne 172.100.2.2
Peer LDP Ident: 172.100.2.2:0; Local LDP Ident 172.100.1.1:0
TCP connection: 172.100.2.2.58476 - 172.100.1.1.646
State: Oper; Msgs sent/rcvd: 507/514; Downstream
Up time: 06:56:19
LDP discovery sources:
 Ethernet2/0, Src IP addr: 172.31.10.13
Addresses bound to peer LDP Ident:
  172.31.10.13  172.100.2.2  172.100.122.122 172.31.10.1
  172.31.10.17

R1#sh access-lists MPLSLDP
Extended IP access list MPLSLDP
  10 permit udp host 172.100.2.2 eq 646 host 224.0.0.2 eq 646
  20 permit tcp host 172.100.2.2 host 172.100.1.1 eq 646 (19 matches)
  30 deny tcp any any eq 646 (16 matches)
  40 deny tcp any eq 646 any
  50 permit ip any any (154 matches)

R2#sh mpls ldp neighbor 172.100.1.1
Peer LDP Ident: 172.100.1.1:0; Local LDP Ident 172.100.2.2:0
TCP connection: 172.100.1.1.646 - 172.100.2.2.58476
State: Oper; Msgs sent/rcvd: 523/512; Downstream
Up time: 06:59:19
LDP discovery sources:
 Ethernet1/0.12, Src IP addr: 172.31.10.14
Addresses bound to peer LDP Ident:
  172.31.10.25  172.31.10.30  172.31.10.41  172.31.10.33
  172.31.10.14  172.31.10.10  172.31.100.100  172.100.1.1

R2#sh access-lists MPLSLDP
Extended IP access list MPLSLDP
  10 permit udp host 172.100.1.1 eq 646 host 224.0.0.2 eq 646
  20 permit tcp host 172.100.1.1 eq 646 host 172.100.2.2 (42 matches)
  30 deny tcp any any eq 646
  40 deny tcp any eq 646 any (42 matches)
  50 permit ip any any (486 matches)
**Label Filtering**

Ensure that R6 and R7 LIB does not contain label bindings for their respective LDP neighbours R4 and R5.

**Configuration:**

**R6**

access-list 10 deny any
mpls ldp neighbor 172.100.4.4 labels accept 10

**R7**

access-list 10 deny any
mpls ldp neighbor 172.100.5.5 labels accept 10

**Verification: Before**

R6# sh mpls ldp bindings
lib entry: 140.60.88.40/30, rev 21
  local binding: label: imp-null
lib entry: 172.31.10.0/30, rev 50
  local binding: label: 34
  remote binding: lsr: 172.100.4.4:0, label: 29
  remote binding: lsr: 172.100.1.1:0, label: 25
  remote binding: lsr: 172.100.7.7:0, label: 31
lib entry: 172.31.10.4/30, rev 48
  local binding: label: 33
  remote binding: lsr: 172.100.4.4:0, label: 28
  remote binding: lsr: 172.100.1.1:0, label: 24
  remote binding: lsr: 172.100.7.7:0, label: 36
lib entry: 172.31.10.8/30, rev 60
  local binding: label: 39
  remote binding: lsr: 172.100.4.4:0, label: imp-null
  remote binding: lsr: 172.100.7.7:0, label: 27

<output omitted>

R7#sh mpls ldp bindings
lib entry: 140.60.88.40/30, rev 73
  remote binding: lsr: 172.100.6.6:0, label: imp-null
lib entry: 172.31.10.0/30, rev 43
  local binding: label: 31
  remote binding: lsr: 172.100.4.4:0, label: 26
  remote binding: lsr: 172.100.1.1:0, label: 25
  remote binding: lsr: 172.100.6.6:0, label: 34
lib entry: 172.31.10.4/30, rev 54
  local binding: label: 36
  remote binding: lsr: 172.100.5.5:0, label: imp-null
  remote binding: lsr: 172.100.1.1:0, label: 24
  remote binding: lsr: 172.100.6.6:0, label: 33
lib entry: 172.31.10.8/30, rev 34
  local binding: label: 27
  remote binding: lsr: 172.100.5.5:0, label: 25
  remote binding: lsr: 172.100.1.1:0, label: imp-null
  remote binding: lsr: 172.100.6.6:0, label: 39

<output omitted>
Note: After we have made the changes we can see that prefixes are no longer accepted from R4 or R5

R6#sh access-list 10
Standard IP access list 10
  10 deny any log (75 matches)

R7#sh access-list 10
Standard IP access list 10
  10 deny any (50 matches)

R6#sh mpls ldp bindings
lib entry: 140.60.88.40/30, rev 21
  local binding: label: imp-null
lib entry: 172.31.10.0/30, rev 50
  local binding: label: 34
  remote binding: lsr: 172.100.7.7:0, label: 31
  remote binding: lsr: 172.100.1.1:0, label: 25
lib entry: 172.31.10.4/30, rev 48
  local binding: label: 33
  remote binding: lsr: 172.100.7.7:0, label: 36
  remote binding: lsr: 172.100.1.1:0, label: 24
lib entry: 172.31.10.8/30, rev 60
  local binding: label: 39
  remote binding: lsr: 172.100.7.7:0, label: 27
  remote binding: lsr: 172.100.1.1:0, label: imp-null

R7#sh mpls ldp bindings
lib entry: 140.60.88.40/30, rev 73
  remote binding: lsr: 172.100.6.6:0, label: imp-null
lib entry: 172.31.10.0/30, rev 43
  local binding: label: 31
  remote binding: lsr: 172.100.6.6:0, label: 34
  remote binding: lsr: 172.100.1.1:0, label: 25
lib entry: 172.31.10.4/30, rev 54
  local binding: label: 36
  remote binding: lsr: 172.100.6.6:0, label: 33
  remote binding: lsr: 172.100.1.1:0, label: 24
lib entry: 172.31.10.8/30, rev 34
  local binding: label: 27
  remote binding: lsr: 172.100.6.6:0, label: 39
  remote binding: lsr: 172.100.1.1:0, label: imp-null

Note: Let’s clear LDP neighbor connections and enable ‘debug mpls ldp bindings’ on R6 and R7

R1#clear mpls ldp neighbor *
  *Dec 25 19:30:26.337: %LDP-5-NBRCHG: LDP Neighbor 172.100.5.5:0 (2) is DOWN (TCP connection closed by peer)
  *Dec 25 19:30:26.337: %LDP-5-NBRCHG: LDP Neighbor 172.100.3.3:0 (3) is DOWN (TCP connection closed by peer)
  *Dec 25 19:30:27.441: %LDP-5-CLEAR_NBR: Clear LDP neighbors (*) by console
  *Dec 25 19:30:27.451: %LDP-5-NBRCHG: LDP Neighbor 172.100.7.7:0 (1) is DOWN (User cleared session manually)
  *Dec 25 19:30:27.451: %LDP-5-NBRCHG: LDP Neighbor 172.100.6.6:0 (5) is DOWN (User cleared session manually)
  *Dec 25 19:30:28.111: %LDP-5-NBRCHG: LDP Neighbor 172.100.1.1:0 (9) is UP
  *Dec 25 19:30:28.443: %LDP-5-NBRCHG: LDP Neighbor 172.100.3.3:0 (8) is UP
  *Dec 25 19:30:31.096: %LDP-5-NBRCHG: LDP Neighbor 172.100.7.7:0 (10) is UP
  *Dec 25 19:30:31.604: %LDP-5-NBRCHG: LDP Neighbor 172.100.6.6:0 (9) is UP
  *Dec 25 19:30:36.109: %LDP-5-NBRCHG: LDP Neighbor 172.100.2.2:0 (1) is UP
Note: Exactly what we expected
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.4/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.36/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.40/30
LDP: discarding lbl binding from 172.100.5.5 for 172.100.5.5/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.55.55/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.122.122/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.7.7/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.2.2/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.1.1/32
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.44/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.28/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.24/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.16/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.8/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.0/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.32/30
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.12/30
LDP: discarding lbl binding from 172.100.5.5 for 172.100.133.133/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.33.33/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.6.6/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.4.4/32
LDP: discarding lbl binding from 172.100.5.5 for 172.100.3.3/32
LDP: discarding lbl binding from 172.100.5.5 for 172.31.10.20/30
LDP: discarding lbl binding from 172.100.5.5 for 172.100.166.166/32
Dec 25 19:30:31.094: %LDP-5-NEIGHG: LDP Neighbor 172.100.1.1:0 (1) is UP
tagcon: 172.100.1.1:0: 172.31.10.25 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.30 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.41 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.33 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.14 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.10 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.31.10.100 added to addr<->ldp ident map
tagcon: 172.100.1.1:0: 172.100.1.1 added to addr<->ldp ident map
tib: 172.31.10.8/30: learn binding 1 from 172.100.1.1:0
tib: a new binding to be added
tagcon: tibent(172.31.10.8/30): label imp-null from 172.100.1.1:0 added
tib: next hop for route 172.31.10.8/30(0, 172.31.10.33, Et1/0.17) is mapped to peer 172.100.1.1:0
VRF Route Leaking

Establish connectivity between office belonging to VRF SFG-WHDC and VRF Berlin-HQRO

Users and Servers in these locations should be able to communicate with each other

You can only make changes on four devices within the MPLS topology

Your solution should produce the following output:

```
R93#sh ip vrf detail Berlin-HQRO | be Import
  Import VPN route-target communities
  RT:300:300  RT:200:200
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

R93#sh ip vrf detail SFG-WHDC | be Import
  Import VPN route-target communities
  RT:200:200  RT:300:300
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

**Configuration:**

```
R2
  ip vrf Berlin-HQRO
  route-target import 200:200

  vrf definition SFG-WHDC
  address-family ipv4
  route-target import 300:300
  exit-address-family

R3
  ip vrf Berlin-HQRO
  route-target import 200:200

  vrf definition SFG-WHDC
  address-family ipv4
  route-target import 300:300
  exit-address-family
```
**Verification:**

<table>
<thead>
<tr>
<th>R2#sh ip vrf</th>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Berlin-DCWH</td>
<td>192.168.210.21:5934</td>
<td>Et0/0.223</td>
</tr>
<tr>
<td></td>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et0/0.222</td>
</tr>
<tr>
<td></td>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et0/0.221</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R3#sh ip vrf</th>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Berlin-DCWH</td>
<td>192.168.210.21:5934</td>
<td>Et0/0.323</td>
</tr>
<tr>
<td></td>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et0/0.322</td>
</tr>
<tr>
<td></td>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et0/0.321</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R92#sh ip vrf</th>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et0/0</td>
</tr>
<tr>
<td></td>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et1/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R93#sh ip vrf</th>
<th>Name</th>
<th>Default RD</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Berlin-DCWH</td>
<td>172.31.100.100:10001</td>
<td>Et0/0</td>
</tr>
<tr>
<td></td>
<td>Berlin-HQRO</td>
<td>300:300</td>
<td>Et3/0.96</td>
</tr>
<tr>
<td></td>
<td>SFG-WHDC</td>
<td>200:200</td>
<td>Et3/0.95</td>
</tr>
</tbody>
</table>

**Note:** We will now begin our testing PC#4 – File Server

PC4#ping 192.168.35.100 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.35.100, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 2/5/10 ms
**Note:** We will now begin our testing PC#4 – Warehouse Manager

PC4#ping 192.168.199.21 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.199.21, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/13 ms

**Note:** File Server – Sales PC #1

R13#ping vrf SFG-WHDC 192.14.14.14 so loo 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.14.14.14, timeout is 2 seconds:
Packet sent with a source address of 192.168.35.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms
VRF/Global Route Leaking

Establish connectivity between VRF Berlin-HQRO (R21) and the Global routing table
Do not use any form of standard redistribution
PC#4 and R21 must be able to reach remote office location within your topology
For example: both Global NTP server prefixes 63.69.0.150/32 and 194.35.252.7/32 should appear in the VRF Berlin-HQRO routing table and become reachable from PC#4 and R21 (Ethernet1/0)
You are only allowed to configure R92 for this task
R14 should already be able to connect to both NTP Server based on its static default route configured in the earlier sections

Configuration:

R92
ip prefix-list GLOBAL-IN-VRF seq 5 permit 0.0.0.0/0 le 32
ip prefix-list VRF-IN-GLOBAL seq 5 permit 0.0.0.0/0 le 32

route-map GLOBAL-IN-VRF permit 10
match ip address prefix-list GLOBAL-IN-VRF

route-map VRF-IN-GLOBAL permit 10
match ip address prefix-list VRF-IN-GLOBAL

ip vrf Berlin-HQRO
import ipv4 unicast map GLOBAL-IN-VRF
export ipv4 unicast map VRF-IN-GLOBAL

Verification:

R92# sh ip pref
ip prefix-list GLOBAL-IN-VRF: 1 entries
  seq 5 permit 0.0.0.0/0 le 32
ip prefix-list VRF-IN-GLOBAL: 1 entries
  seq 5 permit 0.0.0.0/0 le 32

R92#sh ip vrf detail Berlin-HQRO
VRF Berlin-HQRO (VRF Id = 1); default RD 300:300; default VPNID <not set>
  Old CLI format, supports IPv4 only
  Flags: 0xC
  Interfaces:
    Et0/0
    Et2/0.93
  VRF Table ID = 1
  Flags: 0x2100
  Export VPN route-target communities
    RT:300:300
  Import VPN route-target communities
    RT:300:300
    RT:200:200
  Import route-map for ipv4 unicast: GLOBAL-IN-VRF (prefix limit: 1000)
  Global export route-map for ipv4 unicast: VRF-IN-GLOBAL (prefix limit: 1000)
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
**Note:** As soon as the leaking kicks in R6 and R7 should begin complaining about two many prefixes being injected into the Berlin-HQRO VRF based on one of the previous tasks.

R6>*

*Dec 25 20:35:21.130: %IPRT-3-ROUTELIMITEXCEEDED: IP routing table limit exceeded - Berlin-HQRO
*Dec 25 20:35:22.298: %IPRT-3-ROUTELIMITEXCEEDED: IP routing table limit exceeded - Berlin-HQRO
R7>*

R6#sh ip vrf detail Berlin-HQRO
VRF Berlin-HQRO (VRF Id = 1); default RD 300:300; default VPNID <not set>
  Old CLI format, supports IPv4 only
  Flags: 0xC
  Interfaces:
  Et0/0.93
  VRF Table ID = 1
  Flags: 0x0
  Export VPN route-target communities
    RT:300:300
  Import VPN route-target communities
    RT:300:300
  No import route-map
  No global export route-map
  No export route-map
  **Route warning limit 50, current count 96**
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix

R7#sh ip vrf detail Berlin-HQRO
VRF Berlin-HQRO (VRF Id = 1); default RD 300:300; default VPNID <not set>
  Old CLI format, supports IPv4 only
  Flags: 0xC
  Interfaces:
  Et0/0.96
  VRF Table ID = 1
  Flags: 0x0
  Export VPN route-target communities
    RT:300:300
  Import VPN route-target communities
    RT:300:300
  No import route-map
  No global export route-map
  No export route-map
  **Route limit 50, warning limit 40% (20), current count 50**
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Note: And it looks like PC#4 and R21 finally can reach every remote location outside IP Address including the servers

PC4#tclsh
PC4(tcl)#foreach CCIE {
>+155.84.74.25
>+155.84.74.30
>+155.84.74.34
>+155.84.74.38
>+155.84.74.41
>+155.84.74.18
>+155.84.74.22
>+117.3.48.150
>+63.69.0.150
>+86.13.117.119
>+124.13.240.150
>+75.6.224.150
>+194.35.252.7
>+4.2.2.2

} { ping $CCIE time 5 re 15 }
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.25, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 16/30/73 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.30, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 9/13/21 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.34, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 11/13/24 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.38, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 19/23/32 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.41, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 19/23/28 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.18, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 20/26/44 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.22, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 17/24/33 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.1, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 18/21/26 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 117.3.48.150, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 19/25/35 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 63.69.0.150, timeout is 5 seconds:
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 10/13/16 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 86.13.117.119, timeout is 5 seconds:
!!!!!!!!!!!!!!!
PC4(tcl)#tclquit

PC4#tclsh

PC4(tcl)#foreach CCIE {
    +>155.84.74.25
    +>155.84.74.30
    +>155.84.74.34
    +>155.84.74.38
    +>155.84.74.41
    +>155.84.74.18
    +>155.84.74.22
    +>155.84.74.1
    +>117.3.48.150
    +>63.69.0.150
    +>86.13.117.119
    +>124.13.240.150
    +>75.6.224.150
    +>194.35.252.7
    +>4.2.2.2
    +} { traceroute $CCIE pro 1 }

Type escape sequence to abort.

Tracing the route to 155.84.74.25

VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 0 msec
2 140.60.88.45 1 msec
3 140.60.88.37 [MPLS: Label 134 Exp 0] 2 msec
4 140.60.88.38 3 msec
5 86.191.16.9 13 msec
6 66.171.14.9 11 msec
7 66.171.14.5 11 msec
8 66.171.14.1 21 msec
9 155.84.74.25 70 msec

Type escape sequence to abort.

Tracing the route to 155.84.74.30

VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec
2 140.60.88.69 11 msec
3 172.31.10.10 [MPLS: Labels 30/104 Exp 0] 7 msec
4 140.60.88.37 [MPLS: Label 104 Exp 0] 7 msec
5 140.60.88.38 8 msec
6 86.191.16.9 21 msec
7 66.171.14.9 12 msec
8 66.171.14.14 17 msec
9 155.84.74.30 18 msec

Type escape sequence to abort.
Tracing the route to 155.84.74.34
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec
2 140.60.88.45 11 msec
3 140.60.88.37 [MPLS: Label 105 Exp 0] 8 msec
4 140.60.88.38 12 msec
5 86.191.16.9 14 msec
6 66.171.14.9 12 msec
7 66.171.14.14 14 msec
8 155.84.74.34 13 msec
Type escape sequence to abort.

Tracing the route to 155.84.74.38
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 10 msec
2 140.60.88.69 5 msec
3 172.31.10.10 [MPLS: Labels 30/133 Exp 0] 5 msec
4 140.60.88.37 [MPLS: Label 133 Exp 0] 3 msec
5 140.60.88.38 3 msec
6 86.191.16.9 13 msec
7 66.171.14.9 12 msec
8 155.84.74.38 22 msec
Type escape sequence to abort.

Tracing the route to 155.84.74.41
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 8 msec
2 140.60.88.45 6 msec
3 140.60.88.37 [MPLS: Label 106 Exp 0] 1 msec
4 140.60.88.38 10 msec
5 86.191.16.9 22 msec
6 66.171.14.9 14 msec
7 66.171.14.14 15 msec
8 155.84.74.41 77 msec
Type escape sequence to abort.

Tracing the route to 155.84.74.18
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 0 msec
2 140.60.88.69 5 msec
3 172.31.10.10 [MPLS: Labels 30/99 Exp 0] 5 msec
4 140.60.88.37 [MPLS: Label 102 Exp 0] 2 msec
5 86.191.16.5 16 msec
6 86.191.16.1 22 msec
7 155.84.74.1 21 msec
8 192.168.10.22 24 msec
9 155.84.74.14 23 msec
10 155.84.74.18 28 msec
Type escape sequence to abort.

Tracing the route to 155.84.74.22
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 9 msec
2 140.60.88.45 7 msec
3 140.60.88.37 [MPLS: Label 103 Exp 0] 2 msec
4 140.60.88.38 3 msec
5 86.191.16.5 11 msec
6 86.191.16.1 20 msec
7 155.84.74.1 23 msec
8 192.168.10.22 33 msec
9 155.84.74.14 22 msec
10 155.84.74.22 24 msec
Type escape sequence to abort.

Tracing the route to 155.84.74.1
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 7 msec
2 140.60.88.69 6 msec
3 172.31.10.10 [MPLS: Labels 30/99 Exp 0] 10 msec
4 140.60.88.37 [MPLS: Label 99 Exp 0] 2 msec
5 140.60.88.38 82 msec
6 86.191.16.5 34 msec
7 86.191.16.1 22 msec
8 155.84.74.1 23 msec
Type escape sequence to abort.
Tracing the route to 117.3.48.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 4 msec
2 140.60.88.45 10 msec
3 140.60.88.37 [MPLS: Label 94 Exp 0] 9 msec
4 140.60.88.38 9 msec
5 86.191.16.5 14 msec
6 86.191.16.1 22 msec
7 155.84.74.1 28 msec
8 192.168.10.22 23 msec
9 155.84.74.14 23 msec
Type escape sequence to abort.
Tracing the route to 63.69.0.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec
2 140.60.88.69 6 msec
3 172.31.10.10 [MPLS: Labels 30/46 Exp 0] 6 msec
4 140.60.88.37 [MPLS: Label 46 Exp 0] 6 msec
5 140.60.88.38 7 msec
6 86.191.16.1 101 msec
Type escape sequence to abort.
Tracing the route to 86.13.117.119
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 7 msec
2 140.60.88.69 1 msec
3 172.31.10.10 [MPLS: Labels 30/71 Exp 0] 3 msec
4 140.60.88.37 [MPLS: Label 71 Exp 0] 6 msec
5 140.60.88.38 3 msec
Type escape sequence to abort.
Tracing the route to 124.13.240.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 4 msec
2 140.60.88.45 10 msec
3 140.60.88.37 [MPLS: Label 97 Exp 0] 11 msec
4 140.60.88.38 10 msec
5 86.191.16.9 12 msec
Type escape sequence to abort.
Tracing the route to 75.6.224.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 4 msec
2 140.60.88.45 5 msec
3 172.31.10.10 [MPLS: Labels 30/70 Exp 0] 7 msec
4 140.60.88.37 [MPLS: Label 70 Exp 0] 7 msec
5 140.60.88.38 7 msec
6 86.191.16.9 11 msec
7 66.171.14.9 13 msec
Type escape sequence to abort.
Tracing the route to 194.35.252.7
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec
2 140.60.88.45 5 msec
3 140.60.88.37 [MPLS: Label 107 Exp 0] 7 msec
4 140.60.88.38 8 msec
5 86.191.16.9 14 msec
6 66.171.14.9 7 msec
7 66.171.14.14 12 msec
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 4 msec
2 140.60.88.69 8 msec
3 172.31.10.10 [MPLS: Labels 30/18 Exp 0] 24 msec
4 140.60.88.37 [MPLS: Label 18 Exp 0] 9 msec
5 140.60.88.38 9 msec
6 86.191.16.9 22 msec
7 66.171.14.9 13 msec
8 66.171.14.5 13 msec
PC4(tcl)#tclquit

R21#tclsh
R21(tcl)#foreach CCIE {
+>155.84.74.25
+>155.84.74.30
+>155.84.74.34
+>155.84.74.38
+>155.84.74.41
+>155.84.74.18
+>155.84.74.22
+>155.84.74.1
+>117.3.48.150
+>63.69.0.150
+>86.13.117.119
+>124.13.240.150
+>75.6.224.150
+>194.35.252.7
+>4.2.2.2
+>} { ping $CCIE sou et 1/0 re 15 }
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 20/30/115 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 11/13/18 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.34, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 10/12/17 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 17/21/25 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.41, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 17/24/53 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
!!!!!!!!!!!!!!!
Success rate is 100 percent (15/15), round-trip min/avg/max = 21/23/29 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 20/24/34 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 155.84.74.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 20/22/27 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 20/23/41 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 63.69.0.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 9/14/41 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 86.13.117.119, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 10/12/17 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 10/13/27 ms
Type escape sequence to abort.
Sending 15, 100-byte ICMP Echos to 75.6.224.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.21
Success rate is 100 percent (15/15), round-trip min/avg/max = 8/12/17 ms
R21(tcl)#tclquit
R21#sh ip eig topology summary
EIGRP-IPv4 Topology Table Summary for AS(200)/ID(192.21.21.21)
Head serial 1, next serial 1777
95 routes, 0 pending replies, 0 dummies
Enabled on 2 interfaces, 2 neighbors present on 2 interfaces
Quiescent interfaces:
Et0/0.322
Et0/0.222
**Note: DMVPN**

Provides full meshed connectivity with simple configuration of hub and spoke
Facilitates zero-touch configuration for addition of new spokes
Features automatic IPsec triggering for building an IPsec tunnel (Usable with or without IPsec encryption)
Supports IP Unicast, IP Multicast, and dynamic routing protocols
Supports remote peers with dynamically assigned addresses
Supports spoke routers behind dynamic NAT and hub routers behind static NAT
Dynamic spoke-to-spoke tunnels for scaling partial- or full-mesh VPNs

DMVPN relies on two proven technologies:

**Next Hop Resolution Protocol (NHRP):** Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses

**Multipoint GRE Tunnel Interface:** Single GRE interface to support multiple GRE and IPsec tunnels; simplifies size and complexity of configuration an IPsec tunnel

**NHRP registration**
- Spoke dynamically registers its mapping with NHS
- Supports spokes with dynamic NBMA addresses or NAT

**NHRP resolutions and redirects**
- Supports building dynamic spoke-to-spoke tunnels
- Control and IP Multicast traffic still through hub
- Unicast data traffic direct; reduced load on hub routers

*directly from Cisco website*
### Note: DMVPN

<table>
<thead>
<tr>
<th>Network Type</th>
<th>Route Control</th>
<th>Converge</th>
<th>CPU</th>
<th>Scaling</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EIGRP</strong></td>
<td>Hub-spoke</td>
<td>Good</td>
<td>Faster</td>
<td>High</td>
<td>Lower</td>
</tr>
<tr>
<td></td>
<td>Spoke-spoke</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OSPF</strong></td>
<td>Hub-spoke</td>
<td>Fair</td>
<td>Faster</td>
<td>High</td>
<td>Lower Single area</td>
</tr>
<tr>
<td></td>
<td>Spoke-spoke</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BGP</strong></td>
<td>Hub-spoke</td>
<td>Good</td>
<td>Slower</td>
<td>Medium</td>
<td>Medium* Static neighbor</td>
</tr>
<tr>
<td></td>
<td>Spoke-spoke</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RIPv2</strong></td>
<td>Hub-spoke**</td>
<td>Poor</td>
<td>Slower</td>
<td>Low</td>
<td>High Passive mode needs IP SLA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ODR</strong></td>
<td>Hub-spoke**</td>
<td>None</td>
<td>Slower</td>
<td>Low</td>
<td>High Default route only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### DMVPN Dual Hub

**Single mGRE Tunnel on All Nodes**

Physical: 172.17.0.5
Tunnel: 10.0.0.2

Physical: 172.17.0.1
Tunnel: 10.0.0.1

Physical: (dynamic)
Tunnel: 10.0.0.12

Physical: (dynamic)
Tunnel: 10.0.0.11
Sydney Business Model HQ/Remote Offices

DMVPN

Configure DMVPN phase 3
R19 and R20 must be the spokes and must participate in NHRP information exchange
R17 and R18 must be the hub routers where R18 primary DMVPN Hub and R17 back up secondary DMVPN Hub
Disable send ICMP redirect message on all three tunnel interfaces
There will be a lot of traffic traversing all Tunnel interfaces therefore ensure that each local router collects interface statistics every "half of the default" value
Establish a GRE Multipoint tunnel from each spoke router to the primary and the backup hub router using Tunnel 10 and Tunnel 20 respectively – see DMVPN diagram
Ensure that spoke to spoke traffic does not transit via the hub
Use subnet 10.10.10.X/24 for the tunnel 10 (X is the router number)
Use subnet 20.20.20.X/24 for the tunnel 20 (X is the router number)
Ensure that spokes are able to reach each other's internal subnets
Authenticate NHRP using the string 12345 key for the primary tunnel and 67890 for the secondary tunnel
Use network ID of 12345 and 67890 for both tunnels primary and secondary respectively
Each Tunnel should carry the key ID of 10 and 20 respectively

- Configure the following parameters for Tunnel 10
  - Bandwidth 1000 kbps
  - Delay 10000 msec
  - MTU 1400 bytes
  - TCP mss 1380
  - NHRP hold time to 5 min

- Configure the following parameters for Tunnel 20
  - Bandwidth 100 kbps
  - Delay 10000 msec
  - MTU 1400 bytes
  - TCP mss 1380
  - NHRP hold time to 5 min

Configuration:

R17

```bash
interface Tunnel20
  bandwidth 100
  ip address 20.20.20.17 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication 67890
  ip nhrp map multicast dynamic
  ip nhrp network-id 67890
  ip nhrp holdtime 3600
  ip nhrp redirect
  ip tcp adjust-mss 1380
  load-interval 150
  delay 10000
  tunnel source Ethernet0/0
  tunnel mode gre multipoint
  tunnel key 20
```
router eigrp 250
  network 20.20.20.17 0.0.0.0
  no passive-interface Tunnel20

R18
  interface Tunnel10
    bandwidth 1000
    ip address 10.10.10.18 255.255.255.0
    no ip redirects
    ip mtu 1400
    no ip next-hop-self eigrp 250
    no ip split-horizon eigrp 250
    ip nhrp authentication 12345
    ip nhrp map multicast dynamic
    ip nhrp network-id 12345
    ip nhrp holdtime 3600
    ip nhrp redirect
    ip tcp adjust-mss 1380
    load-interval 150
    delay 100000
    tunnel source Ethernet0/0
    tunnel mode gre multipoint
    tunnel key 10

router eigrp 250
  network 10.10.10.18 0.0.0.0
  no passive-interface Tunnel10

R19
  interface Tunnel10
    bandwidth 1000
    ip address 10.10.10.19 255.255.255.0
    no ip redirects
    ip mtu 1400
    ip nhrp authentication 12345
    ip nhrp map multicast dynamic
    ip nhrp map 10.10.10.18 155.84.74.34
    ip nhrp map multicast 155.84.74.34
    ip nhrp network-id 12345
    ip nhrp holdtime 3600
    ip nhrp nhs 10.10.10.18
    ip nhrp shortcut
    ip tcp adjust-mss 1380
    load-interval 150
    delay 100000
    tunnel source Multilink1
    tunnel mode gre multipoint
    tunnel key 10

interface Tunnel20
  bandwidth 100
  ip address 20.20.20.19 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication 67890
  ip nhrp map multicast dynamic
  ip nhrp map 20.20.20.17 155.84.74.30
  ip nhrp map multicast 155.84.74.30
  ip nhrp network-id 67890
ip nhrp holdtime 3600
ip nhrp nhs 20.20.20.17
ip nhrp shortcut
ip tcp adjust-mss 1380
load-interval 150
delay 10000
tunnel source Multilink1
tunnel mode gre multipoint
tunnel key 20

router eigrp 250
network 10.10.10.19 0.0.0.0
network 20.20.20.19 0.0.0.0
no passive-interface Tunnel10
no passive-interface Tunnel20

interface Tunnel10
   bandwidth 1000
   ip address 10.10.10.20 255.255.255.0
   no ip redirects
   ip mtu 1400
   ip nhrp authentication 12345
   ip nhrp map multicast dynamic
   ip nhrp map 10.10.10.18 155.84.74.34
   ip nhrp map multicast 155.84.74.34
   ip nhrp network-id 12345
   ip nhrp holdtime 3600
   ip nhrp nhs 10.10.10.18
   ip tcp adjust-mss 1380
   load-interval 150
   delay 10000
   tunnel source Serial1/0
   tunnel mode gre multipoint
   tunnel key 10

interface Tunnel20
   bandwidth 100
   ip address 20.20.20.20 255.255.255.0
   no ip redirects
   ip mtu 1400
   ip nhrp authentication 67890
   ip nhrp map multicast dynamic
   ip nhrp map 20.20.20.17 155.84.74.30
   ip nhrp map multicast 155.84.74.30
   ip nhrp network-id 67890
   ip nhrp holdtime 3600
   ip nhrp nhs 20.20.20.17
   ip tcp adjust-mss 1380
   load-interval 150
   delay 10000
   tunnel source Serial1/0
   tunnel mode gre multipoint
   tunnel key 20

router eigrp 250
network 10.10.10.20 0.0.0.0
network 20.20.20.20 0.0.0.0
no passive-interface Tunnel10
no passive-interface Tunnel20
Verification:

**Note:** Once the configuration has been applied we should be able to reach internal LAN interfaces of R19 and R20

**We will test from Server#4 and R16 Loopback0**

SERVER4#ping 192.168.150.19 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.150.19, timeout is 2 seconds:
Success rate is 38 percent (38/100), round-trip min/avg/max = 8/15/62 ms

SERVER4#ping 192.168.160.20 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.160.20, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 82 percent (82/100), round-trip min/avg/max = 7/11/23 ms

**Note:** Also we can see that we are choosing R18 as our exit point being the primary DMVPN Hub

SERVER4#traceroute 192.168.150.19
Type escape sequence to abort.
Tracing the route to 192.168.150.19
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107  6 msec  5 msec  5 msec
2 192.168.110.18  6 msec  2 msec 12 msec
3 10.10.10.19       13 msec * 39 msec

SERVER4#traceroute 192.168.160.20
Type escape sequence to abort.
Tracing the route to 192.168.160.20
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107  5 msec  5 msec  5 msec
2 192.168.110.18  7 msec  4 msec  1 msec
3 10.10.10.20       11 msec * 26 msec

R16#ping 192.168.150.19 so loo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.19, timeout is 2 seconds:
Packet sent with a source address of 192.16.16.16
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/11/16 ms

R16#ping 192.168.160.20 so loo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.20, timeout is 2 seconds:
Packet sent with a source address of 192.168.16.16
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/11/13 ms

R18#sh ip eig ne
EIGRP-IPv4 Neighbors for AS(250)

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold</th>
<th>Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10.10.10.20</td>
<td>Tu10</td>
<td>10 01:07:04</td>
<td>35</td>
<td>210</td>
<td>0</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10.10.10.19</td>
<td>Tu10</td>
<td>12 01:07:42</td>
<td>23</td>
<td>138</td>
<td>0</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>192.168.110.107</td>
<td>Et1/0</td>
<td>12 10:30:02</td>
<td>232</td>
<td>1392</td>
<td>0</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>192.168.110.16</td>
<td>Et1/0</td>
<td>13 10:30:02</td>
<td>162</td>
<td>972</td>
<td>0</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
### R17#sh ip eigrp

**EIGRP-IPv4 Neighbors for AS(250)**

<table>
<thead>
<tr>
<th></th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime (sec)</th>
<th>SRTT (ms)</th>
<th>RTO  (ms)</th>
<th>Q</th>
<th>Seq (Cnt</th>
<th>Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>20.20.20.20</td>
<td>Tu20</td>
<td>12 01:07:20</td>
<td>209</td>
<td>1362</td>
<td>0</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20.20.20.19</td>
<td>Tu20</td>
<td>11 01:07:50</td>
<td>42</td>
<td>1362</td>
<td>0</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>192.168.100.16</td>
<td>Et1/0</td>
<td>10 10:30:19</td>
<td>16</td>
<td>100</td>
<td>0</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>192.168.100.106</td>
<td>Et1/0</td>
<td>12 10:30:29</td>
<td>47</td>
<td>282</td>
<td>0</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

### R19#sh ip eigrp

**EIGRP-IPv4 Neighbors for AS(250)**

<table>
<thead>
<tr>
<th></th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime (sec)</th>
<th>SRTT (ms)</th>
<th>RTO  (ms)</th>
<th>Q</th>
<th>Seq (Cnt</th>
<th>Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.10.10.18</td>
<td>Tu10</td>
<td>12 01:08:31</td>
<td>39</td>
<td>234</td>
<td>0</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>20.20.20.17</td>
<td>Tu20</td>
<td>13 01:08:32</td>
<td>120</td>
<td>1398</td>
<td>0</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

### R20#sh ip eigrp

**EIGRP-IPv4 Neighbors for AS(250)**

<table>
<thead>
<tr>
<th></th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime (sec)</th>
<th>SRTT (ms)</th>
<th>RTO  (ms)</th>
<th>Q</th>
<th>Seq (Cnt</th>
<th>Num</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20.20.20.17</td>
<td>Tu20</td>
<td>12 01:07:36</td>
<td>52</td>
<td>1398</td>
<td>0</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>10.10.10.18</td>
<td>Tu10</td>
<td>11 01:07:36</td>
<td>31</td>
<td>186</td>
<td>0</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Let’s perform few checks on both hubs R17 and R18

### R18#sh dmvpn detail

Legend: Attrb -- S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       # Ent --> Number of NHRP entries with same NBMA peer
       NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
       UpDn Time --> Up or Down Time for a Tunnel

**Interface Tunnel10 is up/up, Addr. is 10.10.10.18, VRF ""**

Tunnel Src./Dest. addr: 155.84.74.34/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect ""
Interface State Control: Disabled
nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.38</td>
<td>10.10.10.19</td>
<td>UP 00:05:45</td>
<td>D</td>
<td>10.10.10.19/32</td>
</tr>
<tr>
<td>1</td>
<td>155.84.74.41</td>
<td>10.10.10.20</td>
<td>UP 00:05:01</td>
<td>D</td>
<td>10.10.10.20/32</td>
</tr>
</tbody>
</table>

Crypto Session Details:

Pending DMVPN Sessions:
### Interface Tunnel20 is up/up, Addr. is 20.20.20.17, VRF ""
- **Tunnel Src./Dest. addr:** 155.84.74.30/MGRE, **Tunnel VRF ""**
- **Protocol/Transport:** "multi-GRE/IP", **Protect ""**
- **Interface State Control:** Disabled
- **nhrp event-publisher : Disabled**

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Addr</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrib</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.38</td>
<td>20.20.20.19</td>
<td>UP</td>
<td>00:08:20</td>
<td>D</td>
<td>20.20.20.19/32</td>
</tr>
<tr>
<td>1</td>
<td>155.84.74.41</td>
<td>20.20.20.20</td>
<td>UP</td>
<td>00:07:38</td>
<td>D</td>
<td>20.20.20.20/32</td>
</tr>
</tbody>
</table>

#### Crypto Session Details:

**Pending DMVPN Sessions:**

<table>
<thead>
<tr>
<th>Target</th>
<th>Via</th>
<th>NBMA</th>
<th>Mode</th>
<th>Intfc</th>
<th>Claimed</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.19/32</td>
<td>10.10.10.19</td>
<td>155.84.74.38</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt; &gt;</td>
</tr>
<tr>
<td>10.10.10.20/32</td>
<td>10.10.10.20</td>
<td>155.84.74.41</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt; &gt;</td>
</tr>
</tbody>
</table>

```python
R17#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
```

**Interface Tunnel20 is up/up, Addr. is 20.20.20.17, VRF ""
- **Tunnel Src./Dest. addr:** 155.84.74.30/MGRE, **Tunnel VRF ""**
- **Protocol/Transport:** "multi-GRE/IP", **Protect ""**
- **Interface State Control:** Disabled
- **nhrp event-publisher : Disabled**

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Addr</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrib</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.38</td>
<td>20.20.20.19</td>
<td>UP</td>
<td>00:08:20</td>
<td>D</td>
<td>20.20.20.19/32</td>
</tr>
<tr>
<td>1</td>
<td>155.84.74.41</td>
<td>20.20.20.20</td>
<td>UP</td>
<td>00:07:38</td>
<td>D</td>
<td>20.20.20.20/32</td>
</tr>
</tbody>
</table>

#### Crypto Session Details:

**Pending DMVPN Sessions:**

<table>
<thead>
<tr>
<th>Target</th>
<th>Via</th>
<th>NBMA</th>
<th>Mode</th>
<th>Intfc</th>
<th>Claimed</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.19/32</td>
<td>10.10.10.19</td>
<td>155.84.74.38</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt; &gt;</td>
</tr>
<tr>
<td>10.10.10.20/32</td>
<td>10.10.10.20</td>
<td>155.84.74.41</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt; &gt;</td>
</tr>
</tbody>
</table>

```python
R18#sh ip nhrp brief
Target         Via            NBMA           Mode   Intfc   Claimed
10.10.10.19/32 | 10.10.10.19    | 155.84.74.38   | dynamic| Tu10    | < >     |
10.10.10.20/32 | 10.10.10.20    | 155.84.74.41   | dynamic| Tu10    | < >     |
```

```python
R18#sh ip nhrp detail
10.10.10.19/32 via 10.10.10.19
Tunnel10 created 00:13:21, expire 00:46:38
Type: dynamic, Flags: unique registered used nhop
NBMA address: 155.84.74.38
10.10.10.20/32 via 10.10.10.20
Tunnel10 created 00:12:38, expire 00:47:21
Type: dynamic, Flags: unique registered used nhop
NBMA address: 155.84.74.41
```

```python
R17#sh ip nhrp brief
Target         Via            NBMA           Mode   Intfc   Claimed
20.20.20.19/32 | 20.20.20.19    | 155.84.74.38   | dynamic| Tu20    | < >     |
20.20.20.20/32 | 20.20.20.20    | 155.84.74.41   | dynamic| Tu20    | < >     |
```

```python
R17#sh ip nhrp detail
20.20.20.19/32 via 20.20.20.19
Tunnel20 created 00:13:33, expire 00:46:26
Type: dynamic, Flags: unique registered used nhop
NBMA address: 155.84.74.38
20.20.20.20/32 via 20.20.20.20
Tunnel20 created 00:12:51, expire 00:47:08
Type: dynamic, Flags: unique registered used nhop
NBMA address: 155.84.74.41
```
Note: And now the spokes R19 and R20

R19#sh dmvpn detail
Legend: Attrb --> S = Static, D = Dynamic, I = Incomplete
N = NATed, L = Local, X = No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel

Interface Tunnel10 is up/up, Addr. is 10.10.10.19, VRF ""
Tunnel Src./Dest. addr: 155.84.74.38/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect ""
Interface State Control: Disabled
nhrp event-publisher : Disabled
IPv4 NHS:
10.10.10.18 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrib</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.34</td>
<td>10.10.10.18</td>
<td>UP</td>
<td>00:19:28</td>
<td>S</td>
<td>10.10.10.18/32</td>
</tr>
</tbody>
</table>

Interface Tunnel20 is up/up, Addr. is 20.20.20.19, VRF ""
Tunnel Src./Dest. addr: 155.84.74.38/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect ""
Interface State Control: Disabled
nhrp event-publisher : Disabled
IPv4 NHS:
20.20.20.17 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

<table>
<thead>
<tr>
<th># Ent</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Add</th>
<th>State</th>
<th>UpDn Tm</th>
<th>Attrib</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.30</td>
<td>20.20.20.17</td>
<td>UP</td>
<td>00:19:22</td>
<td>S</td>
<td>20.20.20.17/32</td>
</tr>
</tbody>
</table>

Crypto Session Details:

Pending DMVPN Sessions:

R19#sh ip nhrp detail
10.10.10.18/32 via 10.10.10.18
Tunnel10 created 00:22:25, never expire
Type: static, Flags: used
NBMA address: 155.84.74.34

20.20.20.17/32 via 20.20.20.17
Tunnel20 created 00:22:19, never expire
Type: static, Flags: used
NBMA address: 155.84.74.30

R19#sh ip nhrp brief

<table>
<thead>
<tr>
<th>Target</th>
<th>Via</th>
<th>NBMA</th>
<th>Mode</th>
<th>Intfc</th>
<th>Claimed</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.18/32</td>
<td>10.10.10.18</td>
<td>155.84.74.34</td>
<td>static</td>
<td>Tu10</td>
<td>&lt; &gt;</td>
</tr>
<tr>
<td>20.20.20.17/32</td>
<td>20.20.20.17</td>
<td>155.84.74.30</td>
<td>static</td>
<td>Tu20</td>
<td>&lt; &gt;</td>
</tr>
</tbody>
</table>
Note: From R19 Ethernet LAN let’s send a ping towards R20 LAN 192.168.160.20

R19#ping 192.168.160.20 so et 0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.20, timeout is 2 seconds:
Packet sent with a source address of 192.168.150.19
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/24/41 ms

R19#sh ip nhrp brief
<table>
<thead>
<tr>
<th>Target</th>
<th>Via</th>
<th>NBMA</th>
<th>Mode</th>
<th>Intfc</th>
<th>Claimed</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.18/32</td>
<td>10.10.10.18</td>
<td>155.84.74.34</td>
<td>static</td>
<td>Tu10</td>
<td>&lt;</td>
</tr>
<tr>
<td>10.10.10.20/32</td>
<td>10.10.10.20</td>
<td>155.84.74.41</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt;</td>
</tr>
<tr>
<td>192.19.19.19/32</td>
<td>192.10.10.10.19</td>
<td>155.84.74.38</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt;</td>
</tr>
<tr>
<td>192.20.20.20/32</td>
<td>192.10.10.20.10</td>
<td>155.84.74.41</td>
<td>dynamic</td>
<td>Tu10</td>
<td>&lt;</td>
</tr>
<tr>
<td>20.20.20.17/32</td>
<td>20.20.20.17</td>
<td>155.84.74.30</td>
<td>static</td>
<td>Tu20</td>
<td>&lt;</td>
</tr>
</tbody>
</table>

R19#sh ip route 192.168.160.0
Routing entry for 192.168.160.0/24
Known via "eigrp 250", distance 90, metric 7705600, type internal
Redistributing via eigrp 250
Last update from 10.10.10.20 on Tunnel10, 00:25:12 ago
Routing Descriptor Blocks:
* 10.10.10.20, from 10.10.10.18, 00:25:12 ago, via Tunnel10
  Route metric is 7705600, traffic share count is 1
  Total delay is 201000 microseconds, minimum bandwidth is 1000 Kbit
  Reliability 255/255, minimum MTU 1400 bytes
  Loading 1/255, Hops 2

R19#sh ip eig topology 192.168.160.0/24
EIGRP-IPv4 Topology Entry for AS(250)/ID(192.19.19.19) for 192.168.160.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 7705600
Descriptor Blocks:
10.10.10.20 (Tunnel10), from 10.10.10.18, Send flag is 0x0
  Composite metric is (7705600/5145600), route is Internal
  Vector metric:
    Minimum bandwidth is 1000 Kbit
    Total delay is 201000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1400
    Hop count is 2
    Originating router is 192.20.20.20
20.20.20.17 (Tunnel20), from 20.20.20.17, Send flag is 0x0
  Composite metric is (30796800/5196800), route is Internal
  Vector metric:
    Minimum bandwidth is 100 Kbit
    Total delay is 203000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1400
    Hop count is 4
    Originating router is 192.20.20.20

Note: Similar outputs should be seen on the other spoke R20
DHCP

R17 must be configured to provide the following parameters for DHCP clients Server#3 and PC#3. Server#3 and PC#3 must be able to obtain IP address on their Ethernet interfaces from R17 over the DMVPN.

Assign IP Address based on the Client ID of Ethernet0/0 interfaces for Server#3 and PC#3.

Use a name of your choice of DHCP pool.

Domain name for the clients should be name `data.co.uk` without the quotes.

DNS servers available for the clients should be R16's Loopback0 IP address.

Server#3 should always obtain .147 and PC#3 should always obtain .100 in the last octet of their IPv4 address.

Clients should not need to renew their IP addresses.

DHCP IP Addresses conflicts should be logged internally on R17.

**Configuration:**

R17

```conf
ip dhcp conflict logging

ip dhcp pool Server#3
    host 192.168.150.147 255.255.255.0
    client-identifier 01aa.bbcc.0053.00
    domain-name data.co.uk
    dns-server 192.16.16.16
    default-router 192.168.150.19
    lease infinite

ip dhcp pool PC#3
    host 192.168.160.100 255.255.255.0
    client-identifier 01aa.bccc.0049.00
    domain-name data.co.uk
    dns-server 192.16.16.16
    default-router 192.168.160.20
    lease infinite
```

R19

```conf
interface Ethernet0/0
    ip helper-address 192.17.17.17
```

R20

```conf
interface Ethernet0/0
    ip helper-address 192.17.17.17
```

SERVER#3

```conf
interface Ethernet0/0
    ip address dhcp client-id Ethernet0/0
```

PC#3

```conf
interface Ethernet0/0
    ip address dhcp client-id Ethernet0/0
```
Verifcation:

SERVER3(config)#interface Ethernet0/0
SERVER3(config-if)#shu
SERVER3(config-if)#
*Dec 25 21:52:59:985: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
SERVER3(config-if)#no sh
*Dec 25 21:53:55:845: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
SERVER3(config-if)#
*Dec 25 21:53:58:878: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.150.147, mask 255.255.255.0, hostname SERVER3

PC3(config)#interface Ethernet0/0
PC3(config-if)#shu
PC3(config-if)#
*Dec 25 21:53:02:846: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Dec 25 21:53:03:851: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
PC3(config-if)#no sh
*Dec 25 21:54:00:238: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Dec 25 21:54:01:238: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
PC3(config-if)#
*Dec 25 21:54:02:551: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.160.100, mask 255.255.255.0, hostname PC3

R17#debug ip dhcp server packet detail
DHCP server packet detail debugging is on.
R17#
*Dec 25 21:53:53:867: DHCPD: Sending DHCPOFFER to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
*Dec 25 21:53:53:867: DHCPD: Sending DHCPACK to client 01aa.bbcc.0053.00 (192.168.150.147).DHCPD: Setting only requested parameters
R17#un all
All possible debugging has been turned off
SERVER4#ping 192.168.160.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/11/15 ms

SERVER4#ping 192.168.150.147
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.147, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/11/16 ms

PC3#ping 192.168.150.147
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.147, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/40/88 ms

Note: As seen below traceroute from PC#3 to Server#3 shows traffic being routed directly from R20 to R19 without going via the hub which means that our DMVPN Phase 3 is working perfectly fine.

PC3#traceroute 192.168.150.147
Type escape sequence to abort.
Tracing the route to 192.168.150.147
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.160.20 5 msec 5 msec 5 msec
  2 10.10.10.19 27 msec 19 msec 18 msec
  3 192.168.150.147 19 msec * 22 msec
DMVPN Routes

Configure R19 to advertise a summary route of 192.168.150/24 outbound on its Tunnel interfaces.

On R20 with a single command convert EIGRP from 32 to 64 bit metric (Classic Mode to Named Mode).

Configure R20 to advertise a summary route of 192.168.160/24 outbound on its Tunnel interfaces.

Ensure that Loopback8 subnet 192.168.168.0/24 is advertise in addition to the summary route.

Configuration:

R19

interface Tunnel10
  ip summary-address eigrp 250 192.168.144.0 255.255.240.0

interface Tunnel20
  ip summary-address eigrp 250 192.168.144.0 255.255.240.0

R20

router eigrp 250
  eigrp upgrade-cli

R20#sh run | se router eigr

router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
  topology base
    redistribute connected route-map CONNECTED
  exit-af-topology
  network 10.10.10.20 0.0.0.0
  network 20.20.20.20 0.0.0.0
  network 192.20.20.20 0.0.0.0
  network 192.168.160.20 0.0.0.0
  eigrp router-id 192.20.20.20
  exit-address-family

  access-list 10 permit 192.168.168.0 0.0.0.255

  route-map LEAK permit 10
  match ip address 10

  router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
  af-interface Tunnel10
    summary-address 192.168.128.0 255.255.192.0 leak-map LEAK
  exit-af-interface

  af-interface Tunnel20
    summary-address 192.168.128.0 255.255.192.0 leak-map LEAK
  exit-af-interface
Verification:

R1#sh ip route eig | be Gate
Gateway of last resort is 155.84.74.33 to network 0.0.0.0

<Output omitted>

```
D 192.168.150.0/24 [90/5145600] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.151.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.152.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.153.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.154.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.155.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.156.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.157.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.158.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.159.0/24 [90/5248000] via 10.10.10.19, 03:29:01, Tunnel10
D 192.168.160.0/24 [90/5145600] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.161.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.162.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.163.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.164.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.165.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.166.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.167.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.168.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.169.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.170.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.171.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.172.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.173.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.174.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
D EX 192.168.175.0/24 [170/5248000] via 10.10.10.20, 03:29:01, Tunnel10
```

Note: After we have made the change all relevant prefixes should be summarised.

R1#sh ip route eig | be Gate
Gateway of last resort is 155.84.74.33 to network 0.0.0.0
```
20.0.0.0/24 is subnetted, 1 subnets
D 20.20.20.0 [90/28211200] via 192.168.110.16, 00:09:11, Ethernet1/0
192.16.16.0/32 is subnetted, 1 subnets
D 192.16.16.16 [90/409600] via 192.168.110.16, 03:48:10, Ethernet1/0
192.17.17.0/32 is subnetted, 1 subnets
D 192.17.17.17 [90/435200] via 192.168.110.16, 03:48:10, Ethernet1/0
192.19.19.0/32 is subnetted, 1 subnets
D 192.19.19.19 [90/5248000] via 10.10.10.20, 03:47:42, Tunnel10
192.20.20.0/32 is subnetted, 1 subnets
D 192.20.20.20 [90/5120032] via 10.10.10.20, 00:09:11, Tunnel10
192.106.106.0/32 is subnetted, 1 subnets
D 192.106.106.106 [90/435200] via 192.168.110.16, 03:48:10, Ethernet1/0
192.107.107.0/32 is subnetted, 1 subnets
192.166.166.0/32 is subnetted, 1 subnets
D 192.166.166.166 [90/409600] via 192.168.110.16, 03:48:10, Ethernet1/0
192.168.120.0/24 [90/5307020] via 192.168.110.16, 03:48:10, Ethernet1/0
192.168.128.0/18 [90/51200032] via 10.10.10.20, 00:07:18, Tunnel10
D 192.168.130.0/24 [90/307456] via 192.168.110.16, 03:48:12, Ethernet1/0
D 192.168.140.0/24 [90/307456] via 192.168.110.16, 03:48:12, Ethernet1/0
D 192.168.144.0/20 [90/5248000] via 10.10.10.19, 00:15:36, Tunnel10
D EX 192.168.168.0/24 [170/51200032] via 10.10.10.20, 00:03:23, Tunnel10
```
DMVPN Encryption

Secure the DMVPN tunnel using IPsec according to the following requirements:
IKE phase 1 should be configured as per the following requirements:

- The key must appear in plain text in the configuration
- All IPsec tunnels must be authenticated using the same IKE phase 1 pre-shared key CCIE
- Module size for DH group calculation must be 1024 bits
- Protection suite policy must be 10

IKE phase 2 should be configured as per the following requirements:

- Use DMVPNSET as transform set name
- Use DMVPNPROFILE as IPsec profile name
- Use IPsec in transport mode
- IPsec protocol ESP and algorithm AES with 128 bits

Configuration:

```
R17
  crypto isakmp policy 10
    encr aes
      authentication pre-share
      group 2
    crypto isakmp key CCIE address 0.0.0.0
  crypto ipsec transform-set DMVPNSET esp-aes
    mode transport
  crypto ipsec profile DMVPNPROFILE
    set transform-set DMVPNSET
  interface Tunnel20
    tunnel protection ipsec profile DMVPNPROFILE shared

R18
  crypto isakmp policy 10
    encr aes
      authentication pre-share
      group 2
    crypto isakmp key CCIE address 0.0.0.0
  crypto ipsec transform-set DMVPNSET esp-aes
    mode transport
  crypto ipsec profile DMVPNPROFILE
    set transform-set DMVPNSET
  interface Tunnel10
    tunnel protection ipsec profile DMVPNPROFILE shared
```
**Verification:**

**R19**

crypto isakmp policy 10
  encr aes
  authentication pre-share
group 2
crypto isakmp key CCIE address 0.0.0.0

crypto ipsec transform-set DMVPNSET esp-aes
  mode transport

crypto ipsec profile DMVPNPROFILE
  set transform-set DMVPNSET

interface Tunnel10
  tunnel protection ipsec profile DMVPNPROFILE shared

interface Tunnel20
  tunnel protection ipsec profile DMVPNPROFILE shared

**R20**

crypto isakmp policy 10
  encr aes
  authentication pre-share
group 2
crypto isakmp key CCIE address 0.0.0.0

crypto ipsec transform-set DMVPNSET esp-aes
  mode transport

crypto ipsec profile DMVPNPROFILE
  set transform-set DMVPNSET

interface Tunnel10
  tunnel protection ipsec profile DMVPNPROFILE shared

interface Tunnel20
  tunnel protection ipsec profile DMVPNPROFILE shared

**Verification:**

R18#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.84.74.41</td>
<td>155.84.74.34</td>
<td>QM_IDLE</td>
<td>1004</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.38</td>
<td>155.84.74.34</td>
<td>QM_IDLE</td>
<td>1003</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.34</td>
<td>155.84.74.41</td>
<td>QM_IDLE</td>
<td>1001</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.38</td>
<td>155.84.74.38</td>
<td>QM_IDLE</td>
<td>1002</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

R20#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.84.74.34</td>
<td>155.84.74.41</td>
<td>QM_IDLE</td>
<td>1001</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.41</td>
<td>155.84.74.38</td>
<td>QM_IDLE</td>
<td>1003</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.41</td>
<td>155.84.74.30</td>
<td>QM_IDLE</td>
<td>1004</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.30</td>
<td>155.84.74.41</td>
<td>QM_IDLE</td>
<td>1002</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.38</td>
<td>155.84.74.41</td>
<td>QM_IDLE</td>
<td>1006</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>155.84.74.41</td>
<td>155.84.74.34</td>
<td>QM_IDLE</td>
<td>1005</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>
```bash
R1#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel

==========================================================================
Interface Tunnel10 is up/up, Addr. is 10.10.10.18, VRF ""
Tunnel Src./Dest. addr: 155.84.74.34/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPNPROFILE"
Interface State Control: Disabled
nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
--- ---------------- -------- --------------------- -------- ------ ------- ------------
1 155.84.74.38    10.10.10.19    UP 01:10:27    D     10.10.10.19/32
1 155.84.74.41    10.10.10.20    UP 01:09:43    D     10.10.10.20/32

Crypto Session Details:
----------------------------------------------------------------------------------
Interface: Tunnel10
Session: [0xA5B34A90]
  Session ID: 0
  IKEv1 SA: local 155.84.74.34/500 remote 155.84.74.38/500 Active
      Capabilities:(none) connid:1003 lifetime:23:56:16
  Session ID: 0
  IKEv1 SA: local 155.84.74.34/500 remote 155.84.74.38/500 Active
      Capabilities:(none) connid:1002 lifetime:23:56:07
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 155.84.74.38
  IPSec FLOW: permit 47 host 155.84.74.34 host 155.84.74.38
      Active SAs: 4, origin: crypto map
      Inbound: #pkts dec'ed 52 drop 0 life (KB/Sec) 4217144/3376
      Outbound: #pkts enc'ed 51 drop 0 life (KB/Sec) 4217144/3376
  Outbound SPI : 0x4A15E75D, transform : esp-aes
  Socket State: Open

Interface: Tunnel10
Session: [0xA5B34B88]
  Session ID: 0
  IKEv1 SA: local 155.84.74.34/500 remote 155.84.74.41/500 Active
      Capabilities:(none) connid:1004 lifetime:23:56:16
  Session ID: 0
  IKEv1 SA: local 155.84.74.34/500 remote 155.84.74.41/500 Active
      Capabilities:(none) connid:1001 lifetime:23:56:07
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1 id: 155.84.74.41
  IPSec FLOW: permit 47 host 155.84.74.34 host 155.84.74.41
      Active SAs: 4, origin: crypto map
      Inbound: #pkts dec'ed 51 drop 0 life (KB/Sec) 4374238/3376
      Outbound: #pkts enc'ed 51 drop 0 life (KB/Sec) 4374238/3376
  Outbound SPI : 0x2559E24A, transform : esp-aes
  Socket State: Open

Pending DMVPN Sessions:
```

R20#sh dmvpn detail
Legend: Attrb --&gt; S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --&gt; Number of NHRP entries with same NBMA peer
NHS Status: E --&gt; Expecting Replies, R --&gt; Responding, W --&gt; Waiting
UpDn Time --&gt; Up or Down Time for a Tunnel

Interface Tunnel10 is up/up, Addr. is 10.10.10.20, VRF ""
Tunnel Src./Dest. addr: 155.84.74.41/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPNPROFILE"
Interface State Control: Disabled
nhrp event-publisher : Disabled
IPv4 NHS:
10.10.10.18 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3

<table>
<thead>
<tr>
<th>#</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Addr State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.34</td>
<td>10.10.10.18</td>
<td>UP 01:15:00</td>
<td>S</td>
<td>10.10.10.18/32</td>
</tr>
<tr>
<td>2</td>
<td>155.84.74.38</td>
<td>10.10.10.19</td>
<td>UP 00:51:30</td>
<td>DT1</td>
<td>10.10.10.19/32</td>
</tr>
<tr>
<td></td>
<td>155.84.74.38</td>
<td>10.10.10.19</td>
<td>UP 00:51:30</td>
<td>DT1</td>
<td>192.168.150.0/24</td>
</tr>
<tr>
<td>2</td>
<td>155.84.74.41</td>
<td>10.10.10.20</td>
<td>UP 00:51:30</td>
<td>DLX</td>
<td>10.10.10.20/32</td>
</tr>
<tr>
<td></td>
<td>155.84.74.41</td>
<td>10.10.10.20</td>
<td>UP 00:51:30</td>
<td>DLX</td>
<td>192.168.160.0/24</td>
</tr>
</tbody>
</table>

Interface Tunnel20 is up/up, Addr. is 20.20.20.20, VRF ""
Tunnel Src./Dest. addr: 155.84.74.41/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPNPROFILE"
Interface State Control: Disabled
nhrp event-publisher : Disabled
IPv4 NHS:
20.20.20.17 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

<table>
<thead>
<tr>
<th>#</th>
<th>Peer NBMA Addr</th>
<th>Peer Tunnel Addr State</th>
<th>UpDn Tm</th>
<th>Attrb</th>
<th>Target Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>155.84.74.30</td>
<td>20.20.20.17</td>
<td>UP 01:14:55</td>
<td>S</td>
<td>20.20.20.17/32</td>
</tr>
</tbody>
</table>

Crypto Session Details:
Session: [0xA3C04CA8]
Session ID: 0
IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.34/500 Active
Capabilities: (none) connid:1001 lifetime:23:50:50
IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.34/500 Active
Capabilities: (none) connid:1005 lifetime:23:50:59
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_Id: 155.84.74.34
IPSEC FLOW: permit 47 host 155.84.74.41 host 155.84.74.34
Active SAs: 4, origin: crypto map
  Inbound: #pkts dec'ed 120 drop 0 life (KB/Sec) 4363489/3059
  Outbound: #pkts enc'ed 119 drop 0 life (KB/Sec) 4363489/3059
Outbound SPI : 0x296DCC30, transform : esp-aes
Socket State: Open

Interface: Tunnel10 Tunnel20
Session: [0xA3C04DAA0]
Session ID: 0
IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.38/500 Active
Capabilities: (none) connid:1003 lifetime:23:50:50
IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.38/500 Active
Capabilities: (none) connid:1006 lifetime:23:51:00
Socket State: Open
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 155.84.74.38
IPSEC FLOW: permit 47 host 155.84.74.41 host 155.84.74.38
    Active SAs: 4, origin: crypto map
    Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4316223/3060
    Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4316223/3060
Outbound SPI : 0x5ABF421F, transform : esp-aes
Socket State: Open

**Interface: Tunnel10 Tunnel20**
Session: [0xA3C04E98]
    Session ID: 0
    IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.30/500 Active
        Capabilities:(none) connid:1004 lifetime:23:50:59
    Session ID: 0
    IKEv1 SA: local 155.84.74.41/500 remote 155.84.74.30/500 Active
        Capabilities:(none) connid:1002 lifetime:23:50:50
    Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 155.84.74.30
IPSEC FLOW: permit 47 host 155.84.74.41 host 155.84.74.30
    Active SAs: 4, origin: crypto map
    Inbound: #pkts dec'ed 119 drop 0 life (KB/Sec) 4268931/3059
    Outbound: #pkts enc'ed 119 drop 0 life (KB/Sec) 4268931/3059
Outbound SPI : 0x2763D327, transform : esp-aes
Socket State: Open

Pending DMVPN Sessions:
VERIFICATION

Note: As per previous Layer3 section ICMP connectivity between R12 and R20 outside internet interfaces Ethernet0/0 and Serial1/0 should still be working

Please ensure that this is the case before continuing

R20#sh ip route 155.84.74.18
% Subnet not in table

R20#sh ip bgp 155.84.74.18
BGP routing table entry for 0.0.0.0/0, version 2
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65527 35426
155.84.74.42 from 155.84.74.42 (217.0.128.150)
Origin IGP, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0

R20#ping 155.84.74.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/39/42 ms

R20#traceroute 155.84.74.18
Type escape sequence to abort.
Tracing the route to 155.84.74.18
VRF info: (vrf in name/id, vrf out name/id)
1 155.84.74.42 [AS 35426] 10 msec 9 msec 9 msec
2 66.171.14.13 [AS 35426] 15 msec 10 msec 10 msec
3 66.171.14.10 [AS 35426] 10 msec 9 msec 13 msec
4 86.191.16.10 [AS 35426] 18 msec 20 msec 18 msec
5 86.191.16.5 [AS 35426] 32 msec 29 msec 27 msec
6 86.191.16.1 [AS 35426] 34 msec 40 msec 37 msec
7 155.84.74.1 [AS 35426] 40 msec 48 msec 38 msec
8 192.168.10.22 [AS 35426] 36 msec 60 msec 47 msec
9 155.84.74.14 [AS 35426] 43 msec 37 msec 36 msec
10 155.84.74.18 [AS 35426] 42 msec *  40 msec
R12#sh ip route 155.84.74.41
Routing entry for 155.84.74.40/30
   Known via "bgp 64784", distance 20, metric 0
   Tag 15789, type external
   Last update from 155.84.74.17 07:06:04 ago
Routing Descriptor Blocks:
   * 155.84.74.17, from 155.84.74.17, 07:06:04 ago
      Route metric is 0, traffic share count is 1
         AS Hops 7
         Route tag 15789
         MPLS label: none

R12#sh ip bgp 155.84.74.41
BGP routing table entry for 155.84.74.40/30, version 161
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   Refresh Epoch 1
      15789 64784 25432 29737 10001 56775 35426
         155.84.74.17 from 155.84.74.17 (117.3.64.150)
            Origin incomplete, localpref 100, valid, external, best
            rx pathid: 0, tx pathid: 0x0

R12#ping 155.84.74.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.41, timeout is 2 seconds:

   !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/48/64 ms

R12#traceroute 155.84.74.41
Type escape sequence to abort.
Tracing the route to 155.84.74.41
VRF info: (vrf in name/id, vrf out name/id)
   1 155.84.74.17 [AS 15789] 9 msec 5 msec 5 msec
   2 155.84.74.13 [AS 15789] 2 msec 2 msec 0 msec
   3 192.168.10.21 2 msec 6 msec 1 msec
   4 155.84.74.2 [AS 25432] 8 msec 9 msec 6 msec
   5 86.191.16.2 [AS 25432] 12 msec 9 msec 12 msec
   6 86.191.16.6 [AS 29737] 26 msec 21 msec 19 msec
   7 86.191.16.9 [AS 10001] 30 msec 31 msec 33 msec
   8 66.171.14.9 31 msec 30 msec 31 msec
  10 155.84.74.41 [AS 35426] 40 msec * 39 msec
Sydney Business – San Francisco Group – Remote Offices

IPsec VPN

Secure IPsec VPN tunnel between R12 and R20 according to the following requirements.

IKE phase 1 should be configured as per the following requirements:
- Authenticate the tunnel using pre-shared key CCIEVVPN
- Module size for DH group calculation must be 1024bits
- Protection suite policy must be 150

IKE phase 2 must be configured as per the following requirements:
- Use CCIEVSET as transform set name
- Use CCIEMAP as IPsec map name
- Use IPsec in tunnel mode
- IPsec protocol ESP and algorithm AES with 128 bits

Finance User PC#1 – R12(LAN) should be able to ICMP to Multicast Receiver User PC#3 – R20 (LAN)

**Configuration:**

R20

```
crypto isakmp policy 1219
  encr aes
  authentication pre-share
  group 2
crypto isakmp key CISCO address 155.84.74.18

crypto ipsec transform-set MY-SET esp-aes esp-sha256-hmac
  mode tunnel

crypto map VPN_MAP 1219 ipsec-isakmp
  set peer 155.84.74.18
  set transform-set MY-SET
  match address 100

interface Serial1/0
  crypto map VPN_MAP

access-list 100 permit icmp host 192.168.160.100 host 192.168.20.100
```
Verification:

R12#sh cry isa sa
IPv4 Crypto ISAKMP SA
data          src  state     conn-id status
155.84.74.18  155.84.74.41 QM_IDLE  1001 ACTIVE
IPv6 Crypto ISAKMP SA

R20#sh cry isa sa
IPv4 Crypto ISAKMP SA
data          src  state     conn-id status
155.84.74.34  155.84.74.41 QM_IDLE  1001 ACTIVE
155.84.74.41  155.84.74.30 QM_IDLE  1004 ACTIVE
155.84.74.30  155.84.74.41 QM_IDLE  1002 ACTIVE
155.84.74.18  155.84.74.41 QM_IDLE  1007 ACTIVE
IPv6 Crypto ISAKMP SA

IPv4 Crypto ISAKMP SA
data          src  state     conn-id status
155.84.74.18  155.84.74.41 QM_IDLE  1001 ACTIVE
155.84.74.41  155.84.74.34 QM_IDLE  1005 ACTIVE
IPv6 Crypto ISAKMP SA

Note: All the above is looking good but we are not able to ping ??

PC3#ping 192.168.20.100 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.20.100, timeout is 2 seconds:
......................................................................
Success rate is 0 percent (0/100)

PC1#ping 192.168.160.100 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
U.U.U.U.U.
Success rate is 0 percent (0/10)

R20#sh crypto ip sa peer 155.84.74.18
interface: Serial1/0
    Crypto map tag: VPN_MAP, local addr 155.84.74.41
    protected vrf: (none)
    remote ident (addr/mask/prot/port): (192.168.160.100/255.255.255.255/1/0)
    current_peer 155.84.74.18 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encap: 123, #pkts encrypt: 123, #pkts digest: 123
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

<Output omitted>
R12#sh crypto ipsec sa peer 155.84.74.41

interface: Ethernet0/0
  Crypto map tag: VPN_MAP, local addr 155.84.74.18
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.20.100/255.255.255.255/1/0)
  remote ident (addr/mask/prot/port): (192.168.160.100/255.255.255.255/1/0)
  current_peer 155.84.74.41 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encap: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 130, #pkts decrypt: 130, #pkts verify: 130
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

<Output omitted>

Note: Looks like we are encapsulation the packets on R20 outbound and decapsulating inbound on R12 however R12 is not encapsulating any packets form its local LAN outbound ?? Let’s do some ACL specific debug on R12:

R12
  access-list 110 permit ip host 192.168.20.100 any
R12#debug ip packet detail 110
  IP packet debugging is on (detailed) for access list 110

PC1#ping 192.168.160.100 re 1000

R12
  IP: s=192.168.20.100 (Ethernet1/0), d=192.168.160.100, len 100, input feature
    ICMP type=0, code=0, MCI Check(99), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
  FIBipv4-packet-proc: route packet from Ethernet1/0 src 192.168.20.100 dst 192.168.160.100
  FIBfwd-proc: Default:0.0.0.0/0 process level forwarding
    FIBfwd-proc: depth 0 first_idx 0 paths 1 long 0(0)
    FIBfwd-proc: try path 0 (of 1) v4-sp first short ext 0{-1}
    FIBfwd-proc: v4-sp valid
    FIBfwd-proc: no nh type 8 - deag
    FIBfwd-proc: ip_pak_table 0 ip_nh_table 65535 if none nh none deag 1 chg_if 0 via fib 0 path type
      special prefix
    FIBfwd-proc: Default:0.0.0.0/0 not enough info to forward via fib (none none)
  FIBipv4-packet-proc: packet routing failed
    IP: s=192.168.20.100 (Ethernet1/0), d=192.168.160.100, len 100, unroutable
    ICMP type=0, code=0
  FIBipv4-packet-proc: route packet from Ethernet1/0 src 192.168.20.100 dst 192.168.160.100
R12#un all
  All possible debugging has been turned off

Note: Ok so we’ve got a routing issue ! R12 does not know how to route packets from 192.168.20.100 to 192.168.160.100 and that is because if we check the routing table on R12 it contains all specific prefixes but a default route is not there , let’s add a static default route on R12 then and check again :

R12
  ip route 0.0.0.0 0.0.0.0 155.84.74.17
PC1#ping 192.168.160.100 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 35/38/41 ms

PC3#ping 192.168.20.100 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.20.100, timeout is 2 seconds:
!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 39/46/57 ms

R20#sh crypto ip sa peer 155.84.74.18 | in pkts
   #pkts encaps: 589, #pkts encrypt: 589, #pkts digest: 589
   #pkts decaps: 130, #pkts decrypt: 130, #pkts verify: 130
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0

R12#sh crypto ipsec sa peer 155.84.74.41 | in pkts
   #pkts encaps: 130, #pkts encrypt: 130, #pkts digest: 130
   #pkts decaps: 589, #pkts decrypt: 589, #pkts verify: 589
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
Sydney Business Model HQ/Remote Offices

Multicast

Enable DMVPN multicast on all interfaces as specified in the Multicast Diagram. The network should never have to flood and prune multicast traffic unnecessarily. Loopback0 of R16 must be elected as the rendezvous point and also used as the source of the mapping information broadcasts. Use a non-proprietary method to discover and announce the RP information.

Configuration:

R16
ip multicast-routing
interface Ethernet2/0
  ip pim sparse-mode
interface Loopback0
  ip pim sparse-mode
  ip pim rp-candidate Loopback0
  ip pim bsr-candidate Loopback0

SW7
ip multicast-routing
interface Vlan668
  ip pim sparse-mode
interface Vlan50
  ip pim sparse-mode

R18
ip multicast-routing
interface Ethernet1/0
  ip pim sparse-mode
interface Loopback0
  ip pim sparse-mode
interface Tunnel10
  ip pim dr-priority 100
  ip pim nbma-mode
  ip pim sparse-mode

R19
ip multicast-routing
interface Ethernet0/0
  ip pim sparse-mode
interface Tunnel10
  ip pim sparse-mode
R20
ip multicast-routing
interface Ethernet0/0
  ip pim sparse-mode
interface Tunnel10
  ip pim sparse-mode

SERVER#3
interface Ethernet0/0
  ip pim sparse-mode

SERVER#4
interface Ethernet0/0
  ip pim sparse-mode

PC#3
interface Ethernet0/0
  ip pim sparse-mode

Verification:

Tip: As soon as we enable Multicast and configure PIM under the interfaces then the router by default creates Tunnel interfaces. In order to see the configuration of these interfaces we can use `show derived-config interface tunnel 0` command.

R16(config) #
%PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.168.110.16 on interface Ethernet2/0
%PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.16.16.16 on interface Loopback0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up

R16#sh derived-config interface tunnel 0
Building configuration...

Derived configuration : 205 bytes
!
interface Tunnel0
  description Pim Register Tunnel (Encap) for RP 192.16.16.16
  ip unnumbered Loopback0
  tunnel source Loopback0
  tunnel destination 192.16.16.16
  tunnel tos 192
  no routing dynamic
end

R16#sh derived-config interface tunnel 1
Building configuration...

Derived configuration : 189 bytes
!
interface Tunnel1
  description Pim Register Tunnel (Decap) for RP 192.16.16.16
  ip unnumbered Loopback0
  tunnel source Loopback0
  tunnel destination 192.16.16.16
  no routing dynamic
end
R16#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor Address       Interface    Uptime/Expires Ver   DR Prio/Mode
192.168.110.18        Ethernet2/0 00:01:38/00:01:33 v2 1 / S P G
192.168.110.107        Ethernet2/0 00:01:55/00:01:34 v2 1 / DR S P G

R16#sh ip pim rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?), v2
    Info source: 192.16.16.16 (?), via bootstrap, priority 0, holdtime 150
     Uptime: 00:02:31, expires: 00:01:37

R18#sh ip pim rp mapping
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?), v2
    Info source: 192.16.16.16 (?), via bootstrap, priority 0, holdtime 150
     Uptime: 00:02:02, expires: 00:02:28

SERVER4#sh ip pim rp map
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?), v2
    Info source: 192.16.16.16 (?), via bootstrap, priority 0, holdtime 150
     Uptime: 00:00:08, expires: 00:02:21

R19#sh ip pim neigh
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor Address       Interface    Uptime/Expires Ver   DR Prio/Mode
192.168.150.100        Ethernet0/0 00:05:37/00:01:33 v2 1 / DR S P G
10.10.10.18             Tunnel10      00:01:23/00:01:27 v2 100/ DR S P G

R19#sh ip pim rp_map
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?), v2
    Info source: 192.16.16.16 (?), via bootstrap, priority 0, holdtime 150
     Uptime: 00:00:46, expires: 00:01:39

R20#sh ip pim neigh
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor Address       Interface    Uptime/Expires Ver   DR Prio/Mode
192.168.160.100        Ethernet0/0 00:05:38/00:01:30 v2 1 / DR S P G
10.10.10.18             Tunnel10      00:01:29/00:01:43 v2 100/ DR S P G
R20#sh ip pim rp map
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?, v2)
    Info source: 192.16.16.16 (?, via bootstrap, priority 0, holdtime 150
    Uptime: 00:01:00, expires: 00:01:28

PC3#sh ip pim rp map
PIM Group-to-RP Mappings
Group(s) 224.0.0.0/4
  RP 192.16.16.16 (?, v2)
    Info source: 192.16.16.16 (?, via bootstrap, priority 0, holdtime 150
    Uptime: 00:02:09, expires: 00:02:21

**Note:** Looks like we are good from the pim neighborship and the RP perspective
Multicast

Multicast server is located in VLAN 50
Ensure that RP process join requests only for group 237.10.50.67 and 225.0.0.3
Receivers must be able to receive traffic sent to the group 237.10.50.67 and 225.0.0.3 over DMVPN
Do not use any route-map or named access-list to achieve this task

Configuration:

SERVER#4
interface Ethernet0/0
   ip igmp join-group 237.10.50.67
   ip igmp join-group 225.0.0.3

R16
   access-list 1 permit 237.10.50.67
   access-list 1 permit 225.0.0.3
   ip pim rp-candidate Loopback0 group-list 1

Verification:

SERVER4#sh ip igmp interface
 Ethernet0/0 is up, line protocol is up
   Internet address is 192.168.140.100/24
   IGMP is enabled on interface
   Current IGMP host version is 2
   Current IGMP router version is 2
   IGMP query interval is 60 seconds
   IGMP configured query interval is 60 seconds
   IGMP querier timeout is 120 seconds
   IGMP configured querier timeout is 120 seconds
   IGMP max query response time is 10 seconds
   Last member query count is 2
   Last member query response interval is 1000 ms
   Inbound IGMP access group is not set
   IGMP activity: 3 joins, 0 leaves
   Multicast routing is enabled on interface
   Multicast TTL threshold is 0
   Multicast designated router (DR) is 192.168.140.107
   IGMP querying router is 192.168.140.100 (this system)
   Multicast groups joined by this system (number of users): 224.0.1.40(1) 237.10.50.67(1) 225.0.0.3(1)

Note: Ok let’s now try and reach one of the multicast group first locally from R16 and then over the DMVPN

R16#ping 225.0.0.3 re 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 225.0.0.3, timeout is 2 seconds:
Reply to request 0 from 192.168.140.100, 53 ms
Reply to request 0 from 192.168.140.100, 77 ms
PC3#ping 237.10.50.67 re 2
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 237.10.50.67, timeout is 2 seconds:
Reply to request 0 from 192.168.140.100, 592 ms
Reply to request 0 from 192.168.140.100, 568 ms
Reply to request 1 from 192.168.140.100, 500 ms
Reply to request 1 from 192.168.140.100, 360 ms

SERVER3#ping 225.0.0.3 re 2
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 225.0.0.3, timeout is 2 seconds:
Reply to request 0 from 192.168.140.100, 636 ms
Reply to request 0 from 192.168.140.100, 672 ms
Reply to request 1 from 192.168.140.100, 312 ms
Reply to request 1 from 192.168.140.100, 536 ms
CCIEv5 R&S Multicast MSDP Topology

Service Provider #2
BGP
AS 29737

Service Provider #6
BGP AS 10001

Service Provider #7
BGP
AS 56775

Copyright © 2015 CCIE4ALL. All rights reserved
PIM Neighbor Control

A PIM router must receive PIM Hellos to establish PIM Neighborship. PIM Neighborship is also the basis for Designated Router (DR) election, and DR failover and accepting / sending PIM Join/Prune/Assert messages.

To inhibit unwanted neighbors use the `ip pim neighbor-filter` command illustrated in the above figure. This command filters from all non-allowed neighbors PIM packets, including Hellos, Join/Prune packets, and BSR packets. Note that hosts on the segment can spoof the source IP address to pretend to be the PIM neighbor. Layer 2 security mechanisms (namely IP source guard) are required to prevent source address spoofing on a segment or use a VLAN ACL in the access switch to prevent hosts from sending protocol 103 packets. The keyword “log-input” can be used in ACLs to log offending packets.

The PIM Join/Prune packet is sent to a PIM neighbor to add or remove that neighbor from a particular (S,G) or (*,G) forwarding path. PIM multicast packets are link local multicast packets sent with TTL=1. All of these packets are multicast to the well known All-PIM-Routers address: 224.0.0.13. This means that all such attacks must originate on the same subnet as the router being attacked. Attacks can include forged Hello, Join/Prune, and Assert packets. Note that forging the TTL value in PIM multicast packets to a higher value than 1 does not create problems, since the All-PIM-Routers address is always received and treated locally on a router. It is never directly forwarded by normal and legitimate routers. To protect the RP against a potential flood of PIM-SM register messages, the DR should rate limit those messages. The following command does this: `ip pim register-rate-limit <count>`

*directly from Cisco website*
PIM unicast packets can be used to attack the RP. Therefore, the RP should be protected by infrastructure ACLs against such attacks. Note again that senders and receivers never need to send PIM packets, so the PIM protocol (IP protocol 103) can usually be filtered at the subscriber edge.

The following additional security measures should be configured with Auto-RP where possible:

**Auto-RP Control - RP Announce Filter**

`ip pim rp-announce-filter`

This should be configured on the Mapping Agent to control which routers are accepted as Candidate RPs for which group ranges / group-mode.

Auto-RP Control - Constrain Auto-RP Messages

Use the multicast boundary command to constrain AutoRP packets to a particular PIM domain:

- `224.0.1.39` (RP-announce)
- `224.0.1.40` (RP-discover)

*directly from Cisco website*
BSR Control - Constrain BSR Messages
Use the `ip pim bsr-border` command to filter BSR messages at the border of a PIM domain. Note that no ACL is necessary since BSR messages are hop-by-hop forwarded with link local multicast.

RP / PIM-SM-related Filtering for Auto-RP, BSR and MSDP messages

Auto-RP Filtering
The following shows an example of Auto-RP working together with address scoping. Two different ways of bounding a region are shown. The two ACLs are equivalent from an Auto-RP perspective.

*directly from Cisco website*
The idea of the interface boundary filters for Auto-RP is to ensure that the auto-rp announcements only reach the regions they are supporting. Regional, Company and Internet-wide scopes are defined, and in each case there exist corresponding RPs and Auto-RP advertisements. We only want the Regional RPs to be known to the Regional routers, the Company RPs to be known to the Regional and Company routers, and we want any Internet RPs to be globally available. Further levels of scoping are possible.

There are two fundamentally different ways to filter Auto-RP packets:

- The Internet boundary explicitly calls out the auto-rp control groups (224.0.1.39 224.0.1.40) resulting in all Auto-RP packets being filtered. This method should be used at the edge of an administrative domain, where no Auto-RP packets should pass through.

- The Region boundary uses the filter-auto-rp keyword to instead create "semantic filtering" of Auto-RP messages. Instead of directly filtering Auto-RP packets, this command will cause an examination of the rp-to-group-range announcements within Auto-RP packets. When an announcement is explicitly denied by the ACL, it will be removed from the Auto-RP packet before the packet is forwarded. This will allow the enterprise-wide RPs to be known within the regions, while the region-wide RPs will be filtered at the boundary from the region to the rest of the enterprise.

Inter-Domain Filters and MSDP – see figure below
ISP1 is acting as a PIM-SM transit provider. They are only supporting MSDP peering with neighbors and they are only accepting (S,G), but no (*,G) traffic on the border routers.

In inter-domain (usually between Autonomous Systems) there are two basic security measures to be taken:

- Securing the data plane, using the multicast boundary command. This ensures that multicast traffic is only accepted for defined groups (and potentially sources).

- Securing the inter-domain control plane traffic (MSDP). This consists of a number of separate security measures: MSDP content control, state limitation, and neighbor authentication.

We show a typical configuration from one of ISP1’s border routers showing an example interface filter. To secure the data plane at the domain boundary we are inhibiting (*,G) joins by filtering "host 0.0.0.0" and administratively scoped addresses via the multicast boundary command:

Fig 13: Interdomain (*,G) filter

```
! directly from Cisco website
```

*directly from Cisco website*
Multicast MSDP Topology Preparation

Configure Loopback Interfaces on R92 R93 R94 R97 Service Provider routers as per the Multicast MSDP Diagram.

On R94 use a network statement to advertise both Loopback 710 IP Addresses into BGP.

At the end of this task all relevant routers should be able to reach each others Loopback 700 and 710 IP Addresses.

There should be no BGP configuration required on any routers except R94.

**Configuration:**

R92

```
interface Loopback710
  description Multicast RP Source
  ip address 160.200.100.92 255.255.255.255
```

R94

```
interface Loopback700
  description Multicast Source
  ip address 170.100.1.94 255.255.255.255

interface Loopback710
  description Multicast RP Source
  ip address 170.250.1.94 255.255.255.255

router bgp 56775
  address-family ipv4
    network 170.250.1.94 mask 255.255.255.255
  exit-address-family
```

R97

```
interface Loopback700
  description Multicast Receiver
  ip address 150.250.1.97 255.255.255.255

interface Loopback710
  description Multicast RP Source
  ip address 150.250.100.97 255.255.255.255
```

**Verification:**

R97#ping 170.250.1.94 so loo 710
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.250.1.94, timeout is 2 seconds:
Packet sent with a source address of 150.250.100.97

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/20/24 ms

R97#ping 170.100.1.94 so loo 700
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.100.1.94, timeout is 2 seconds:
Packet sent with a source address of 150.250.100.97

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/19/22 ms
Note: We will break this section into a few parts so that it is easier to understand. Ultimately the goal is to enable Finance department (Loopback700) of R97 to receive multicast stream for the group 226.1.2.3 from (Loopback700) R94

MSDP

Multicast SP#2

R97 Loopback710 must be elected as the rendezvous point in its domain and must also be used as the source of the mapping information broadcasts
Use a proprietary method to discover and announce the RP information
Block all auto RP messages from entering or leaving the domain
The network should never have to flood and prune multicast traffic unnecessarily

Configuration:

R97

ip multicast-routing

interface Loopback700
  ip pim sparse-mode
  ip igmp join-group 226.1.2.3

interface Loopback710
  ip pim sparse-mode

ip access-list standard BLOCK_MCAST
  deny 224.0.1.39
  deny 224.0.1.40
  permit 224.0.0.0 15.255.255.255

interface Serial2/0
  ip pim sparse-mode
  ip multicast boundary BLOCK_MCAST

ip pim send-rp-announce Loopback710 scope 100
ip pim send-rp-discovery Loopback710 scope 100
ip pim autorp listener

Verification:

R97#sh ip pim interface
Address       Interface                Ver/   Nbr    Query  DR     DR
Mode   Count  Intvl  Prior
150.250.1.97  Loopback700              v2/S 0      30     1      150.250.1.97
150.250.100.97 Loopback710              v2/S 0      30     1      150.250.100.97
86.191.16.5   Serial2/0                v2/S 0      30     1      0.0.0.0

R97#sh ip igmp groups
IGMP Connected Group Membership
Group Address Interface       Uptime       Expires       Last Reporter     Group Accounted
  226.1.2.3 Loopback700 00:19:00 00:02:11 150.250.1.97
  224.0.1.39 Serial2/0 00:16:15 stopped 86.191.16.5
  224.0.1.39 Loopback710 00:18:11 00:02:16 150.250.100.97
  224.0.1.39 Loopback700 00:18:11 00:02:10 150.250.1.97
  224.0.1.40 Loopback710 00:18:11 00:02:23 150.250.100.97
R97#sh ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent (Loopback710)

Group(s) 224.0.0.0/4
  RP 150.250.100.97 (?), v2v1
    Info source: 150.250.100.97 (?), elected via Auto-RP
    Uptime: 00:17:49, expires: 00:02:09

R97#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
     P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor Address    Interface    Uptime/Expires    Ver   DR
Note: No PIM neighbours as of yet so let’s move on to the next section SP#6
Multicast SP#6

R92 Loopback710 must be elected as the rendezvous point within the SP#6 domain
Use a static method to discover and announce the RP information
Block all auto RP messages from entering or leaving the domain
The network should never have to flood and prune multicast traffic unnecessarily

**Configuration:**

**R92**

ip multicast-routing

interface Loopback710
ip pim sparse-mode

interface Serial3/0
ip pim sparse-mode
ip multicast boundary BLOCK_MCAST

interface Serial4/0
ip pim sparse-mode

ip access-list standard BLOCK_MCAST
deny 224.0.1.39
deny 224.0.1.40
permit 224.0.0.0 15.255.255.255

ip pim rp-address 160.200.100.92

**R93**

ip multicast-routing

interface Serial5/0
ip pim sparse-mode

interface Ethernet4/0
ip pim sparse-mode
ip multicast boundary BLOCK_MCAST

ip access-list standard BLOCK_MCAST
deny 224.0.1.39
deny 224.0.1.40
permit 224.0.0.0 15.255.255.255

ip pim rp-address 160.200.100.92

**Verification:**

```
R92#sh ip pim interface
Address          Interface                Ver/ Nbr Query DR    DR
Mode  Count  Intvl Prior
86.191.16.10     Serial4/0                v2/S 1   30   1  0.0.0.0
160.200.100.92   Loopback710              v2/S 0   30   1 160.200.100.92
86.191.16.6      Serial3/0                v2/S 1   30   1  0.0.0.0
```
R92#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address           Prio/Mode
86.191.16.9       Serial4/0                01:40:50/00:01:18 v2    1 / S P G
86.191.16.5       Serial3/0                00:06:17/00:01:22 v2    1 / S P G

R92#sh ip pim rp mapping
PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4, Static

RP: 160.200.100.92 (?)

R93#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address
86.191.16.10      Serial5/0                01:44:43/00:01:22 v2    1 / S P G

R93#sh access-list
Standard IP access list BLOCK_MCAST
10 deny 224.0.1.39 (19 matches)
20 deny 224.0.1.40 (15 matches)
30 permit 224.0.0.0, wildcard bits 15.255.255.255
Multicast SP#7

R94 Loopback710 must be elected as the rendezvous point within the SP#7 domain
Use a non proprietary method to discover and announce the RP information
Block all auto RP messages from entering or leaving the domain
The network should never have to flood and prune multicast traffic unnecessarily

**Configuration:**

```
R94
ip multicast-routing

interface Loopback710
ip pim sparse-mode

interface Loopback700
ip pim sparse-mode

interface Ethernet0/0
ip pim bsr-border
ip pim sparse-mode

ip pim bsr-candidate Loopback710 0
ip pim rp-candidate Loopback710
```

**Verification:**

```
R94#sh ip pim interface
Address  Interface    Ver/ Nbr    Query  DR     DR
         Mode   Count  Intvl Prior
170.250.1.94  Loopback710  v2/S   0      30     1      170.250.1.94
170.100.1.94  Loopback700  v2/S   0      30     1      170.100.1.94
66.171.14.9    Ethernet0/0  v2/S * 1      30     1      66.171.14.10

R94#sh ip pim rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)
Group(s) 224.0.0.0/4
    RP 170.250.1.94 (?), v2
    Info source: 170.250.1.94 (?), via bootstrap, priority 0, holdtime 150
    Uptime: 00:02:54, expires: 00:01:34

R94#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor  Interface  Uptime/Expires  Ver  DR  Prio/Mode
66.171.14.10  Ethernet0/0  00:04:07/00:01:32 v2 1 / DR S P G
```
Multiservice BGP Extension

Enable Multicast BGP between each Service Provider – refer to Multicast MSDP Diagram
Enable Finance department (Loopback700) of R97 to receive multicast stream for the group 226.1.2.3
from the Multicast Server (Loopback700) R94

Note: The ‘connect-source’ is the local peering address. This is analogous to BGP with the neighbor address and
update-source configuration settings.
The ‘remote-as’ value in MSDP peerings is optional, because MSDP can automatically derive that value based on the
BGP peering information

Configuration:

R94
router bgp 6775
  address-family ipv4 multicast
  neighbor 66.171.14.10 activate
  exit-address-family
ip msdp peer 160.200.100.92 connect-source Loopback710
ip msdp cache-sa-state

R93
router bgp 10001
  address-family ipv4 multicast
  neighbor 66.171.14.9 activate
  neighbor 86.191.16.10 activate
  exit-address-family
ip msdp peer 150.250.100.97 connect-source Loopback710
ip msdp peer 170.250.1.94 connect-source Loopback710
ip msdp cache-sa-state

R92
router bgp 10001
  address-family ipv4 multicast
  neighbor 86.191.16.5 activate
  neighbor 86.191.16.9 activate
  exit-address-family
ip msdp peer 150.250.100.97 connect-source Loopback710
ip msdp peer 170.250.1.94 connect-source Loopback710
ip msdp cache-sa-state

R97
router bgp 29737
  address-family ipv4 multicast
  neighbor 86.191.16.6 activate
  exit-address-family
ip msdp peer 160.200.100.92 connect-source Loopback710
ip msdp cache-sa-state
Verification:

R92#sh bgp ipv4 multicast summary
BGP router identifier 110.1.16.150, local AS number 10001
BGP table version is 1, main routing table version 1

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>86.191.16.5</td>
<td>4</td>
<td>29737</td>
<td>21</td>
<td>36</td>
<td>1</td>
<td>0</td>
<td>00:03:03</td>
<td>0</td>
</tr>
<tr>
<td>86.191.16.9</td>
<td>4</td>
<td>10001</td>
<td>155</td>
<td>108</td>
<td>1</td>
<td>0</td>
<td>00:03:36</td>
<td>0</td>
</tr>
</tbody>
</table>

R93#sh bgp ipv4 multicast summary
BGP router identifier 124.19.254.150, local AS number 10001
BGP table version is 1, main routing table version 1

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>66.171.14.9</td>
<td>4</td>
<td>56775</td>
<td>18</td>
<td>97</td>
<td>1</td>
<td>0</td>
<td>00:04:34</td>
<td>0</td>
</tr>
<tr>
<td>86.191.16.10</td>
<td>4</td>
<td>10001</td>
<td>108</td>
<td>155</td>
<td>1</td>
<td>0</td>
<td>00:03:52</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: We will enable different debugs on R94 and R97 to see MSDP peer establishment in action:

R94#debug ip msdp peer
MSDP Peer debugging is on
*Dec 27 13:37:12.808: %MSDP-5-PEER_UPDOWN: Session to peer 160.200.100.92 going up
MSDP(0): 160.200.100.92: TCP connection established
MSDP(0): 160.200.100.92: Sending Keepalive message to peer
MSDP(0): 160.200.100.92: Received 3-byte msg 45 from peer
MSDP(0): 160.200.100.92: Keepalive TLV
MSDP(0): 160.200.100.92: Originating SA message
MSDP(0): 160.200.100.92: Building SA message from SA cache
MSDP(0): 160.200.100.92: Originating SA message
MSDP(0): 160.200.100.92: Building SA message from SA cache
MSDP(0): 160.200.100.92: Sending Keepalive message to peer
MSDP(0): 160.200.100.92: Received 3-byte msg 46 from peer
MSDP(0): 160.200.100.92: Keepalive TLV
R94#un all
All possible debugging has been turned off

R97
access-list 101 per tcp host 160.200.100.92 any
R97#debug ip packet detail 101
IP packet debugging is on (detailed) for access list 101
IP packet details:
TCP src=639, dst=30136, seq=2575351520, ack=554960037, win=16384 ACK SYN, MCI Check(99), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
IP: s=160.200.100.92 (Serial2/0), d=150.250.100.97, len 44, input feature
TCP src=639, dst=30136, seq=2575351520, ack=554960037, win=16384 ACK SYN
IP: s=160.200.100.92 (Serial2/0), d=150.250.100.97, len 44, rcvd 4
TCP src=639, dst=30136, seq=2575351520, ack=554960037, win=16384 ACK SYN
Dec 27 13:46:21.720: %MSDP-5-PEER_UPDOWN: Session to peer 160.200.100.92 going up
IP: s=160.200.100.92 (Serial2/0), d=150.250.100.97, len 40, input feature
TCP src=639, dst=30136, seq=2575351520, ack=554960037, win=16384 ACK SYN
Dec 27 13:46:21.720: %MSDP-5-PEER_UPDOWN: Session to peer 160.200.100.92 going up
IP: s=160.200.100.92 (Serial2/0), d=150.250.100.97, len 40, input feature
TCP src=639, dst=30136, seq=2575351520, ack=554960037, win=16384 ACK SYN
R97#un all
All possible debugging has been turned off

Note: MSDP uses TCP/639
R97#sh ip msdp peer 160.200.100.92 accepted-SAs
MSDP SA accepted from peer 160.200.100.92 (?)
226.1.2.3 170.100.1.94 (?) RP: 170.250.1.94

R92#sh ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/ Reset SA    Peer Name
                  Downtime Count Count
150.250.100.97   29737 Up       00:26:00 0     0     ?
170.250.1.94     56775 Up       00:26:05 0     0     ?

R94#sh ip msdp peer
MSDP Peer 160.200.100.92 (?), AS 10001
Connection status:
  State: Up, Resets: 0, Connection source: Loopback710 (170.250.1.94)
  Uptime(Downtime): 00:26:42, Messages sent/received: 30/26
  Output messages discarded: 0
  Connection and counters cleared 00:28:06 ago
SA Filtering:
  Input (S,G) filter: none, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
  Number of connection transitions to Established state: 1
  Input queue size: 0, Output queue size: 0
MD5 signature protection on MSDP TCP connection: not enabled
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 0/17
  SA Requests in: 0
  SA Responses out: 0
  Data Packets in/out: 0/1

Note: Let’s validate the unicast and rpf route on all RP’s and make sure they are in agreement

R97#sh ip route 160.200.100.92
Routing entry for 160.200.100.92/32
  Known via “bgp 29737”, distance 20, metric 0
  Tag 10001, type external
  Last update from 86.191.16.6 00:41:36 ago
Routing Descriptor Blocks:
  * 86.191.16.6, from 86.191.16.6, 00:41:36 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 10001
    MPLS label: none

R97#sh ip rpf 160.200.100.92
RPF information for ? (160.200.100.92)
  RPF interface: Serial2/0
  RPF neighbor: ? (86.191.16.6)
  RPF route/mask: 160.200.100.92/32
  RPF type: unicast (bgp 29737)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base, originated from ipv4 unicast base
R94#sh ip route 160.200.100.92
Routing entry for 160.200.100.92/32
    Known via "bgp 56775", distance 20, metric 0
    Tag 10001, type external
    Last update from 66.171.14.10 00:44:33 ago
Routing Descriptor Blocks:
    * 66.171.14.10, from 66.171.14.10, 00:44:33 ago
        Route metric is 0, traffic share count is 1
        AS Hops 1
        Route tag 10001
        MPLS label: none

R94#sh ip rpf 160.200.100.92
RPF information for ? (160.200.100.92)
    RPF interface: Ethernet0/0
    RPF neighbor: ? (66.171.14.10)
    RPF route/mask: 160.200.100.92/32
    RPF type: unicast (bgp 56775)
    Doing distance-preferred lookups across tables
    RPF topology: ipv4 multicast base, originated from ipv4 unicast base

R92#sh ip route 150.250.100.97
Routing entry for 150.250.100.97/32
    Known via "bgp 10001", distance 20, metric 0
    Tag 29737, type external
    Last update from 86.191.16.5 00:43:33 ago
Routing Descriptor Blocks:
    * 86.191.16.5, from 86.191.16.5, 00:43:33 ago
        Route metric is 0, traffic share count is 1
        AS Hops 1
        Route tag 29737
        MPLS label: none

R92#sh ip rpf 150.250.100.97
RPF information for ? (150.250.100.97)
    RPF interface: Serial3/0
    RPF neighbor: ? (86.191.16.5)
    RPF route/mask: 150.250.100.97/32
    RPF type: unicast (bgp 10001)
    Doing distance-preferred lookups across tables
    RPF topology: ipv4 multicast base, originated from ipv4 unicast base

R92#sh ip route 170.250.1.94
Routing entry for 170.250.1.94/32
    Known via "bgp 10001", distance 20, metric 0
    Tag 56775, type internal
    Last update from 86.191.16.9 00:44:13 ago
Routing Descriptor Blocks:
    * 86.191.16.9, from 86.191.16.9, 00:44:13 ago
        Route metric is 0, traffic share count is 1
        AS Hops 1
        Route tag 56775
        MPLS label: none

R92#sh ip rpf 170.250.1.94
RPF information for ? (170.250.1.94)
    RPF interface: Serial4/0
    RPF neighbor: ? (86.191.16.9)
    RPF route/mask: 170.250.1.94/32
    RPF type: unicast (bgp 10001)
    Doing distance-preferred lookups across tables
    RPF topology: ipv4 multicast base, originated from ipv4 unicast base
**Note:** All seems fine so now we'll send a ping to 226.1.2.3 and check MSDP cache on R92

R94#ping 226.1.2.3 source loopback 700 re 2
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 226.1.2.3, timeout is 2 seconds:
Packet sent with a source address of 170.100.1.94

Reply to request 0 from 150.250.1.97, 20 ms
Reply to request 0 from 150.250.1.97, 20 ms
Reply to request 1 from 150.250.1.97, 18 ms
Reply to request 1 from 150.250.1.97, 23 ms
R94#

R92#sh ip msdp sa-cache
MSDP Source-Active Cache - 1 entries

(170.100.1.94, 226.1.2.3), RP 170.250.1.94, BGP/AS 56775, 00:01:06/00:05:23, **Peer 170.250.1.94**

R97#sh ip mroute 226.1.2.3
IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - UDR, I - Received Source Specific Host Report,
Z - Multicast Tunnel, z - MDT-data group sender,
Y - Joined MDT-data group, y - Sending to MDT-data group,
G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
Q - Received BGP S-A Route, q - Sent BGP S-A Route,
V - RD & Vector, v - Vector, p - PIM Joins on route

Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 226.1.2.3), 01:55:31/stopped, RP 150.250.100.97, flags: SJCL
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Loopback700, Forward/Sparse, 01:55:31/00:02:36

(170.100.1.94, 226.1.2.3), 00:01:07/00:01:51, flags: LMT
Incoming interface: Serial2/0, RPF nbr 86.191.16.6
Outgoing interface list:
Loopback700, Forward/Sparse, 00:01:07/00:02:36

R92#sh ip mroute 226.1.2.3 | be Outgoing
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 226.1.2.3), 00:04:53/stopped, RP 160.200.100.92, flags: SP
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list: Null

(170.100.1.94, 226.1.2.3), 00:01:45/00:01:14, flags: T
Incoming interface: Serial14/0, RPF nbr 86.191.16.9
Outgoing interface list:
Serial3/0, Forward/Sparse, 00:01:45/00:02:43
R94#sh ip mroute 226.1.2.3 | be Outgoing
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 226.1.2.3), 00:05:04/stopped, RP 170.250.1.94, flags: SP
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list: Null
(170.100.1.94, 226.1.2.3), 00:05:04/00:02:51, flags: TA
Incoming interface: Loopback700, RPF nbr 0.0.0.0
Outgoing interface list:
  Ethernet0/0, Forward/Sparse, 00:05:04/00:02:31

Note: Let’s now traceroute and request information on R94 using the ‘mstat’ ‘mtrace’ and ‘mrinfo’ commands:

R94>mstat 170.100.1.94 150.250.1.97 226.1.2.3
Type escape sequence to abort.
Mtrace from 170.100.1.94 to 150.250.1.97 via group 226.1.2.3
From source (?) to destination (?)
Waiting to accumulate statistics.....**
Results after 13 seconds:
Source Response Dest Packet Statistics For Only For Traffic
170.100.1.94 170.100.1.94 All Multicast Traffic From 170.100.1.94
| / rtt 29 ms Lost/Sent = Pct Rate To 226.1.2.3
v / hop 11 ms ------------------------ --------------
170.100.1.94
66.171.14.9 ? Reached RP/Core
| ^ ttl 0
v | hop -12 ms -1/0 = --% 0 pps 0/0 = --% 0 pps
66.171.14.10
86.191.16.9 ? Reached RP/Core
| ^ ttl 1
v | hop 5 ms 0/0 = --% 0 pps 0/0 = --% 0 pps
86.191.16.10
86.191.16.6 ? Reached RP/Core
| ^ ttl 2
v | hop 5 ms 0/0 = --% 0 pps 0/0 = --% 0 pps
Route changed, start again.

R94>mtrace 170.100.1.94 150.250.1.97 226.1.2.3
Type escape sequence to abort.
Mtrace from 170.100.1.94 to 150.250.1.97 via group 226.1.2.3
From source (?) to destination (?)
Querying full reverse path...
  0 150.250.1.97
-1 0.0.0.0 == 86.191.16.5 PIM/MBGP Reached RP/Core [170.100.1.94/32]
-2 86.191.16.6 --> 86.191.16.10 PIM/MBGP Reached RP/Core [170.100.1.94/32]
-3 86.191.16.9 --> 86.171.14.10 PIM/MBGP [170.100.1.94/32]
-4 86.171.14.9 == 170.100.1.94 PIM_MT Reached RP/Core [170.100.1.94/32]

R94#mrinfo 150.250.100.97 loopback 710
150.250.100.97 [version 15.4] [flags: PMA]:
  150.250.1.97 -> 0.0.0.0 [1/0/pim querier/leaf]
  150.250.100.97 -> 0.0.0.0 [1/0/pim querier/leaf]
  86.191.16.5 -> 86.191.16.6 [1/0/pim]
MSDP Password Protection/Timers

Secure all MSDP peering using MD5 authentication with a password of CISCO-MSDP. MSDP peers should wait 15 seconds after peering sessions are reset before attempting to reestablish the sessions.

**Configuration:**

```
R94
ip msdp password peer 160.200.100.92 CISCO-MSDP
ip msdp timer 45

R92
ip msdp password peer 150.250.100.97 CISCO-MSDP
ip msdp password peer 170.250.1.94 CISCO-MSDP
ip msdp timer 45

R97
ip msdp password peer 160.200.100.92 CISCO-MSDP
ip msdp timer 45
```

**Verification:**

```
R94#sh ip msdp peer
MSDP Peer 160.200.100.92 (?), AS 10001
Connection status:
  State: Up, Resets: 3, Connection source: Loopback710 (170.250.1.94)
  Uptime(Downtime): 00:28:22, Messages sent/received: 32/43
  Output messages discarded: 0
  Connection and counters cleared 01:25:03 ago
SA Filtering:
  Input (S,G) filter: none, route-map: none
  Input RP filter: none, route-map: none
  Output (S,G) filter: none, route-map: none
  Output RP filter: none, route-map: none
SA-Requests:
  Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
  Number of connection transitions to Established state: 4
  Input queue size: 0, Output queue size: 0
  **MD5 signature protection on MSDP TCP connection: enabled**
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 22/8
  SA Requests in: 0
  SA Responses out: 0
  Data Packets in/out: 7/2
```
The network manager of your network cannot justify a full security implementation but wants to implement a solution that provides only a password prompt from R1 when the keyboard entry 1 is entered on the console port (as opposed to the normal CR/Enter key) – Configure R1 appropriately.

### Router(config-line) Configuration

- **escape-character**
  - Changes the system escape character. We recommend the use of the ASCII characters represented by the decimal numbers 1 through 30. The escape character can be a single character (such as `)`), a key combination (such as Ctrl-X), or a sequence of keys (such as Ctrl-^, X). The default escape character (key combination) is Ctrl-Shift-6 (Ctrl-^), or Ctrl-Shift-6, X (Ctrl-^, X).

- **activation-character**
  - Defines a session activation character. Entering this character at a vacant terminal begins a terminal session. The default activation character is the Return key.

- **disconnect-character**
  - Defines the session disconnect character. Entering this character at a terminal ends the session with the router. There is no default disconnect character.

- **hold-character**
  - Defines the hold character that causes output to the screen to pause. After this character has been set, a user can enter the character at any time to pause output to the terminal screen. To resume output, the user can press any key. To use the hold character in normal communications, precede it with the escape character. There is no default hold character.

### Configuration:

```
R1
line console 0
activation-character 49
```

### Verification:  *Enter* key should NOT allow to get into R1’s console

```
R1 con0 is now available/
Press RETURN to get started.

R1#sh line console 0

Tty Typ    Tx/Rx  A Modem  Roty AccO AccI Uses Noise Overruns  Int
*  0 CTY    -    -    -    - 0 0 0/0 -

Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
Status: FSI Enabled, Ready, Active, Automore On
Capabilities: none
Modem state: Ready
Group codes: 0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
  ^x  none  -  -  none
Timeouts: Idle EXEC  Idle Session  Modem Answer  Session  Dispatch
  00:10:00  never  none  not set
```

<Output omitted>
Verification: Hit 1 key to enter R1's console

R1 con0 is now available
Press RETURN to get started.

R1#sh line console 0

<table>
<thead>
<tr>
<th>Tty Typ</th>
<th>Tx/Rx</th>
<th>A Modem</th>
<th>Roty</th>
<th>AccO</th>
<th>AccI</th>
<th>Uses</th>
<th>Noise</th>
<th>Overruns</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>0 CTY</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
</tbody>
</table>

Line 0, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600, no parity, 2 stopbits, 8 databits
Status: PSI Enabled, Ready, Active, Automore On
Capabilities: none
Modem state: Ready
Group codes: 0
Special Chars: Escape Hold Stop Start Disconnect Activation
\[\text{^x} \quad \text{none} \quad - \quad - \quad \text{none} \quad 1\]
Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch
00:10:00 never none never not set
Idle Session Disconnect Warning never

<Output omitted>

Note: This is a tricky question because the CLI entry requires an ASCII entry. You would need to search to discover that ASCII numeric figures (0 to 9) are prefixed by the binary value of 0011, so a value of 1 (0001) would be 00110001. Therefore, the decimal conversion is 32 + 16 + 1 = 49. This is a good question on which to use the (?) on the CLI for clues and your documentation CD or search facility in the lab if you were not aware of this feature. For the remaining Lab questions remember to press '1' and NOT Enter to activate R1's console.
Service Provider #6

System Protection

R92 acts as one of the “Internet Looking Glass” router
The network administrator has decided to give limited access to the LSR Router for basic troubleshooting and verification

Inexperienced user Network Admin in Service Provider#1 R96 Loopback307 will be logging into R92
Global Terminal Station 86.13.117.119 IP Address via telnet with the username MPLS_USER and password of MPLSPASSWORD

The following menu should appear when he/she successfully connects:

Menu for MPLS_USER PE Router
1. View VPN VRF Berlin-HQRO Routing Table
2. View VPN VRF Berlin-HQRO BGP Table
3. View VPN VRF Berlin-HQRO MPLS Forwarding Table
4. View VPN VRF Berlin-HQRO BGP MPLS Label Forwarding Table
5. Exit
Choose your selection:

Option 1 should display the IP routing table for VRF Berlin-HQRO
Option 2 should display the BGP table for VRF Berlin-HQRO
Option 3 should display the MPLS forwarding table for VRF Berlin-HQRO
Option 4 should display the BGP learned labels for VRF Berlin-HQRO
Option 5 should exit the users out

Configuration:

R92

    menu MPLS_USER title ^ Menu for Menu for MPLS_USER PE Router ^C
    menu MPLS_USER prompt ^ Choose your selection: ^C

    menu MPLS_USER text 1. View VPN VRF Berlin-HQRO Routing Table
    menu MPLS_USER text 2. View VPN VRF Berlin-HQRO BGP Table
    menu MPLS_USER text 3. View VPN VRF Berlin-HQRO MPLS Forwarding Table
    menu MPLS_USER text 4. View VPN VRF Berlin-HQRO BGP MPLS Label Forwarding Table
    menu MPLS_USER text 5. Exit

    menu MPLS_USER command 1. show ip route vrf Berlin-HQRO
    menu MPLS_USER command 2. show ip bgp vpnv4 vrf Berlin-HQRO
    menu MPLS_USER command 3. show mpls forwarding-table vrf Berlin-HQRO
    menu MPLS_USER command 4. show ip bgp vpnv4 vrf Berlin-HQRO labels
    menu MPLS_USER command 5. exit

    menu MPLS_USER options 1. pause
    menu MPLS_USER options 2. pause
    menu MPLS_USER options 3. pause
    menu MPLS_USER options 4. pause

    menu MPLS_USER clear-screen

username MPLS_USER privilege 15 password MPLSPASSWORD
username MPLS_USER autocommand menu MPLS_USER
line vty 0 4
login local
transport input telnet

Verification:

R96#telnet 86.13.117.119 /source-interface lo307
Trying 86.13.117.119 ... Open

User Access Verification
Username: MPLS_USER
Password:
Menu for Menu for MPLS_USER PE Router
1. View VPN VRF Berlin-HQRO Routing Table
2. View VPN VRF Berlin-HQRO BGP Table
3. View VPN VRF Berlin-HQRO MPLS Forwarding Table
4. View VPN VRF Berlin-HQRO BGP MPLS Label Forwarding Table
5. Exit
Choose your selection:
Choose your selection:

[Connection to 86.13.117.119 closed by foreign host]
R96#
## DSCP, ToS and IP Precedence Mappings

<table>
<thead>
<tr>
<th>DSCP Decimal</th>
<th>DSCP Binary</th>
<th>Codepoint Name</th>
<th>IP Precedence</th>
<th>ToS Value</th>
<th>Service Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000 000</td>
<td>CS0</td>
<td>0</td>
<td>0</td>
<td>Standard</td>
</tr>
<tr>
<td>2</td>
<td>000 010</td>
<td></td>
<td>0</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>000 100</td>
<td></td>
<td>0</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>000 110</td>
<td></td>
<td>0</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>001 000</td>
<td>CS1</td>
<td>1</td>
<td>32</td>
<td>Low-Priority Data</td>
</tr>
<tr>
<td>10</td>
<td>001 010</td>
<td>AF11</td>
<td>1</td>
<td>40</td>
<td>High-Throughput Data</td>
</tr>
<tr>
<td>12</td>
<td>001 100</td>
<td>AF12</td>
<td>1</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>001 110</td>
<td>AF13</td>
<td>1</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>010 000</td>
<td>CS2</td>
<td>2</td>
<td>64</td>
<td>OAM</td>
</tr>
<tr>
<td>18</td>
<td>010 010</td>
<td>AF21</td>
<td>2</td>
<td>72</td>
<td>Low Latency Data</td>
</tr>
<tr>
<td>20</td>
<td>010 100</td>
<td>AF22</td>
<td>2</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>010 110</td>
<td>AF23</td>
<td>2</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>011 000</td>
<td>CS3</td>
<td>3</td>
<td>96</td>
<td>Broadcast Video</td>
</tr>
<tr>
<td>26</td>
<td>011 010</td>
<td>AF31</td>
<td>3</td>
<td>104</td>
<td>Multimedia Streaming</td>
</tr>
<tr>
<td>28</td>
<td>011 100</td>
<td>AF32</td>
<td>3</td>
<td>112</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>011 110</td>
<td>AF33</td>
<td>3</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>100 000</td>
<td>CS4</td>
<td>4</td>
<td>128</td>
<td>Realtime Interactive</td>
</tr>
<tr>
<td>34</td>
<td>100 010</td>
<td>AF41</td>
<td>4</td>
<td>136</td>
<td>Multimedia Conferencing</td>
</tr>
<tr>
<td>36</td>
<td>100 100</td>
<td>AF42</td>
<td>4</td>
<td>144</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>100 110</td>
<td>AF43</td>
<td>4</td>
<td>152</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>101 000</td>
<td>CS5</td>
<td>5</td>
<td>160</td>
<td>Signalling</td>
</tr>
<tr>
<td>42</td>
<td>101 010</td>
<td></td>
<td>5</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>101 100</td>
<td></td>
<td>5</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>101 110</td>
<td>EF</td>
<td>5</td>
<td>184</td>
<td>Telephony</td>
</tr>
<tr>
<td>48</td>
<td>110 000</td>
<td>CS6</td>
<td>6</td>
<td>192</td>
<td>Network Control</td>
</tr>
<tr>
<td>50</td>
<td>110 010</td>
<td></td>
<td>6</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>110 100</td>
<td></td>
<td>6</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>110 110</td>
<td></td>
<td>6</td>
<td>216</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>111 000</td>
<td>CS7</td>
<td>7</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>111 010</td>
<td></td>
<td>7</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>111 100</td>
<td></td>
<td>7</td>
<td>240</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>111 110</td>
<td></td>
<td>7</td>
<td>248</td>
<td></td>
</tr>
</tbody>
</table>

### Class Selector
- Assured Forwarding: [RFC 2474](https://tools.ietf.org/rfc/rfc2474.txt)
- Expedited Forwarding: [RFC 3246](https://tools.ietf.org/rfc/rfc3246.txt)
- Diffserv Service Classes: [RFC 4594](https://tools.ietf.org/rfc/rfc4594.txt)
Sydney Business Model HQ

TELNET

R17 interface Ethernet1/0 should ‘always’ be used as a source of all telnet packets
Telnet packet should be marked with IP Precedence 3
R16 should act as a DNS server
Ensure that when ‘SERVER4’ is typed on R17 in exec mode, the connection is made without seeing the IP address of SERVER4 or any other informational messages
Ensure that the password used to gain access is “DATA”
Do not explicitly configure username and password anywhere

**Configuration:**

**R16**
- ip dns server
- ip domain-lookup

- ip host SERVER4 192.168.140.100

**R17**
- ip name-server 192.168.140.16
- ip domain-lookup
- ip telnet source-interface ethernet1/0
- ip telnet tos 60
- ip telnet hidden addresses
- ip telnet quiet

**SERVER#4**
- line vty 0 4
- privilege level 15
- password DATA
- login
- transport input telnet

**Verification:**

Below is without any special telnet configuration

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]
Trying SERVER4 (192.168.140.100)... Open

User Access Verification

Password:
SERVER4#exi
[Connection to SERVER4 closed by foreign host]
R17#
Below is after ‘ip telnet quiet’ has been applied on R17

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]

User Access Verification
Password:
SERVER4#exit
R17#

Below is after ‘ip telnet hidden addresses’ has been applied on R17

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]
Trying SERVER4 address #1 ... Open

User Access Verification
Password:
SERVER4#exit
[Connection closed by foreign host]
R17#

Below is after ‘ip telnet hidden hostnames’ has been applied on R17

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]
Trying (192.168.140.100)... Open

User Access Verification
Password:
SERVER4#exit

[Connection closed by foreign host]
R17#

Below is as per the question requirements: ‘ip telnet hidden addresses’ and ‘ip telnet quiet’ has been applied on R17

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]

User Access Verification
Password:
SERVER4#exit
R17#
Note: To verify the TOS byte settings are correct telnet to SERVER#4 from R17, then telnet back and verify the TCP connection properties. Note that the TOS value is entered in HEX format in the configuration.

Ok so now we need to configure telnet access on R17 so that we can test.

```
R17
line vty 0 4
  privilege level 15
  password DATA
  login
  transport input telnet
```

```
R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]
User Access Verification
Password:
SERVER4#
```

```
SERVER4#telnet 192.17.17.17
Trying 192.17.17.17 ... Open
User Access Verification
Password:
R17#
```

```
R17#sh tcp brief all
TCB Local Address Foreign Address (state)
A57A9278 192.17.17.17.23 SERVER4.44546 ESTAB
A4A63758 155.84.74.30.179 155.84.29.22720 ESTAB
A3B60F68 192.168.100.17.48342 SERVER4.23 ESTAB
A47CC580 0.0.0.0.179 155.84.74.29.* LISTEN
```

```
R17#sh tcp tcb A57A9278
Connection state is ESTAB, I/O status: 1, unread input bytes: 1
Connection is ECN Disabled, Minimum incoming TTL 0, Outgoing TTL 255
Local host: 192.17.17.17, Local port: 23
Foreign host: 192.168.140.100, Foreign port: 44546
Connection tableid (VRF): 0
Maximum output segment queue size: 20
SRTT: 999 ms, RTTO: 1009 ms, RTV: 10 ms, KRTT: 0 ms
minRTT: 1 ms, maxRTT: 1000 ms, ACK hold: 200 ms
Status Flags: passive open, active open
Option Flags: Retrans timeout
IP Precedence value : 3
```

Datagrams (max data segment is 536 bytes):
Rcvd: 86 (out of order: 0), with data: 51, total data bytes: 95
Sent: 68 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 62, total data bytes: 1649
Packets received in fast path: 0, fast processed: 0, slow path: 0
fast lock acquisition failures: 0, slow lock: 0
TCP Semaphore 0xA4E6F07C FREE
TELNET

Make sure telnet to SERVER#4 is only allowed during normal business hours from Monday to Friday (8:00 AM to 20:00 PM) This functionality should be applied to VTYs 0–4 also every connection should be logged to the console Reduce the amount of time when trying to establish telnet sessions to minimum SERVER4 should automatically log the telnet user out of the session after 60 seconds window

Configuration:

SERVER#4
ip tcp synwait-time 5

Verification:

Note: Let's check the time of Server#4 and first configure an ACL that DOES NOT match the current time

SERVER4#sh clock
*12:07:52.957 CET Fri Dec 26 2014

SERVER#4
time-range TELNET
periodic weekdays 14:00 to 20:00
ip access-list extended VTY_ACCESS
permit tcp any any eq telnet time-range TELNET log
line vty 0 4
access-class VTY_ACCESS in

Note: Seems like we are not able to telnet to Server#4 anymore

R17#SERVER4
(192.16.16.16)
Translating "SERVER4"...domain server (192.16.16.16) [OK]
R17#

SERVER4#sh access-list VTY_ACCESS
Extended IP access list VTY_ACCESS
10 permit tcp any any eq telnet time-range TELNET [inactive] log
**Note:** We will change the time in our ACL

```plaintext
SERVER#4
    time-range TELNET
    no periodic weekdays 14:00 to 20:00
    periodic weekdays 09:00 to 20:00
```

R17#SERVER4
Translating "SERVER4"...domain server (192.16.16.16) [OK]
User Access Verification
Password:
SERVER4#exit
R17#

SERVER4#
*Dec 26 11:14:58.555: %SEC-6-IPACCESSLOGP: list VTY_ACCESS permitted tcp 192.168.100.17(56130) -> 0.0.0.0(23), 1 packet
```
Service Provider #9

Control Plane

On R7 Log all dropped and permitted packets that hit the control-plane host feature path only, regardless of the interface from which the packets enter the router.

Ensure that the router rate-limits the log messages to one every 20 seconds

Configuration:

```plaintext
R7
class-map type logging match-any CPLOG-CLASS
   match packets dropped
   match packets permitted

policy-map type logging CPLOG-POLICY
   class CPLOG-CLASS
   log interval 20000

control-plane host
   service-policy type logging input CPLOG-POLICY
```

Verification:

```plaintext
R7#
  *Dec 26 10:27:20.952: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:27:51.184: %CP-6-TCP: PERMIT 172.100.5.5(646) -> 172.100.7.7(15666)
  *Dec 26 10:28:13.824: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:28:39.407: %CP-6-TCP: PERMIT 172.100.5.5(646) -> 172.100.7.7(15666)
  *Dec 26 10:28:59.558: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:29:19.771: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:29:46.203: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:30:13.579: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:30:38.988: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:30:58.845: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:31:08.984: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:31:30.451: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:31:53.314: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:32:00.456: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:32:51.637: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:33:25.528: %CP-6-TCP: PERMIT 172.100.1.1(57552) -> 172.100.7.7(179)
  *Dec 26 10:33:48.528: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
  *Dec 26 10:34:17.988: %CP-6-TCP: PERMIT 172.100.6.6(646) -> 172.100.7.7(11950)
```

R7#sh control-plane host counters
Control plane host path counters:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Packets Processed/Dropped/Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control-plane Logging</td>
<td>1333/0/0</td>
</tr>
</tbody>
</table>
**Note: NTP**

NTP is designed to synchronize the time on a network of machines. NTP runs over the User Datagram Protocol (UDP), using port 123 as both the source and destination, which in turn runs over IP. NTP Version 3 RFC 1305 leavingcisco.com is used to synchronize timekeeping among a set of distributed time servers and clients. A set of nodes on a network are identified and configured with NTP and the nodes form a synchronization subnet, sometimes referred to as an overlay network. While multiple masters (primary servers) may exist, there is no requirement for an election protocol.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. An NTP client makes a transaction with its server over its polling interval (from 64 to 1024 seconds) which dynamically changes over time depending on the network conditions between the NTP server and the client. The other situation occurs when the router communicates to a bad NTP server (for example, NTP server with large dispersion); the router also increases the poll interval. No more than one NTP transaction per minute is needed to synchronize two machines. It is not possible to adjust the NTP poll interval on a router.

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock directly attached to it. It then sends its time to a stratum 2 time server through NTP, and so on. A machine running NTP automatically chooses the machine with the lowest stratum number that it is configured to communicate with using NTP as its time source.

NTP avoids synchronizing to a machine whose time may not be accurate in two ways. First of all, NTP never synchronizes to a machine that is not synchronized itself. Secondly, NTP compares the time reported by several machines, and will not synchronize to a machine whose time is significantly different than the others, even if its stratum is lower.

The communications between machines running NTP (associations) are usually statically configured. Each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is made possible by exchanging NTP messages between each pair of machines with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each machine can be configured to send or receive broadcast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

Cisco's implementation of NTP supports the stratum 1 service in certain Cisco IOS software releases. If a release supports the ntp refclock command, it is possible to connect a radio or atomic clock. Certain releases of Cisco IOS support either the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only) or the Telecom Solutions Global Positioning System (GPS) device. If the network uses the public time servers on the Internet and the network is isolated from the Internet, Cisco's implementation of NTP allows a machine to be configured so that it acts as though it is synchronized through NTP, when in fact it has determined the time using other means. Other machines then synchronize to that machine through NTP.

*directly from Cisco website*
**Note: NTP**
The following sections describe the associating modes used by NTP servers to associate with each other.

**Client/Server Mode**
Dependent clients and servers normally operate in client/server mode, in which a client or dependent server can be synchronized to a group member, but no group member can synchronize to the client or dependent server. This provides protection against malfunctions or protocol attacks.

Client/server mode is the most common Internet configuration.
A client sends an NTP message to one or more servers and processes the replies as received. The server interchanges addresses and ports, overwrites certain fields in the message, recalculates the checksum, and returns the message immediately.

Information included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock accordingly. In addition, the message includes information to calculate the expected timekeeping accuracy and reliability, as well as select the best server.

Servers that provide synchronization to a sizeable population of clients normally operate as a group of three or more mutually redundant servers, each operating with three or more stratum 1 or stratum 2 servers in client/server modes, as well as all other members of the group in symmetric modes. This provides protection against malfunctions in which one or more servers fail to operate or provide incorrect time.

**Symmetric Active/Passive Mode**
Symmetric active/passive mode is intended for configurations where a group of low stratum peers operate as mutual backups for each other. Each peer operates with one or more primary reference sources, such as a radio clock, or a subset of reliable secondary servers. Should one of the peers lose all reference sources or simply cease operation, the other peers automatically reconfigure so that time values can flow from the surviving peers to all the others in the clique.

Configuring an association in symmetric-active mode, usually indicated by a peer declaration in the configuration file, indicates to the remote server that one wishes to obtain time from the remote server and that one is also willing to supply time to the remote server if necessary. This mode is appropriate in configurations involving a number of redundant time servers interconnected through diverse network paths, which is presently the case for most stratum 1 and stratum 2 servers on the Internet today.

A peer is configured in symmetric active mode by using the peer command and specifying the DNS name or address of the other peer. The other peer is also configured in symmetric active mode in this way; this mode should always be authenticated.

**Broadcast and/or Multicast Mode**
Where the requirements in accuracy and reliability are modest, clients can be configured to use broadcast and/or multicast modes.

Normally, these modes are not utilized by servers with dependent clients. The advantage is that clients do not need to be configured for a specific server, allowing all operating clients to use the same configuration file. Broadcast mode requires a broadcast server on the same subnet. Since broadcast messages are not propagated by routers, only broadcast servers on the same subnet are used.

Broadcast mode is intended for configurations involving one or a few servers and a potentially large client population. A broadcast server is configured using the broadcast command and a local subnet address. A broadcast client is configured using the broadcastclient command, allowing the broadcast client to respond to broadcast messages received on any interface. Since an intruder can impersonate a broadcast server and inject false time values, this mode should always be authenticated.

**Peer** – permits router to respond to NTP requests and accept NTP updates. NTP control queries are also accepted. This is the only class which allows a router to be synchronized by other devices.

**Serve** – permits router to reply to NTP requests, but rejects NTP updates (e.g. replies from a server or update packets from a peer). Control queries are also permitted.

**Serve-only** – permits router to respond to NTP requests only. Rejects attempt to synchronize local system time, and does not access control queries.

**Query-only** – only accepts NTP control queries. No response to NTP requests are sent, and no local system time synchronization with remote system is permitted.

*directly from Cisco website*
NTP – Part I

SP#2 (R97) and SP#8 (R95) must provide an authoritative time source using stratum of 1 using their respective “NTP time server Loopback” interfaces to source packets from both Global NTP Servers should synchronize with each other using “GLOBALNTP” authentication key.

All Internet facing client office routers R13 R14 R20 and R21 (refer to NTP Diagram) must operate in a client mode and should synchronize their clocks with the global Internet NTP servers using “NTPBROADKEY?” authentication key 20, without the quotes.

SP#8 in BGP AS35426 should be the preferred global NTP time source.

Both SP Routers should always provide time on its interfaces (refer to NTP Diagram) without being asked for it.

Ensure that all devices retain the clock between in the event of a reboot.

All NTP clients must “always” use their Internet facing interfaces as the source of the NTP updates.

**Note:** At this point in the exam we should have reachability across between both Global NTP servers and all other routers required for completion of this section.

```
R13 R14 R20 R21 R95 R97

tclsh
foreach CCIE {
    63.69.0.150
    194.35.252.7
} { ping $CCIE re 10 }
tclquit

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 63.69.0.150, timeout is 2 seconds:
!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/10/12 ms

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 7/9/11 ms
R14(tcl)#tclquit
```

**Configuration:**

```
R97
ntp master 1
ntp source Loopback1032
ntp authenticate
ntp authentication-key 10 md5 GLOBALNTP
ntp trusted-key 10
ntp peer 194.35.252.7 key 10
ntp authentication-key 20 md5 NTPBROADKEY
ntp trusted-key 20

interface Serial2/0
ntp broadcast
```
R95
ntp master 1
ntp source Loopback110
ntp authenticate
ntp authentication-key 10 md5 GLOBALNTP
ntp authentication-key 20 md5 NTPBROADKEY?
ntp trusted-key 10
ntp trusted-key 20
ntp peer 63.69.0.150 key 10

interface Ethernet0/0
  ntp broadcast

interface Serial3/0
  ntp broadcast

R13
ntp authentication-key 20 md5 NTPBROADKEY?
npt authenticate
ntp trusted-key 20
ntp server 63.69.0.150 key 20
ntp server 194.35.252.7 key 20 prefer
ntp source Ethernet0/0

R14
ntp authentication-key 20 md5 NTPBROADKEY?
npt authenticate
ntp trusted-key 20
ntp server 63.69.0.150 key 20
ntp server 194.35.252.7 key 20 prefer
ntp source Ethernet2/0

R20
ntp authentication-key 20 md5 NTPBROADKEY?
npt authenticate
ntp trusted-key 20
ntp server 63.69.0.150 key 20
ntp server 194.35.252.7 key 20 prefer
ntp source Serial1/0

R21
ntp authentication-key 20 md5 NTPBROADKEY?
npt authenticate
ntp trusted-key 20
ntp server 63.69.0.150 key 20
ntp server 194.35.252.7 key 20 prefer
ntp source Ethernet0/0.222
Verification:

R13#sh ntp status
Clock is synchronized, stratum 2, reference is 194.35.252.7
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 40000 (1/100 of seconds), resolution is 4000
reference time is D847CAC8.CH66AA20 (12:53:44.796 CET Fri Dec 26 2014)
clock offset is -4.5000 msec, root delay is 11.00 msec
root dispersion is 16.07 msec, peer dispersion is 6.53 msec
loopfilter state is "CTRL" (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 89 sec ago.

R13#sh ntp associations detail
63.69.0.150 configured, ipv4, authenticated, insane, invalid, stratum 2
ref ID 194.35.252.7, time D847CAE4.EC8B4620 (12:54:12.924 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 18.99 msec, root disp 12.64, reach 77, sync dist 33.20
delay 10.00 msec, offset 0.0000 sec, dispersion 4.36, jitter 1.36 sec
precision 2**10, version 4
assoc id 54808, assoc name 63.69.0.150
assoc in packets 11, assoc out packets 11, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CB10.CA7EFC08 (12:54:56.791 CET Fri Dec 26 2014)
xmt time D847CB10.CA7EFC08 (12:54:56.791 CET Fri Dec 26 2014)
filtdelay = -1.70 -10.00 -10.00 -10.00 -10.00 -10.00 -10.00 -10.00
filtoffset = 1.95 3.96 4.99 6.00 6.88 4.19 3.94 3.94
filterror = 1.95 2.94 4.02 5.05 3.94 3.94 3.94 3.94
minpoll = 6, maxpoll = 10

194.35.252.7 configured, ipv4, authenticated, our master, sane, valid, stratum 1
ref ID .LOCL., time D847CB0A.E978D780 (12:54:50.912 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 2.19, reach 77, sync dist 17.67
delay 11.00 msec, offset 0.0000 msec, dispersion 2.76 sec
precision 2**10, version 4
assoc id 54807, assoc name 194.35.252.7
assoc in packets 11, assoc out packets 11, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CB0D.C72B0430 (12:54:53.778 CET Fri Dec 26 2014)
xmt time D847CB0D.C72B0430 (12:54:53.778 CET Fri Dec 26 2014)
filtdelay = 20.00 16.00 16.00 16.00 14.00 11.00 11.00 11.00
filtoffset = -9.00 -8.00 -7.00 -6.50 -6.00 -5.50 -5.00 -4.50
filterror = 1.95 2.98 4.02 5.05 6.09 6.93 6.96 6.99
minpoll = 6, maxpoll = 10

R14#sh ntp status
Clock is synchronized, stratum 2, reference is 194.35.252.7
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 37900 (1/100 of seconds), resolution is 4000
reference time is D847CB5E.D6C8B688 (12:56:14.839 CET Fri Dec 26 2014)
clock offset is 2.0000 msec, root delay is 6.00 msec
root dispersion is 23.66 msec, peer dispersion is 3.31 msec
loopfilter state is "CTRL" (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 128, last update was 25 sec ago.

R14#sh ntp associations detail
63.69.0.150 configured, ipv4, authenticated, insane, invalid, stratum 2
ref ID 194.35.252.7, time D847CAE4.EC8B4620 (12:54:12.924 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 18.99 msec, root disp 12.64, reach 77, sync dist 33.20
delay 10.00 msec, offset 0.0000 msec, dispersion 4.36, jitter 1.36 msec
precision 2**10, version 4
assoc id 31227, assoc name 63.69.0.150
assoc in packets 11, assoc out packets 11, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CB0D.C72B0430 (12:54:53.778 CET Fri Dec 26 2014)
xmt time D847CB0D.C72B0430 (12:54:53.778 CET Fri Dec 26 2014)
filtdelay = 30.00 10.00 10.00 10.00 12.00 10.00 10.00 10.00
filtoffset = -10.00 -9.00 -8.00 -7.50 -7.00 -6.50 -6.00 -5.50
filterror = 1.95 2.98 4.02 5.05 6.09 6.93 6.96 6.99
minpoll = 6, maxpoll = 10
194.35.252.7 configured, ipv4, authenticated, our master, sane, valid, stratum 1
ref ID: LOCL, time D847CB9A.EB852140 (12:56:11.056 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 64
root delay 0.00 msec, offset 2.21, reach 77, sync dist 24.78
delay 6.00 msec, offset 2.0000 msec, dispersion 3.31, jitter 15.76 msec
precision 2**10, version 4
assoc id 31226, assoc name 194.35.252.7
assoc in packets 11, assoc out packets 11, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CB8F.14FDF3F0 (12:57:03.082 CET Fri Dec 26 2014)
xmt time D847CB8F.14FDF3F0 (12:57:03.082 CET Fri Dec 26 2014)
filtdelay = 23.00 11.00 9.00 9.00 9.00 10.00 12.00 10.00
filtoffset = 4.50 -1.50 0.50 0.50 0.50 -1.00 1.00 0.00
filterror = 1.95 2.97 3.97 4.98 5.97 6.84 6.87 6.90
minpoll = 6, maxpoll = 10

R21#sh ntp status
Clock is synchronized, stratum 2, reference is 194.35.252.7
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 28800 (1/100 of seconds), resolution is 4000
reference time is D847CB8F.14FDF3F0 (12:57:03.082 CET Fri Dec 26 2014)
clock offset is 0.0000 msec, root delay is 12.00 msec
root dispersion is 7.41 msec, peer dispersion is 3.95 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.00000000 s/s
system poll interval is 64, last update was 77 sec ago.
R21#sh ntp associations detail
63.69.0.150 configured, ipv4, authenticated, insane, invalid, stratum 2
ref ID 194.35.225.7, time D847CB6D.EDGE5890 (12:56:29.926 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 18.99 msec, root disp 14.84, reach 37, sync dist 38.41
delay 10.00 msec, offset 1.0000 msec, dispersion 3.91, jitter 3.39 msec
precision 2**10, version 4
assoc id 29556, assoc name 63.69.0.150
assoc in packets 10, assoc out packets 10, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CBAF.ED0E5890 (12:56:29.926 CET Fri Dec 26 2014)
filtdelay = 15.00 33.00 13.00 12.00 13.00 13.00 10.00 15.00
filtoffset = -1.50 -7.50 0.50 0.00 0.50 0.50 1.00 1.50
filterror = 1.95 2.98 3.99 4.98 5.85 5.88 5.91 5.94
minpoll = 6, maxpoll = 10

194.35.252.7 configured, ipv4, authenticated, our master, sane, valid, stratum 1
ref ID LOCL, time D847CBAA.EAC08598 (12:57:30.917 CET Fri Dec 26 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 2.21, reach 37, sync dist 25.61
delay 12.00 msec, offset 0.0000 msec, dispersion 3.95, jitter 13.25 msec
precision 2**10, version 4
assoc id 29555, assoc name 194.35.252.7
assoc in packets 10, assoc out packets 10, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CBAF.E147B080 (12:57:35.880 CET Fri Dec 26 2014)
xmt time D847CBAF.E147B080 (12:57:35.880 CET Fri Dec 26 2014)
filtdelay = 84.00 12.00 13.00 12.00 13.00 15.00 15.00 15.00
filtoffset = 35.00 0.00 -1.50 0.00 -0.50 0.50 0.50 1.50
filterror = 1.95 2.98 3.99 5.02 5.88 5.91 5.94 5.97
minpoll = 6, maxpoll = 10

R95#sh ntp status
Clock is synchronized, stratum 1, reference is LOCL.
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 88000 (1/100 of seconds), resolution is 4000
reference time is D847CBDA.E9FBE9F0 (12:58:18.914 CET Fri Dec 26 2014)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.18 msec, peer dispersion is 1.20 msec
loop filter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 0 sec ago.

R95#sh ntp associations detail
127.127.1.1 configured, ipv4, our master, sane, valid, stratum 0
ref ID LOCL, time D847CBDA.E9FBE9F0 (12:58:18.914 CET Fri Dec 26 2014)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00 msec, reach 377, sync dist 2.34
delay 0.00 msec, offset 0.0000 msec, dispersion 1.20, jitter 0.97 msec
precision 2**10, version 4
assoc id 23756, assoc name 127.127.1.1
assoc in packets 56, assoc out packets 56, assoc error packets 0
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
xmt time D847CBDA.E9FBE9F0 (12:58:18.914 CET Fri Dec 26 2014)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtoffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 0.97 1.21 1.45 1.69 1.93 2.17 2.41 2.65
minpoll = 4, maxpoll = 4
63.69.0.150 configured, ipv4, authenticated, insane, invalid, stratum 2
ref ID 194.35.252.7, time D847CBBR1.EDC833B0 (12:57:37.922 CET Fri Dec 26 2014)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 1024
root delay 18.99 msec, root disp 14.20, reach 377, sync dist 42.18
delay 16.00 msec, offset -9.0000 msec, dispersion 5.59, jitter 4.12 msec
precision 2**10, version 4
assoc id 23757, assoc name 63.69.0.150
assoc in packets 21, assoc out packets 18, assoc error packets 3
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
filtdelay = 19.00 22.00 40.00 19.00 21.00 16.00 39.00 20.00
filtocffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 1.95 2.94 3.90 4.83 5.76 6.69 7.62 8.55
minpoll = 6, maxpoll = 10

R97#sh ntp status
Clock is synchronized, stratum 2, reference is 194.35.252.7
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 94500 (1/100 of seconds), resolution is 4000
reference time is D847CBFB.EE2589B0 (12:58:44.926 CET Fri Dec 26 2014)
clock offset is -0.5000 msec, root delay is 19.00 msec
root dispersion is 12.66 msec, peer dispersion is 4.15 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 1024, last update was 15 sec ago.
R97#sh ntp associations detail
127.127.1.1 configured, ipv4, insane, invalid, stratum 0
ref ID .LOCL., time D847CC0B.991688DD (12:58:58.598 CET Fri Dec 26 2014)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 2.31
delay 0.00 msec, offset 0.0000 msec, dispersion 1.20, jitter 0.97 msec
precision 2**10, version 4
assoc id 29932, assoc name 127.127.1.1
assoc in packets 60, assoc out packets 60, assoc error packets 0
rec time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
xmt time D847CC0B.991688DD (12:58:58.598 CET Fri Dec 26 2014)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtocffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 0.97 1.21 1.45 1.69 1.93 2.17 2.41 2.65
minpoll = 4, maxpoll = 4

194.35.252.7 configured, ipv4, authenticated, our master, sane, valid, stratum 1
ref ID .LOCL., time D847CBEA.E9374E58 (12:58:34.911 CET Fri Dec 26 2014)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 0.00 msec, root disp 2.31, reach 377, sync dist 21.79
delay 19.00 msec, offset -0.5000 msec, dispersion 4.15, jitter 5.48 msec
precision 2**10, version 4
assoc id 29933, assoc name 194.35.252.7
assoc in packets 19, assoc out packets 23, assoc error packets 1
org time 00000000.00000000 (01:00:00.000 CET Mon Jan 1 1900)
rec time D847CBEB.EA74E58C (12:58:44.916 CET Fri Dec 26 2014)
xmt time D847CBEB.EA74E58C (12:58:44.916 CET Fri Dec 26 2014)
filtdelay = 19.00 22.00 28.00 32.00 19.00 24.00 34.00 20.00
filtocffset = -0.50 1.00 4.00 -6.00 0.50 -1.00 12.00 0.00
filterror = 1.95 2.95 3.97 5.01 6.03 7.02 8.01 9.03
minpoll = 6, maxpoll = 10
NTP – Part II

SP#2 and SP#8 should only accept time updates from each other

Configuration:

**R95**

access-list 97 permit 63.69.0.150
ntp access-group peer 97

**R97**

access-list 95 permit 194.35.252.7
ntp access-group peer 95

Verification:

R95#sh access-lists 97
Standard IP access list 97
  10 permit 63.69.0.150 (5 matches)

R97#sh access-lists 95
Standard IP access list 95
  10 permit 194.35.252.7 (4 matches)

R97#debug ntp all
NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on

NTP message received from 194.35.252.7 on interface 'Loopback1032' (63.69.0.150).
NTP Core(DEBUG): ntp_receive: message received
NTP Core(NOTICE): ntp_receive: dropping message: RES_DONTSERVE restriction.
NTP message sent to 255.255.255.255, from interface 'Serial2/0' (86.191.16.5).
NTP message received from 155.84.74.41 on interface 'Loopback1032' (63.69.0.150).
NTP Core(DEBUG): ntp_receive: message received
NTP Core(NOTICE): ntp_receive: dropping message: RES_DONTSERVE restriction.
NTP message received from 194.35.252.7 on interface 'Loopback1032' (63.69.0.150).
NTP Core(DEBUG): ntp_receive: message received

R97#un all
All possible debugging has been turned off
R97#
DNS

SP#3 (R98) Loopback 1040 simulates Global DNS server 4.2.2.2
SP#3 (R91) and SP#3 (R93) are hosting www.facebook.com (117.3.48.150/32) and www.google.com (124.13.240.150/32) websites respectively
Make sure users from Sydney Business Model HQ VLAN10 VLAN20 VLAN50 are able to reach both websites by their FQDN names www.facebook.com and www.google.com, also open a telnet connection on port 80 and 443

Note: This question is a bit tricky and it is one of the reasons why is best to read the whole exam before going straight into configuration. In one of the BGP earlier sections we configured a route-map called ‘VIRUS’ on R98 to block any prefixes originated from BGP AS 15789 tagged with the community value of 91:91 meaning that R98 at this point is not able to reach Facebook Server IP Address 117.3.48.150/32 hence Sydney Business Model HQ users will not be able to get to it either.

R98#sh ip bgp regexp _15789$
BGP table version is 108, local router ID is 199.53.176.150
Status codes: s suppressed, d damped, h history, * valid, > best, i = internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i = IGP, e = EGP, ? = incomplete
RPFK validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf Weight Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 117.0.32.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 117.0.128.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 117.0.144/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 117.1.0.0/22</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 155.84.74.8/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 155.84.74.12/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 155.84.74.16/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>* 155.84.74.20/30</td>
<td>66.171.14.6</td>
<td>0 56775 10001 29737 25432 64784 15789 i</td>
</tr>
</tbody>
</table>

Note: There are few ways to fix it: One is we can either shutdown the internet connection Ethernet0/0 on R16 and let R17 and R18 takes over their Gateway roles as per one of the earlier sections or we can manipulate a route-map on R91 just for the Facebook Prefix and allow it into the BGP Table on R98 or we can remove the filtering from R98 but that would be way to easy so let’s focus on making changes on R91

R91

ip access-list standard FACEBOOK
   permit 117.3.48.150

route-map RedConnBGP permit 25
   match ip address FACEBOOK
R98#sh ip bgp regexp _15789$
BGP table version is 109, local router ID is 199.53.176.150
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>117.0.32.0/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>117.0.128.0/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>117.0.144.0/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>117.1.0.0/22</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 i</td>
</tr>
<tr>
<td>117.3.48.150/32</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>117.3.48.12/30</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>117.3.48.16/30</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 ?</td>
</tr>
<tr>
<td>117.3.48.20/30</td>
<td>66.171.14.6</td>
<td>0</td>
<td>56775</td>
<td>10001</td>
<td>29737 25432 64784 15789 ?</td>
</tr>
</tbody>
</table>

Note: This way we are still blocking the relevant prefixes from AS 15789 but we should be able to get to Facebook from VLAN10 VLAN20 and VLAN50. Let’s send a test ping from Server#4

SERVER#4#ping 117.3.48.150 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/25/28 ms

R16#sh ip nat translations
<table>
<thead>
<tr>
<th>Pro Inside global</th>
<th>Inside local</th>
<th>Outside local</th>
<th>Outside global</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp 155.84.74.15:4</td>
<td>192.168.140.100:4</td>
<td>117.3.48.150:4</td>
<td>117.3.48.150:4</td>
</tr>
</tbody>
</table>

Configuration:

R98
ip dns server
ip host www.google.com 124.13.240.150
ip host www.facebook.com 117.3.48.150
ip domain lookup source-interface Loopback1040

R16
ip name-server 4.2.2.2
ip domain lookup

SW6
ip domain lookup
ip name-server 192.16.16.16

SW7
ip domain lookup
ip name-server 192.16.16.16

SERVER#4
ip domain lookup

R91
ip http server
ip http secure-server

R93
ip http server
ip http secure-server
**Verification:**

R1#ping www.google.com

Translating "www.google.com"...domain server (4.2.2.2) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/10 ms

R1#ping www.facebook.com

Translating "www.facebook.com"...domain server (4.2.2.2) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/27/38 ms

SW6#ping google.com source vl 10

Translating "www.google.com"...domain server (192.16.16.16) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.120.106
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/14 ms

SW6#ping www.facebook.com source vl 10

Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.120.106
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 23/24/25 ms

SERVER4#ping www.google.com

Translating "www.google.com"...domain server (192.16.16.16) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/11 ms

SERVER4# ping www.facebook.com

Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/25/26 ms

SERVER4#telnet www.facebook.com 80

Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Trying www.facebook.com (117.3.48.150, 80) ... Open
exit
HTTP/1.1 400 Bad Request
Date: Fri, 26 Dec 2014 13:16:24 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to www.facebook.com closed by foreign host]
SERVER4#
SERVER4#telnet www.facebook.com 443
Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Trying www.facebook.com (117.3.48.150, 443)... Open
exit
^S^C
[Connection to www.facebook.com closed by foreign host]

SW6#telnet www.facebook.com 80 /source-interface vlan 10
Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Trying www.facebook.com (117.3.48.150, 80)... Open
exit
HTTP/1.1 400 Bad Request
Date: Fri, 26 Dec 2014 13:17:41 GMT
Server: cisco- IOS
Accept-Ranges: none
400 Bad Request
[Connection to www.facebook.com closed by foreign host]

SW6#telnet www.facebook.com 443 /source-interface vlan 10
Translating "www.facebook.com"...domain server (192.16.16.16) [OK]
Trying www.facebook.com (117.3.48.150, 443)... Open
^Z^S^C^V
[Connection to www.facebook.com closed by foreign host]

Note: 'show run' on R91 and R93 should show the pki certificate generated after we have issued 'ip http secure-server' command

crypto pki trustpoint TP-self-signed-91
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-91
  revocation-check none
  rsakeypair TP-self-signed-91

crypto pki certificate chain TP-self-signed-91
  certificate selfsigned 01
  3082021B 30820184 A0D30201 02020101 300D0609 2A864886 F70DD010 05050030
  2931273D 25060355 0403313B 49F532DD 53656CC6 2D536967 6E65642D 43657274
  69666693 6174652D 39313018 170D3134 31323236 31333134 35375A17 00323030
  31303130 30303030 305A3029 31273025 06035504 03011E49 4F325D35 656CC62D
  5369676E 65622D43 65727469 66696361 74652D39 310819F 300D0609 2A864886
  F70DD010 01050003 81000030 819028B1 81000C2D 560C2D26 6A2564C4 95591672
  AF004A14 99646CF5 3C43960F DEA809DE 663B8901 13575601 886BDE2 1DF3FE3E
  C360CD5B 63579BE 464D252B 807F4D7D E891EF69 78AC5173 187BF9B4 34176ADA
  F1F8C0C4 CAF1FA4B 15206380 BA6D86B7 D3314D56 0CD9F9BE F2F63748 5DDA7709
  F322FA87 F1A1CD0D 53BC3E69 4A240CBE 2C5F0203 010001A3 53050130 0F063055
  1D030101 0F040530 0301010F 301F0603 551D2304 18301680 147FE21D 5ABA8B90
  D617D918 848C76C1 68635FE4 38301D06 03551D0E 04160414 7FE21D5A BA89B09D
  17D91884 B76C16B 635FE438 300D0609 2A864886 F70DD010 05050003 811800D9
  E219EB2B B24A65B9 D077F755 B64ED6D3 315065EF 4EA965B5 8E93EFA1 2201681E
  A79B58EC F57B86A5 95AF5901 CDD41414 F894F2CC AF2C1408 1706762C 0A695255
  632305D0 F0FB55BD E5C3D610 5BDD83B3 DDB8A23F F889052D 7C4B1245 0B5F27E
  5AD1CCCD 578A4049 697C2568 0B73EC8F 8B5ACB5E 1B5420ED AD4F00DE CE30A2
  quit
HTTP

Berlin Remote Office internet facing router R14 has been dropping packets on its Ethernet2/0 Interface
R19 in Sydney needs to download R14’s Ethernet2/0 interface output “show interface Ethernet2/0” over HTTP
The file named “ethernetoutput” without the quotes, should be stored locally on R14’s flash
Ensure that only R19 is allowed to download this file via HTTP
R19 should authenticate with a username/password of HTTPUSER/HTTPPASSWORD

Configuration:

R14
  sh interface ethernet2/0 | redirect flash:ethernetoutput
  access-list 10 permit 155.84.74.38
  ip http server
  ip http path flash:ethernetoutput
  ip http authentication local
  ip http access-class 10

  username HTTPUSER password HTTPPASSWORD
  username HTTPUSER privilege 15

Verification:

R19#copy http://HTTPUSER:HTTPPASSWORD@140.60.88.29/unix:ethernetoutput unix:
  Destination filename [unix:ethernetoutput]? ethernetoutput
  Accessing http://*****:*****@140.60.88.29/unix:ethernetoutput...
  Loading http://*****:*****@140.60.88.29/unix:ethernetoutput
  1212 bytes copied in 0.105 secs (11543 bytes/sec)

R14#debug ip http all
  Protocol = HTTP/1.1 Method = GET
  Protocol = HTTP/1.1 Method = GET
  R14#un all
  All possible debugging has been turned off

R14#debug ip http authentication
  HTTP Server Authentication debugging is on
R14#
R19#dir unix:
Directory of unix:
57918 -rw- 131072 Dec 26 2014 01:00:45 +01:00 nvram_00019
59198 -rw- 1212 Dec 26 2014 14:36:31 +01:00 ethernetoutput
2147479552 bytes total (2147479552 bytes free)

R19#more unix:ethernetoutput
Ethernet2/0 is up, line protocol is up
   Hardware is AmdP2, address is aabb.cc00.0e02 (bia aabb.cc00.0e02)
   Internet address is 140.60.88.29/30
   MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input 00:00:27, output 00:00:05, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue: 0/40 (size/max)
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   253 packets input, 83422 bytes, 0 no buffer
   Received 243 broadcasts (0 IP multicasts)
   0 runs, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   1420 packets output, 153520 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
NETFLOW

Configure R18 as per the following requirements
The output shown below must be seen on R18 after R16 successfully pings PC#3
Netflow collector is located in the remote office#2 Loopback0 of R20

**Configuration:**

```
R18
  ip flow-export version 9
  ip flow-export destination 192.20.20.20 9996
  ip flow-top-talkers
top 10
  sort-by packets
  interface Tunnel10
  ip flow ingress
```

**Verification:**

```
R16#ping 192.168.160.100 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/12/67 ms

R18#sh ip flow top-talkers

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr SrcP DstP Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tu10</td>
<td>192.168.160.100</td>
<td>Et1/0</td>
<td>192.168.110.16</td>
<td>01 0000 0000 100</td>
</tr>
<tr>
<td>Tu10</td>
<td>10.10.10.19</td>
<td>Null</td>
<td>224.0.0.10</td>
<td>58 0000 0000 8</td>
</tr>
<tr>
<td>Tu10</td>
<td>10.10.10.20</td>
<td>Null</td>
<td>224.0.0.10</td>
<td>58 0000 0000 7</td>
</tr>
</tbody>
</table>

3 of 10 top talkers shown. 3 flows processed.

R18#sh ip flow export
```
Flow export v9 is enabled for main cache
Export source and destination details:
VRF ID : Default
  Destination(1)  192.20.20.20 (9996)
Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
NETFLOW

On R15 Enable Netflow to monitor the traffic leaving OSPF area0 towards the MPLS Backbone
Netflow collector IP Address is 172.155.155.155 where all statistics should be exported using port 2222
In case the export to this server fails, the accounting information should be exported to a backup server 172.156.156.156 with the same port number
If the primary server is not reachable within 3 seconds, then R15 should start exporting to the backup server
When the primary server becomes available R15 should wait 20 seconds before switching back
Generate Netflow samples on 1 out-of-every 800 packets

Configuration:

R15
ip flow-export source Loopback0
ip flow-export version 9
ip flow-export destination 172.155.155.155 2222 sctp
backup destination 172.156.156.156 2222
reliability full
backup mode fail-over
backup restore-time 20
backup mode fail-over
flow-sampler-map FLOW
mode random one-out-of 800
ip flow-export template options sampler
interface Ethernet0/0
flow-sampler FLOW
flow-sampler FLOW egress

Verification:

SERVER2#ping 192.168.210.21 re 1700
Type escape sequence to abort.
Sending 1700, 100-byte ICMP Echos to 192.168.210.21, timeout is 2 seconds:

Success rate is 100 percent (1700/1700), round-trip min/avg/max = 1/5/262 ms
R15#sh flow-sampler FLOW
Sampler : FLOW, id : 1, packets matched : 4, mode : random sampling mode
 sampling interval is : 800

R15#sh ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
 Source(1) 172.15.15.15 (Loopback0)
 Destination(1) 172.155.155.155 (2222) via SCTP
Version 9 flow records
0 flows exported in 0 udp datagrams
4 flows exported in 12 sctp messages
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
Flexible NETFLOW

R10 must examine all traffic sent and received via interfaces Ethernet0/0
R10 must collect a fingerprint of each IPv4 and IPv6 packet and determine if it is unique or similar to other packets
Each flow should be exported to the Solarwinds Netflow Collector SW#2 Loopback 0 IP Address 192.102.102.102 using UDP port 90 interface Loopback 0
The attributes that R10 must examine for both IPv4 and IPv6 flows are as follows:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- Class of Service
- Router interface
- ICMPv4 and ICMPv6

Configuration:

R10

```
flow record v4_RECORD1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport icmp ipv4 type
collect interface input
collect interface output

flow record v6_RECORD1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
match transport icmp ipv6 type
collect interface input
collect interface output

flow exporter EXPORTER-1
destination 192.102.102.102
source Loopback0
transport udp 90

flow monitor FLOW-MONITOR-1
exporter EXPORTER-1
record v4_RECORD1

flow monitor FLOW-MONITOR-2
exporter EXPORTER-1
record v6_RECORD1
interface Ethernet0/0
ip flow monitor FLOW-MONITOR-1 input
ip flow monitor FLOW-MONITOR-2 input
ip flow monitor FLOW-MONITOR-1 output
ip flow monitor FLOW-MONITOR-2 output
```
Verification:

R10#sh flow exporter statistics
Flow Exporter EXPORTER-1:
Packet send statistics (last cleared 00:03:46 ago):
Successfully sent: 9 (1079 bytes)

Client send statistics:
Client: Flow Monitor FLOW-MONITOR-1
Records added: 5
  - sent: 5
Bytes added: 115
  - sent: 115

Client: Flow Monitor FLOW-MONITOR-2
Records added: 5
  - sent: 4
Bytes added: 235
  - sent: 188
NAT

Your Web Server in San Francisco Data Centre (192.168.30.100) is listening on TCP port 80.
The server responds on public address 155.84.74.22:2323 from the Internet.
R96 Network Admin Loopback 307 (197.0.112.150/32) should manage the Server via telnet.
Ensure that telnet to the Web Server is successful as shown in exhibit:

**Configuration:**

```
R13
  interface Ethernet0/0
  ip nat outside

  interface Ethernet1/0
  ip nat inside

  ip nat inside source static tcp 192.168.30.100 80 155.84.74.22 2323 extendable
```

**Verification:**

Note: Before any changes are made:

```
R96#telnet 155.84.74.22 2323 /source-interface loopback 307
Trying 155.84.74.22, 2323 ...  
% Connection refused by remote host
WEBSEVERM1#debug ip tcp packet
TCP Packet debugging is on
WEBSEVERM1#debug ip tcp transactions
TCP special event debugging is on

Reserved port 0 in Transport Port Agent for TCP IP type 0
tcp0: I LISTEN 197.0.112.150:58266 192.168.30.100:80 seq 493388139
  OPTS 4 SYN WIN 4128
TCP: connection attempt to port 80
TCP: sending RST, seq 0, ack 493388140
TCP: sent RST to 197.0.112.150:58266 from 192.168.30.100:80
Released port 0 in Transport Port Agent for TCP IP type 0 delay 240000
TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
TCB 0x1F0C2D0 destroyed
WEBSEVERM1#
```

Note: Now after we have configured R13:

```
R96#telnet 155.84.74.22 2323 /source-interface loopback 307
Trying 155.84.74.22, 2323 ... Open
HTTP/1.1 400 Bad Request
Date: Fri, 26 Dec 2014 15:43:24 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 155.84.74.22 closed by foreign host]
```
WEBSERVER#1#

tcp0: I LISTEN 197.0.112.150:30043 192.168.30.100:80 seq 1676498596
    OPTS 4 SYN WIN 4128
TCB053B9938 created
TCB053B9938 getting property TCP STRICT_ADDR_BIND (19)
TCP0: state was LISTEN -> SYNRCVD [80 -> 197.0.112.150(30043)]
    TCP: tcb 53B9938 connection to 197.0.112.150:30043, peer MSS 536, MSS is 516
    TCP: sending SYN, seq 130666677, ack 1676498597
TCP0: Connection to 197.0.112.150:30043, advertising MSS 536

tcp0: O SYNRCVD 197.0.112.150:30043 192.168.30.100:80 seq 130666677
    OPTS 4 ACK 1676498597 SYN WIN 4128

tcp0: I SYNRCVD 197.0.112.150:30043 192.168.30.100:80 seq 1676498597
    ACK 130666678 WIN 4128
WEBSERVER#1#
TCP0: state was SYNRCVD -> ESTAB [80 -> 197.0.112.150(30043)]
TCB01F0C2D0 accepting 053B9938 from 197.0.112.150.30043
TCB053B9938 setting property TCP NONBLOCKING WRITE (10) 2E8BFD0
TCB053B9938 setting property TCP NONBLOCKING_READ (14) 2E8C0B4
TCB053B9938 setting property TCP KEEPALIVE (17) 2E8C0B4
TCP: Setting Keepalive interval and retries to 60 and 4

tcp0: I ESTAB 197.0.112.150:30043 192.168.30.100:80 seq 1676498597
    ACK 130666678 WIN 4128
TCP0: ACK timeout timer expired

tcp0: O ESTAB 197.0.112.150:30043 192.168.30.100:80 seq 130666678
    ACK 1676498597 WIN 4128
WEBSERVER#1#un all
All possible debugging has been turned off

Note: Check NAT translation on R13

R13#sh ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 155.84.74.22:2323 192.168.30.100:80 197.0.112.150:60560 197.0.112.150:60560
tcp 155.84.74.22:2323 192.168.30.100:80 --- --
EEM I

On R15 write a Cisco IOS EEM applet named "RESTART-INTERFACE" – without quotes
Use the " %LINEPROTO-5-UPDOWN" syslog pattern in order to trigger the script
Ensure that the script restarts interface Ethernet0/0 first then restarts interface Ethernet1/0

Configuration:

R15
event manager applet RESTART-INTERFACE
event syslog pattern "%LINEPROTO-5-UPDOWN"
action 1.0 cli command "enable"
action 2.0 cli command "conf t"
action 3.0 cli command "interface Ethernet0/0"
action 4.0 cli command "shut"
action 5.0 cli command "no shut"
action 6.0 cli command "interface Ethernet1/0"
action 7.0 cli command "shut"
action 8.0 cli command "no shut"

Verification:

R15#debug event manager action cli
Debug EEM action cli debugging is on
R15(config)#int et 0/0
R15#conf t
Debug EEM action cli debugging is on

R15(config-if)#sh
removal from session Interface flap

R15(config-if)#

dec 26 15:57:19.679: %BGP-5-ADJCHANGE: Process 100, Nbr 93.93.93.93 on Ethernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
R15(config-if)#

dec 26 15:57:21.649: %LINK5-CHANGED: Interface Ethernet0/0, changed state to administratively down
dec 26 15:57:22.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
R15(config-if)#

show interfaces status
NAME    IS STATUS  DESCRIPTION
Ethernet0/0     Down Down due to administratively shut
Ethernet1/0     Down Down due to administratively shut

R15(config-if)#

set interface Ethernet0/0 admin up
R15(config-if)#

show interfaces status
NAME    IS STATUS  DESCRIPTION
Ethernet0/0     Up Up
Ethernet1/0     Down Down due to administratively shut

R15(config-if)#

set interface Ethernet1/0 admin up
R15(config-if)#

show interfaces status
NAME    IS STATUS  DESCRIPTION
Ethernet0/0     Up Up
Ethernet1/0     Up Up
%HA_EM-LOG: RESTART-INTERFACE : DEBUG(cli_lib) : : OUT : R15>
%HA_EM-LOG: RESTART-INTERFACE : DEBUG(cli_lib) : : IN : R15>enable
%HA_EM-LOG: RESTART-INTERFACE : DEBUG(cli_lib) : : OUT : R15#
%HA_EM-LOG: RESTART-INTERFACE : DEBUG(cli_lib) : : IN  : R15#conf t

*Dec 26 15:57:26.758: %OSPF-5-ADJCHG: Process 100, Nbr 93.93.93.93 on Ethernet0/0 from EXSTART to DOWN, Neighbor Down: Interface down or detached.

R15(config-if)#do sh ip int br | ex un
Interface                IP-Address      OK? Method Status                Protocol
Ethernet0/0                140.60.88.33    YES NVRAM  up                    up
Ethernet1/0                172.31.100.15   YES NVRAM  up                    up
Loopback0                  172.15.15.15    YES NVRAM  up                    up

R15#show event manager history events
No.  Job Id Proc Status   Time of Event            Event Type        Name
1    1      Actv success  Fri Dec26 16:57:22 2014  syslog  applet: RESTART-INTERFACE
2    2      Actv success  Fri Dec26 16:57:26 2014  syslog  applet: RESTART-INTERFACE

R15#show event manager statistics policy
No.  Class     Triggered   Suppressed  Average     Maximum  Name
1    applet    2           0          1.181       1.203 RESTART-INTERFACE

tty is now going through its death sequence
R15(config-if)#
EEM II

Configure R16 with event manager applet “PIM_NEIGH_DOWN_DEBUG”
When the PIM adjacency goes down to R18 it should enable the “debug ip pim hello” and “debug ip pim timers”

Configure another EEM applet “PIM_NEIGH_UP_DEBUG”
When PIM neighborship comes up to R18 it should disable all the debug messages
Make sure that each event generates a syslog message with a priority of 6 that shows the name of the event being activated
These logs should be seen both in the console and in the log buffer
All events should be send as per the following:
- Email Server IP Address : 192.168.111.111
- Email sent to: networkteam@sydney.com
- Email sent from: 3rdparty@sydney.com
- CEO should be CC’d: ceo@sydney.com
- Subject: MulticastDown
- Loopback 0 should be used to source all messages from

Configuration:

R16

event manager applet PIM_NEIGH_DOWN_DEBUG
event syslog pattern "%PIM-5-NBRCHG: neighbor 192.168.110.18 DOWN"
action 1.0 cli command "enable"
action 2.0 cli command "debug ip pim hello"
action 3.0 cli command "debug ip pim timers"
action 4.0 syslog priority informational msg "PIM_NEIGH_DOWN_DEBUG"
action 5.0 mail server "192.168.111.111" to "networkteam@sydney.com" from "3rdparty@sydney.com" cc "ceo@sydney.com" subject "MulticastDown" source-interface Loopback0

R16

event manager applet PIM_NEIGH_UP_DEBUG
event syslog pattern "%PIM-5-NBRCHG: neighbor 192.168.110.18 UP"
action 1.0 cli command "enable"
action 2.0 cli command "undebug all"
action 3.0 syslog priority informational msg "PIM_NEIGH_UP_DEBUG"
action 4.0 mail server "192.168.111.111" to "networkteam@sydney.com" from "3rdparty@sydney.com" cc "ceo@sydney.com" subject "MulticastDown" source-interface Loopback0

logging on
logging console debugging
logging buffered debugging

Verification:

R16#debug event manager action cli
Debug EEM action cli debugging is on
R16#debug event manager action mail
Debug EEM action mail debugging is on

%PIM-5-NBRCHG: neighbor 192.168.110.18 DOWN on interface Ethernet2/0 DR
%PIM-5-DRCHG: DR change from neighbor 192.168.110.18 to 192.168.110.16 on interface Ethernet2/0
*Dec 26 19:00:47.370: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : CTL : cli_open called.
*Dec 26 19:00:47.375: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : IN : R16>enable
*Dec 26 19:00:47.375: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : OUT : R16#
*Dec 26 19:00:47.375: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : IN : R16>enable
*Dec 26 19:00:47.375: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : OUT : R16#
Dec 26 19:00:47.493: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : IN : R16#debug ip pim hello
Dec 26 19:00:47.619: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : OUT : PIM-HELLO debugging is on
Dec 26 19:00:47.619: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : OUT : R16#
Dec 26 19:00:47.619: %HA_EM-6-LOG: PIM_NEIGH_DOWN_DEBUG : DEBUG(cli_lib) : : IN : R16#debug ip pim timers
Dec 26 19:00:47.743: %HA_EM-6-LOG: fh_send_mail : : DEBUG(smtp_lib) ; <XML version="1.0" encoding="UTF-8" ?>
Dec 26 19:00:47.743: %HA_EM-6-LOG: fh_send_mail : : DEBUG(smtp_lib) ; <XML version="1.0" encoding="UTF-8" ?><fh_smtp_args><fh_smtp_src>Loopback0</fh_smtp_src><fh_smtp_port>25</fh_smtp_port><fh_smtp_secure>0</fh_smtp_secure></fh_smtp_args>
Dec 26 19:00:47.743: %HA_EM-6-LOG: fh_send_mail : : DEBUG(smtp_lib) ; <XML version="1.0" encoding="UTF-8" ?><fh_smtp_args><fh_smtp_src>Loopback0</fh_smtp_src><fh_smtp_port>25</fh_smtp_port><fh_smtp_secure>0</fh_smtp_secure></fh_smtp_args>
Dec 26 19:00:50.916: PIM(0) Twheel Start: Periodic Timer. delay: 1000 ms. jitter 0.
Dec 26 19:00:50.916: PIM(0) Twheel Clear: Periodic Timer.
Dec 26 19:00:57.920: PIM(0): Received v2 hello on Loopback0 from 192.16.16.16
Dec 26 19:00:57.920: PIM(0): Send periodic v2 Hello on Loopback0 with GenID = 3469957767
Dec 26 19:00:57.920: PIM(0): Twheel Clear: Hello Timer for idb Loopback0.
Dec 26 19:01:01.046: PIM(0): Received v2 hello on Ethernet2/0 from 192.168.110.18
PIM-5-NBRCHANGE: neighbor 192.168.110.18 UP on interface Ethernet2/0
Dec 26 19:01:01.046: PIM(0) Twheel Start: Hello Timer for idb Loopback0. delay: 29939 ms. jitter 3.
Dec 26 19:01:01.046: PIM(0): Send triggered v2 Hello on Ethernet2/0 with GenID = 3469942768
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Check Timer. delay: 500 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Reset Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Periodic Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0): Received v2 hello on Ethernet2/0 from 192.168.110.18
PIM-5-NBRCHANGE: neighbor 192.168.110.18 UP on interface Ethernet2/0
Dec 26 19:01:01.046: PIM(0) Twheel Start: Hello Timer for idb Loopback0. delay: 29939 ms. jitter 3.
Dec 26 19:01:01.046: PIM(0): Send triggered v2 Hello on Ethernet2/0 with GenID = 3469942768
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Check Timer. delay: 500 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Reset Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Periodic Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0): Received v2 hello on Ethernet2/0 from 192.168.110.18
PIM-5-NBRCHANGE: neighbor 192.168.110.18 UP on interface Ethernet2/0
Dec 26 19:01:01.046: PIM(0) Twheel Start: Hello Timer for idb Loopback0. delay: 29939 ms. jitter 3.
Dec 26 19:01:01.046: PIM(0): Send triggered v2 Hello on Ethernet2/0 with GenID = 3469942768
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Check Timer. delay: 500 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Reset Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Periodic Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0): Received v2 hello on Ethernet2/0 from 192.168.110.18
PIM-5-NBRCHANGE: neighbor 192.168.110.18 UP on interface Ethernet2/0
Dec 26 19:01:01.046: PIM(0) Twheel Start: Hello Timer for idb Loopback0. delay: 29939 ms. jitter 3.
Dec 26 19:01:01.046: PIM(0): Send triggered v2 Hello on Ethernet2/0 with GenID = 3469942768
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Check Timer. delay: 500 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Reset Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Periodic Timer. delay: 1000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Neighbor Timer for Nbr: 192.168.110.18. idb Ethernet2/0. delay: 105000 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0): Received v2 hello on Ethernet2/0 from 192.168.110.18
PIM-5-NBRCHANGE: neighbor 192.168.110.18 UP on interface Ethernet2/0
Dec 26 19:01:01.046: PIM(0) Twheel Start: Hello Timer for idb Loopback0. delay: 29939 ms. jitter 3.
Dec 26 19:01:01.046: PIM(0): Send triggered v2 Hello on Ethernet2/0 with GenID = 3469942768
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Check Timer. delay: 500 ms. jitter 0.
Dec 26 19:01:01.046: PIM(0) Twheel Start: Triggered RPF Reset Timer. delay: 1000 ms. jitter 0.
EEM III

R17 is considered a sensitive router due to its DHCP capabilities. Ensure that every time someone types the show run command it does not display any of the interfaces names in other words only the configuration applied under each interface should be visible as per below output.

**Configuration:**

```
R17
event manager applet SHOW_RUN_FILTER
event tag 1.0 cli pattern "show run" sync yes
action 1.0 cli command "enable"
action 2.0 cli command "show run | exclude interface"
action 3.0 puts $_cli_result
action 4.0 set $_exit_status 0
```

**Verification:**

```
R17#sh run
Building configuration...
<Output omitted>
ip address 192.17.17.17 255.255.255.255
!
bandwidth 100
ip address 20.20.20.17 255.255.255.0
!
no ip redirects
ip mtu 1400
ip nhrp authentication 67890
ip nhrp map multicast dynamic
ip nhrp network-id 67890
ip nhrp holdtime 3600
ip nhrp redirect
ip tcp adjust-mss 1380
load-interval 150
delay 10000
MTP source Ethernet0/0
MTP mode gre multipoint
MTP key 20
MTP protection ipsec profile DMVPNPROFILE shared
!
ip address 155.84.74.30 255.255.255.252
ip nat enable
!
no ip address
shutdown
!
no ip address
<Output omitted>
```

```
R17#show event manager statistics policy
<table>
<thead>
<tr>
<th>No.</th>
<th>Class</th>
<th>Triggered</th>
<th>Suppressed</th>
<th>Average Run Time</th>
<th>Maximum Run Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>applet</td>
<td>1</td>
<td>0</td>
<td>152.396</td>
<td>152.396</td>
<td>SHOW_RUN_FILTER</td>
</tr>
</tbody>
</table>
```

**Note:** 'show run' output on R17 should not show any interface names.
EEM IV

On R9 ensure that when users issue “show run” they will not be able to see the EEM configuration lines in the consoles output
Use an applet named “NOEEM”

Configuration:

```
R9
    event manager applet NOEEM
    event cli pattern "show run" sync yes
    action 111 cli command "enable"
    action 112 cli command "show run | excl applet|event|action"
    action 113 puts "$_cli_result"
    action 114 set _exit_status "0"
```

Verification:

```
R9#show event manager statistics policy

<table>
<thead>
<tr>
<th>No.</th>
<th>Class</th>
<th>Triggered</th>
<th>Suppressed</th>
<th>Average Run Time</th>
<th>Maximum Run Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>applet</td>
<td>1</td>
<td>0</td>
<td>2.991</td>
<td>2.991</td>
<td>NOEEM</td>
</tr>
<tr>
<td></td>
<td>event</td>
<td>{} cli</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Note:** ‘show run’ output on R9 should not show any EEM configuration lines
TFTP

Configure R10 to serve an IOS image named **R10IOS.bin** from flash via TFTP. Allow only requests from R13 to download the (fictitious) IOS image. R10 must use Ethernet0/0 interface for sending files via TFTP. Minimum timeout between TFTP retransmissions must be 6 seconds.

**Configuration:**

R10

```
ip tftp source-interface ethernet0/0

copy flash:vlan.dat flash:R10IOS.bin

access-list 60 permit 155.84.74.22

tftp-server unix:R10IOS.bin 60

ip tftp min-timeout 6
```

**Verification:**

R10#dir unix:
Directory of unix: /
57926 -rw- 131072 Jan 18 2015 10:56:27 +01:00 nvram_00010
59262 -rw- 131072 Jan 18 2015 12:04:55 +01:00 **R10IOS.bin**
2147479552 bytes total (2147479552 bytes free)

R10#debug tftp events
TFTP Event debugging is on
R10#debug tftp packets
TFTP Packet debugging is on

R13#copy tftp: null:
Address or name of remote host [155.84.74.9]?
Source filename [R10IOS.bin]?

Accessing tftp://155.84.74.9/R10IOS.bin...
Loading R10IOS.bin from 155.84.74.9 (via Ethernet0/0): !
[OK - 131072 bytes]
131072 bytes copied in 0.887 secs (147770 bytes/sec)

TFTP: Server request for port 63819, socket_id 0x4571590 for process 364
TFTP: read request from host 155.84.74.22(63819) via Ethernet0/0
TFTP: Locked for R10IOS.bin
TFTP: Opened flash:R10IOS.bin, fd 0, size 131072 for process 364
TFTP: Sending block 1 (retry 0), len 512, socket_id 0x4571590
TFTP: Received ACK for block 1, socket_id 0x4571590
TFTP: Sending block 2 (retry 0), len 512, socket_id 0x4571590
TFTP: Received ACK for block 2, socket_id 0x4571590
TFTP: Sending block 3 (retry 0), len 512, socket_id 0x4571590
<Output omitted>
TFTP: Finished flash:R10IOS.bin, time 00:00:01 for process 364
R10#un all
All possible debugging has been turned off
Sydney Business Model HQ

DHCP Snooping

Protect users in VLANs 567 from rogue DHCP servers
Ensure that only R17 services the DHCP requests
All the insertion and removal of option-82

In the near future the customer will connect a printer to SW7's interface Ethernet1/3 in VLAN 50
The printer should be assigned a static IP address 192.168.140.155 that should expire after 1 hour
The printer's MAC address is abcd.abcd.abcd

Ensure that the printer is able to communicate with the users on VLAN 50
SW1 should ensure that your solution survives a reload and should store the binding database in flash
with the filename `dhcpbindings.txt`, and use a 15 second delay between changes

**Configuration:**

**SW7**

```
ip dhcp snooping
ip dhcp snooping vlan 567
ip dhcp snooping information option allow-untrusted

ip dhcp snooping binding abcd.abcd.abcd vlan 50 192.168.140.155 interface ethernet 1/3 expiry 1800

interface Ethernet0/0
  ip dhcp snooping trust

interface Ethernet0/1
  ip dhcp snooping trust
```

**SW6**

```
ip dhcp snooping
ip dhcp snooping vlan 567
ip dhcp snooping information option allow-untrusted
ip dhcp snooping database unix:/dhcp-bindings.txt_00056
ip dhcp snooping database write-delay 15

interface Ethernet0/0
  ip dhcp snooping trust

interface Ethernet0/1
  ip dhcp snooping trust

interface Ethernet0/2
  ip dhcp snooping trust

interface Ethernet0/3
  ip dhcp snooping trust
```

**R17**

```
ip dhcp relay information trust-all
```
SERVER4(config)#int et 0/0
SERVER4(config-if)#shu

*Dec 26 19:16:55.580: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Dec 26 19:16:56.585: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SERVER4(config-if)#no sh

*Dec 26 19:20:53.418: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Dec 26 19:29:25.643: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.140.100, mask 255.255.255.0, hostname SERVER4

SM6#debug ip dhcp snooping packet
DHCP Snooping Packet debugging is on
SM6#debug ip dhcp snooping event
DHCP Snooping Event debugging is on

*Dec 26 19:29:21.593: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/3)

*Dec 26 19:29:21.595: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/2)


*Dec 26 19:29:21.604: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/3)

*Dec 26 19:29:21.604: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input interface: Et0/3, MAC da: aabb.cc00.1101, MAC sa: aabb.cc00.1001, IP da: 192.17.17.17, IP sa: 192.168.140.107, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 192.168.140.107, DHCP chaddr: aabb.ccdd.aabb


*Dec 26 19:29:21.604: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/2)


SM6#un all
All possible debugging has been turned off

SW6#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
  567
DHCP snooping is operational on following VLANs:
  567
DHCP snooping is configured on the following L3 Interfaces:

<table>
<thead>
<tr>
<th>Insertion of option 82 is enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>circuit-id default format: vlan-mod-port</td>
</tr>
<tr>
<td>remote-id: aabb.cc00.3800 (MAC)</td>
</tr>
</tbody>
</table>

Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Allow option</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

**Custom circuit-ids:**

<table>
<thead>
<tr>
<th>Circuit-id</th>
<th>Description</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Allow option</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Custom circuit-ids:</th>
</tr>
</thead>
</table>

435 | Page
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:

567

DHCP snooping is operational on following VLANs:

567

DHCP snooping is configured on the following L3 Interfaces:

**Insertion of option 82 is enabled**
- circuit-id default format: vlan-mod-port
- remote-id: aabb.cc00.3900 (MAC)

**Option 82 on untrusted port is not allowed**

Verification of hwaddr field is enabled
Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Allow option</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Custom circuit-ids:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>yes</td>
<td>yes</td>
<td>unlimited</td>
</tr>
<tr>
<td>Custom circuit-ids:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Switch DHCP snooping database
Agent URL : unix:/dhcp-bindings.txt_00056
Write delay Timer : 15 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeeded Time : 20:40:16 CET Fri Dec 26 2014
Last Failed Time : None
Last Failed Reason : No failure recorded.

<table>
<thead>
<tr>
<th>Total Attempts</th>
<th>1</th>
<th>Startup Failures : 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Transfers</td>
<td>1</td>
<td>Failed Transfers : 0</td>
</tr>
<tr>
<td>Successful Reads</td>
<td>0</td>
<td>Failed Reads : 0</td>
</tr>
<tr>
<td>Successful Writes</td>
<td>1</td>
<td>Failed Writes : 0</td>
</tr>
<tr>
<td>Media Failures</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Directory of unix:/dhcp-bindings.txt_00056
59201 -rw- 47 Dec 26 2014 20:40:16 +01:00 dhcp-bindings.txt_00056
21479552 bytes total (21479552 bytes free)
**NBAR**

San Francisco Group DC staff need to block all HTTP download attempts coming from Server#1 to the internet

Configure R13 to drop any download attempts with "**.exe**, **.com**" file extension

Server#1 should only be able to download "**.bin**" files extension from the internet R91

Simulate HTTP server with R91 and create the **vlan.dat** file with the above extensions

Username should be **admin** with password of **cisco**

**Configuration:**

**R91**

username admin privilege 15 password 0 cisco

ip http server
ip http authentication local
ip http path flash:

copy flash:vlan.dat flash:vlan.exe
Destination filename [vlan.exe]?
Copy in progress...C
1216 bytes copied in 1.082 secs (1124 bytes/sec)

copy flash:vlan.dat flash:vlan.com
Destination filename [vlan.com]?
Copy in progress...C
1216 bytes copied in 0.023 secs (48640 bytes/sec)

copy flash:vlan.dat flash:vlan.BIN
Destination filename [vlan.BIN]?
Copy in progress...C
1216 bytes copied in 0.025 secs (48640 bytes/sec)

**R13**

class-map match-all EXTENSION
  match protocol http url "**.exe|*.com""

policy-map DROP
  class EXTENSION
    drop

interface Ethernet 1/0
  service-policy output DROP

**Verification:**

**Note: We will try and download all three files before making any configuration changes on R13**

WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.exe null:
Accessing http://*****:*****@155.84.74.21/vlan.exe...
Loading http://*****:*****@155.84.74.21/vlan.exe !
131072 bytes copied in 0.316 secs (414785 bytes/sec)
WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.com null:
Accessing http://*****:*****@155.84.74.21/vlan.com...
Loading http://*****:*****@155.84.74.21/vlan.com !
131072 bytes copied in 0.331 secs (395988 bytes/sec)

WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.bin null:
Accessing http://*****:*****@155.84.74.21/vlan.bin...
Loading http://*****:*****@155.84.74.21/vlan.bin !
131072 bytes copied in 0.273 secs (480117 bytes/sec)

**Note:** Looks like at the moment we are able download anything from the internet so let’s now try again after we have configured appropriate policy on R13

WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.com null:
Accessing http://*****:*****@155.84.74.21/vlan.com...
*Error opening http://*****:*****@155.84.74.21/vlan.com (I/O error)*

WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.exe null:
Accessing http://*****:*****@155.84.74.21/vlan.exe...
*Error opening http://*****:*****@155.84.74.21/vlan.exe (I/O error)*

WEBSERVER1#copy http://admin:cisco@155.84.74.21/vlan.bin null:
Accessing http://*****:*****@155.84.74.21/vlan.bin...
Loading http://*****:*****@155.84.74.21/vlan.bin !
131072 bytes copied in 0.291 secs (450419 bytes/sec)

R13#sh policy-map interface et 1/0
Ethernet1/0
Service-policy output: DROP
Class-map: EXTENSION (match-all)
  18 packets, 2372 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: protocol http url "*.exe|*.com" drop
Class-map: class-default (match-any)
  1496 packets, 644496 bytes
  5 minute offered rate 5000 bps, drop rate 0000 bps
  Match: any

**Note:** Much better, now we can only download files with .bin extension
QOS

Configure an outbound MQC policy on R16 Ethernet link to R99 per the following requirements:

· WWW traffic from HR Dept on VLAN 10 should be marked with an IP Precedence of 2
· VoIP packets with UDP ports in the destination range of 16384 – 32767 and a Layer 3 packet size of 60 bytes should be marked with DSCP EF
· ICMP packets larger than 1000 bytes should be dropped
· All other packets with an IP precedence of 0 should be remarked with an IP precedence of 1

Do not use an access-list to classify ICMP packets

Configuration:

R16

ip access-list extended HTTP
  permit tcp 192.168.120.0 0.0.0.255 eq www any

ip access-list extended VOICE
  permit udp any any range 16384 32767

class-map match-all LARGE_ICMP
  match protocol icmp
  match packet length min 1001

class-map match-all HTTP
  match access-group name HTTP

class-map match-all OTHER
  match ip precedence 0

class-map match-all VOICE
  match access-group name VOICE
  match packet length min 60 max 60

policy-map QOS-MARK
  class VOICE
    set ip dscp ef
  class HTTP
    set ip precedence 2
  class OTHER
    set ip precedence 1
  class LARGE_ICMP
    drop

  interface Ethernet0/0
  /service-policy output QOS-MARK

Note: In order to source 'voice-like' packets on SW6 we need to start IP SLA jitter operation with the G.729 codec(60 bytes each) and we will target SP#4 Ethernet0/0 interface

SW6

ip sla 1
  udp-jitter 155.84.74.26 16384 source-ip 192.168.120.106 codec g729a
  ip sla schedule 1 life forever start-time now

R99

ip sla responder
SW6#sh ip sla statistics
IPSla's Latest Operation Statistics
IPSLA operation id: 1

**Type of operation: udp-jitter**

Latest RTT: 1 milliseconds
Latest operation start time: 20:06:23 CET Sat Dec 27 2014
Latest operation return code: OK

**RTT Values:**
- Number Of RTT: 1000  
  RTT Min/Avg/Max: 1/1/158 milliseconds

**Latency one-way time:**
- Number of Latency one-way Samples: 721  
  Source to Destination Latency one way Min/Avg/Max: 0/1/16 milliseconds  
  Destination to Source Latency one way Min/Avg/Max: 1/0/153 milliseconds

**Jitter Time:**
- Number of SD Jitter Samples: 999
- Number of DS Jitter Samples: 999
- Source to Destination Jitter Min/Avg/Max: 0/1/16 milliseconds
- Destination to Source Jitter Min/Avg/Max: 0/2/153 milliseconds

**Packet Loss Values:**
- Loss Source to Destination: 0
- Source to Destination Loss Periods Number: 0
- Source to Destination Loss Period Length Min/Max: 0/0
- Source to Destination Inter Loss Period Length Min/Max: 0/0
- Loss Destination to Source: 0
- Destination to Source Loss Periods Number: 0
- Destination to Source Loss Period Length Min/Max: 0/0
- Destination to Source Inter Loss Period Length Min/Max: 0/0
- Out Of Sequence: 0
- Tail Drop: 0
- Packet Late Arrival: 0
- Packet Skipped: 0

**Voice Score Values:**
- Calculated Planning Impairment Factor (ICPIF): 11
- MOS score: 4.06

**Number of successes: 2**
**Number of failures: 0**

**Operation time to live: Forever**

R16#sh policy-map interface et 0/0
Ethernet0/0/
Service-policy output: QOS-MARK
Class-map: VOICE (match-all)

  **1324 packets**, 97976 bytes
  5 minute offered rate 3000 bps, drop rate 0000 bps
  Match: access-group name VOICE
  Match: packet length min 60 max 60
  QoS Set
dscp ef
  Packets marked 1324

Class-map: HTTP (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name HTTP
QoS Set
Precedence 2
Packets marked 0
Class-map: OTHER (match-all)
279 packets, 24808 bytes
SW6#ping 4.2.2.2 source 192.168.120.106 repeat 100 size 1500 timeout 0
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 4.2.2.2, timeout is 0 seconds:
Packet sent with a source address of 192.168.120.106

Success rate is 0 percent (0/100)

R16#sh policy-map interface et 0/0
Ethernet0/0
Service-policy output: QOS-MARK
Class-map: VOICE (match-all)
  4000 packets, 296000 bytes
  5 minute offered rate 10000 bps, drop rate 0000 bps
  Match: access-group name VOICE
  Match: packet length min 60 max 60
  QoS Set:
    dscp ef
    Packets marked 4000
Class-map: HTTP (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: access-group name HTTP
  QoS Set:
    precedence 2
    Packets marked 0
Class-map: OTHER (match-all)
  433 packets, 41036 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: ip precedence 0
  QoS Set:
    precedence 1
    Packets marked 312
Class-map: LARGE_ICMP (match-all)
  100 packets, 100800 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: protocol icmp
  Match: packet length min 1001
  drop
Class-map: class-default (match-any)
  456 packets, 33368 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any
SNMP

On R9 permit any SNMP to access all objects with read-only permission using the community string named public.

The device should be configured as follows:

- Traps send to the Solarwinds Serve simulated by SW2 Loopback 0 IPv4 and IPv6 Address
- Border Gateway Protocol (BGP)
- OSPFv3 state changes

```
R9#sh snmp host
Notification host: 192.102.102.102  udp-port: 162  type: trap
user: public  security model: v1

Notification host: 2010:CAFE:102::102  udp-port: 162  type: trap
user: public  security model: v2c
```

Configuration:

```
R9
snmp-server community public RO
snmp-server enable traps bgp
snmp-server enable traps ospfv3 state-change
snmp-server host 192.102.102.102 public
snmp-server host 2010:CAFE:102::102 version 2c public
```

Verification:

```
R9#debug snmp packets
SNMP packet debugging is on

R9(config)#int loo 0
R9(config-if)#sh
R9(config-if)#int et 1/0
R9(config-if)#sh

SNMP: Queuing packet to 192.102.102.102
SNMP: V1 Trap, ent ospfv3MIB, addr 192.168.10.9, gentrap 6, spectrap 10
  ospfv3GeneralGroup.1 = 3221817609
  ospfv3IfEntry.12 = 1

SNMP: Queuing packet to 2010:CAFE:102::102
SNMP: V2 Trap, reqid 88, errstat 0, erridx 0
  sysUpTime.0 = 2705528
  snmpTrapOID.0 = ospfv3Notifications.10
  ospfv3GeneralGroup.1 = 3221817609
  ospfv3IfEntry.12 = 1

SNMP: Packet sent via UDP to 192.102.102.102
SNMP: Packet sent via UDP to 2010:CAFE:102::102

SNMP: Queuing packet to 192.102.102.102
SNMP: V1 Trap, ent bgpTraps, addr 192.168.10.9, gentrap 6, spectrap 2
  bgpPeerEntry.14.192.8.8.8 = 04 00
  bgpPeerEntry.2.192.8.8.8 = 1

SNMP: Queuing packet to 2010:CAFE:102::102
SNMP: V2 Trap, reqid 94, errstat 0, erridx 0
  sysUpTime.0 = 2721770
```
snmpTrapOID.0 = bgpTraps.2
bgpPeerEntry.14.192.8.8.8 = 04 00
bgpPeerEntry.2.192.8.8.8 = 1
SNMP: Queuing packet to 192.102.102.102
SNMP: V1 Trap, ent ciscoBgp4MIB, addr 192.168.10.9, gentrap 6, spectrap 2
bgpPeerEntry.14.192.8.8.8 = 04 00
bgpPeerEntry.2.192.8.8.8 = 1
cbgpPeerEntry.7.192.8.8.8 = hold time expired
cbgpPeerEntry.8.192.8.8.8 = 6
SNMP: Queuing packet to 2010:CAFE:102::102
SNMP: V2 Trap, reqid 96, errstat 0, erridx 0
sysUpTime.0 = 2721771
snmpTrapOID.0 = ciscoBgp4NotifyPrefix.2
bgpPeerEntry.14.192.8.8.8 = 04 00
bgpPeerEntry.2.192.8.8.8 = 1
cbgpPeerEntry.7.192.8.8.8 = hold time expired
cbgpPeerEntry.8.192.8.8.8 = 6
R3(config-if)#do u all
**SNMP**

Configure R19 to send SNMPv2 NHRP notifications to host 192.200.200.200 using community string public with read-write access permissions
Allow the system to be reloaded via SNMP

**Configuration:**

```
R19

snmp mib nhrp

snmp-server community public rw
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server host 192.200.200.200 version 2c public
snmp-server system-shutdown
```

**Verification:**

```
R19#show snmp mib nhrp status
NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 0

R19#debug snmp packets
SNMP packet debugging is on

R19(config)#int mul 1
R19(config-if)#shu
R19(config-if)#
SNMP: Queuing packet to 192.200.200.200
SNMP: V2 Trap, reqid 1, errstat 0, erridx 0
sysUpTime.0 = 2907146
snmpTrapOID.0 = cneNotifNextHopRegServerDown
nhrpClientInternetworkAddrType.1 = 1
nhrpClientInternetworkAddr.1 = 0A 0A 0A 13
nhrpClientNbmaAddrType.1 = 1
nhrpClientNbmaAddr.1 = 9B 54 4A 26
nhrpClient NbmaSubaddr.1 = NULL TYPE/VALUE
nhrpClientNhsInternetworkAddrType.1.1 = 1
nhrpClientNhsInternetworkAddr.1.1 = 0A 0A 0A 12
nhrpClientNhsNbmaAddrType.1.1 = 1
nhrpClientNhsNbmaAddr.1.1 = 9B 54 4A 22
nhrpClientNhsNbmaSubaddr.1.1 = NULL TYPE/VALUE
cneNextHopDownReason.0 = 6
cneNHRPException.0 = 256
R19(config-if)#do u all
All possible debugging has been turned off

R19#sh snmp mib nhrp status
NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 2
```
**SNMPv3**

On R20 configure two SNMP views:

**ADMIN** – enable ISO and cisco MIB

**LEVEL1** – enable system mib

SNMPv3 group **ADMIN** – should have a read/write privilege configured and must view only iso and cisco MIBs

SNMPv3 group **LEVEL1** – should have a view privilege and write only system mibs

User **LEVEL1** should be from the LEVEL1 group and use md5 password of CISCO

Ensure that LEVEL1 group only allow users access from 192.168.0.0/16

SNMPv3 group named **TRAP** with the security model “priv”

Assign the user named **TRAP** to this group, set the SHA1 password to CISCO, and the encryption key to CISCO

SNMP traps should be generated when an interface changes its state up/down
SNMP traps should be sent to the destination NMS 192.168.161.20 using the security model “priv” and the username **TRAP**

**Configuration:**

```
R20
access-list 99 permit 192.168.0.0 0.0.255.255
snmp-server ifindex persist
snmp-server view ADMIN iso included
snmp-server view ADMIN cisco included
snmp-server view LEVEL1 system included

snmp-server group ADMIN v3 priv read ADMIN write ADMIN
snmp-server group LEVEL1 v3 auth read LEVEL1 access 99
snmp-server group TRAP v3 priv

snmp-server user ADMIN ADMIN v3 auth sha CISCO priv des56 CISCO
snmp-server user LEVEL1 LEVEL1 v3 auth sha CISCO
snmp-server user TRAP TRAP v3 auth sha CISCO priv des56 CISCO

snmp-server enable traps snmp linkup linkdown
snmp-server host 192.168.161.20 traps version 3 priv TRAP
```

**Verification:**

```
R20#sh snmp user

User name: TRAP
Engine ID: 800000090300AABBCC001400
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: TRAP

User name: ADMIN
Engine ID: 800000090300AABBCC001400
storage-type: nonvolatile active
```
Authentication Protocol: SHA
Privacy Protocol: DES

Group-name: ADMIN

User name: LEVEL1
Engine ID: 8000000090300AABBCC001400
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: None

Group-name: LEVEL1

R20#sh snmp group

groupname: ILMI
contextname: <no context specified>
readview: *ilmi
notifyview: <no notifyview specified>
row status: active

security model:v1
storage-type: permanent
writeview: *ilmi

contextname: <no context specified>
readview: *ilmi
notifyview: <no notifyview specified>
row status: active

security model:v2c
storage-type: permanent
writeview: *ilmi

groupname: TRAP
contextname: <no context specified>
readview: vldefault
notifyview: *(tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
row status: active

security model:v3 priv
storage-type: nonvolatile
writeview: <no writeview specified>

groupname: ADMIN
contextname: <no context specified>
readview: ADMIN
notifyview: <no notifyview specified>
row status: active

security model:v3 priv
storage-type: nonvolatile
writeview: ADMIN

groupname: LEVEL1
contextname: <no context specified>
readview: LEVEL1
notifyview: <no notifyview specified>
row status: active

security model:v3 auth
storage-type: nonvolatile
writeview: <no writeview specified>

R20#sh snmp view

*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
ADMIN iso - included nonvolatile active
ADMIN cisco - included nonvolatile active
LEVEL1 system - included nonvolatile active
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view interfaces - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ifMIB - included read-only active
cac_view hzrpMIB - included read-only active
cac_view ipMRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
Note: We will now check if SNMP traps are being sent encrypted and authenticated

R20

   access-list 115 permit udp any any eq 162

R20#debug ip packet detail 115 dump
IP packet debugging is on (detailed) (dump) for access list 115
R20#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R20(config)#int lo 0
R20(config-if)#shut

*Jan 6 17:18:33.412: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
*Jan 6 17:18:34.417: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
R20#

A312CC80: 45000011B 00000000 FF11F757 C0A8A114 E........e @(!.
A312CC90: C0A8A114 DFD600A2 01075FA4 3081FCO2 @(!._V."..._S0.
A312CCAO: 01033000 02010000 0205DC04 01030201 .0........\\
A312CCBO: 03043530 3304C800 00090903 00AABBCC ....503.........*;L
A312CCCO: 00140002 01010202 05B40404 54524150 ..........."\TRAP Q
A312CCD0: 040C5997 F7B7F9C3 333523C3 B5240408 \7\w7..35B<566.
A312CCEO: 00000000 C8641E80 0481B02F 79A88B58 ....Nd.../y..X
A312CCFO: A7079DE7 5C5B1814 198E389A C7F2D710 \...gD...8:GrW.
A312CCDO: 10FB6250 E9D299DE F403AEEF C3A2F700 .(bPIR."...?C/\p
A312CCDO: 87234274 4CD3F0C0 BBACF968 9645F3E5 .#Btl?....y.y.Exe
A312CCDO: A01784F2 DD67DDFD 014A9FBB B1CB5FFF ..r]g][.]f:KK.
A312CCDO: 9F4E7E99 PTOF6E29 94C13B66 9C7F272E \N..ppn).L:f.Wc-
A312CCDO: 81FE79FD 97169328 89A21646 07E91426 \..y)...E!d.i&
A312CCDO: D7B75812 31346898 20FB8CD1 CFC62380 W7...14h. 7.QOF#.
A312CCDO: 4ACDA2A 147902C8 56416240 785B5ABE JCC"."y."%66%2Z2
A312CCDO: 197D4E7D 1D06FA99 202F966F EEEBEFFF ..Mg.Vt)../kn&.
A312CCDO: 31FA5555 C110B602 562100F4 63C5F36A 1zUW.6.V.tcoca
A312CCDO: 9086F92F 9522BEB7 8B8CA5 .olryR++..2 , Logical MN local(14), rtype 0,
forus FALSE, sendself FALSE, mtu 0, fdwck FALSE
FIBip4-packet: FIBip4-packet: route packet from (local) src 192.168.161.20
dst 192.168.161.20

Note: Change the security model for the destination host to 'noauth'; and generate trap message again. The message
now should not be encrypted.

R20(config)#int lo 0
R20(config-if)#shu
R20(config-if)#^Z

*Jan 6 17:24:08.975: %SYS-5-CONFIG_I: Configured from console by console
*Jan 6 17:24:09.190: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
R20#
*Jan 6 17:24:10.196: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
IP: s=192.168.161.20 (local), d=192.168.161.20 (Loopback1), routed via RIB
UDP src=57302, dst=162

Note: Change the security model for the destination host to 'noauth'; and generate trap message again. The message
now should not be encrypted.

R20(config)#int lo 0
R20(config-if)#shu
R20(config-if)#^Z

*Jan 6 17:24:08.975: %SYS-5-CONFIG_I: Configured from console by console
*Jan 6 17:24:09.190: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
R20#
*Jan 6 17:24:10.196: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
IP: s=192.168.161.20 (local), d=192.168.161.20, len 258, local feature
UDP src=57302, dst=162
FIBipv4-packet-proc: route packet from (local) src 192.168.161.20 dst 192.168.161.20
FIBfwd-proc: Default:192.168.161.20/32 receive entry
FIBipv4-packet: routing failed

IP: s=192.168.161.20 (Loopback1), d=192.168.161.20 (Loopback1), len 258, sending
UDP src=57302, dst=162
All possible debugging has been turned off.
VERIFICATION

Note: End of Configuration Lab#1 – If you have configured each question without looking at the solution you should consider booking your CCIEv5 Lab Exam.
We should be able to establish reachability between the following so the final test is:

PC#3 – PC#1 over IPSec VPN

ping 192.168.20.100 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.20.100, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 22/25/30 ms

Other devices

R20(tcl)#foreach CCIE 
>{155.84.74.38} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 17/24/42 ms

R20(tcl)#foreach CCIE 
>{155.84.74.30} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 8/10/15 ms

R20(tcl)#foreach CCIE 
>{155.84.74.29} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.29, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/10/15 ms

R20(tcl)#foreach CCIE 
>{155.84.74.22} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/25/29 ms

R20(tcl)#foreach CCIE 
>{155.84.74.18} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/30/69 ms

R20(tcl)#foreach CCIE 
>{155.84.74.1} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/30/69 ms

R20(tcl)#foreach CCIE 
>{192.168.50.5} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/23/34 ms

R20(tcl)#foreach CCIE 
>{194.35.252.7} { ping $CCIE re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 8/19/92 ms
Sending 10, 100-byte ICMP Echo to 75.6.224.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 7/13/23 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 60.99.98.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 17/25/70 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 6/12/26 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 124.13.240.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/10/14 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/25/30 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 86.13.117.119, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/20/22 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.38, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/26/32 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.30, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/25/30 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 63.69.0.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 24/31/39 ms
R20(tcl)#tclquit

webserven9#(tcl)#foreach ccie {
+>155.84.74.38
+>155.84.74.30
+>155.84.74.34
+>155.84.74.25
+>140.60.88.29
+>155.84.74.22
+>155.84.74.18
+>155.84.74.1
+>192.168.50.5
+>194.35.252.7
+>75.6.224.150
+>60.99.98.150
+>4.2.2.2
+>124.13.240.150
+>117.3.48.150
+>86.13.117.119
+>197.0.112.150
+>63.69.0.150
} { ping $ccie re 10 }

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echo to 155.84.74.38, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/18/31 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.30, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/21/51 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.25, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 19/23/35 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 140.60.88.29, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 26/37/81 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 140.60.88.29, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/27/36 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/5/12 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/5/9 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echo to 155.84.74.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/4/8 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 22/27/37 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 14/18/22 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 75.6.224.150, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 26/36/68 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 60.99.98.150, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 23/32/79 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 29/32/38 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 26/33/50 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/6/39 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 86.13.117.119, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 13/16/21 ms
Type escape sequence to abort.

SERVER4#tclsh
SERVER4(tcl)#foreach CCIE {
|>155.84.74.38
|>155.84.74.30
|>155.84.74.34
|>155.84.74.25
|>140.60.88.29
|>155.84.74.22
|>155.84.74.18
|>155.84.74.1
|>192.168.50.5
|>194.35.252.7
|>75.6.224.150
|>60.99.98.150
|>4.2.2.2
|>124.13.240.150
|>117.3.48.150
|>86.13.117.119
|>197.0.112.150
|>63.69.0.150
|>}
|}

Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 19/20/26 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/11/15 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/17/57 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/4/8 ms
Type escape sequence to abort.

Sending 10, 100-byte ICMP Echos to 140.60.88.29, timeout is 2 seconds: 
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 13/16/21 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 24/28/43 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/26/34 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/26/34 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 16/30/64 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 16/30/64 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 75.6.224.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 8/11/17 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 60.99.98.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/6 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/11/16 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/12/19 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 12/20/27 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 24/31/55 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 63.69.0.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 27/31/37 ms
SERVER4(tcl)#tclquit
SERVER4(tcl)#tclsh
SERVER4(tcl)#foreach CCIE {
>155.84.74.38
>155.84.74.30
>155.84.74.22
>155.84.74.18
>155.84.74.14
>155.84.74.10
>155.84.74.6
>155.84.74.2
>}
traceroute $CCIE probe 1

Tracing the route to 155.84.74.30
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 2 msec
2 192.168.110.16 6 msec
3 155.84.74.24 1 msec
4 66.171.14.2 10 msec
5 66.171.14.6 11 msec
6 155.84.74.30 26 msec

Tracing the route to 155.84.74.34
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.24 7 msec
4 66.171.14.2 14 msec
5 66.171.14.6 13 msec
6 66.171.14.14 12 msec
7 155.84.74.34 14 msec

Tracing the route to 140.60.88.29
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.24 7 msec
4 66.171.14.2 10 msec
5 66.171.14.6 14 msec
6 66.171.14.10 16 msec
7 140.60.88.29 18 msec

Tracing the route to 155.84.74.22
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.24 1 msec
4 66.171.14.2 107 msec
5 66.171.14.6 12 msec
6 86.191.16.10 20 msec
7 86.191.16.5 28 msec
8 86.191.16.1 35 msec
9 10.55.84.74.1 36 msec
10 192.168.10.22 27 msec
11 155.84.74.22 33 msec
12 155.84.74.22 39 msec

Tracing the route to 155.84.74.18
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.24 1 msec
4 66.171.14.2 14 msec
5 66.171.14.6 13 msec
6 66.171.14.10 11 msec
7 86.191.16.10 20 msec
8 86.191.16.5 28 msec
9 86.191.16.1 35 msec
10 155.84.74.1 24 msec
11 192.168.10.22 27 msec
12 155.84.74.18 33 msec
13 155.84.74.22 39 msec

Type escape sequence to abort.
Tracing the route to 155.84.74.1
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.26 3 msec
4 66.171.14.2 11 msec
5 66.171.14.6 6 msec
6 66.171.14.10 10 msec
7 86.191.16.10 20 msec
8 86.191.16.5 32 msec
9 86.191.16.1 26 msec
10 155.84.74.1 33 msec
Type escape sequence to abort.

Tracing the route to 192.168.50.5
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 3 msec
2 192.168.110.16 1 msec
3 155.84.74.26 1 msec
4 66.171.14.2 15 msec
5 66.171.14.6 9 msec
6 66.171.14.10 19 msec
7 86.191.16.10 29 msec
8 140.60.88.10 20 msec
9 140.60.88.45 [MPLS: Labels 22/42 Exp 0] 22 msec
10 192.168.50.5 29 msec
Type escape sequence to abort.

Tracing the route to 194.35.252.7
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.26 4 msec
4 66.171.14.2 15 msec
5 66.171.14.6 7 msec
6 66.171.14.14 34 msec
Type escape sequence to abort.

Tracing the route to 75.6.224.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 1 msec
2 192.168.110.16 1 msec
3 155.84.74.26 1 msec
4 66.171.14.2 12 msec
5 66.171.14.6 14 msec
Type escape sequence to abort.

Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 1 msec
2 192.168.110.16 1 msec
3 155.84.74.26 9 msec
4 66.171.14.2 11 msec
5 66.171.14.6 10 msec
6 66.171.14.10 12 msec
Type escape sequence to abort.

Tracing the route to 86.13.34.150
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 0 msec
2 192.168.110.16 1 msec
3 155.84.74.26 1 msec
4 66.171.14.2 10 msec
5 66.171.14.6 11 msec
6 66.171.14.10 12 msec
7 86.191.16.10 21 msec
8 86.191.16.5 28 msec
9 86.191.16.1 30 msec
10 155.84.74.1 31 msec
11 192.168.10.22 30 msec
12 155.84.74.14 25 msec
Type escape sequence to abort.

Tracing the route to 86.13.34.151
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.140.107 4 msec
2 192.168.110.16 2 msec
3 155.84.74.26 3 msec
4 66.171.14.2 10 msec
5 66.171.14.6 11 msec
6 66.171.14.10 12 msec
7 86.191.16.10 21 msec
8 86.191.16.5 28 msec
9 86.191.16.1 30 msec
10 155.84.74.1 31 msec
11 192.168.10.22 30 msec
12 155.84.74.14 25 msec
Type escape sequence to abort.
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/18/31 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/24/32 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 140.60.88.29, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 9/10/16 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/24/32 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/26/41 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/28/56 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 2/6/18 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 20/22/28 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/16/27 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/14/24 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/30/65 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 86.13.117.119, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 3/4/8 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 3/33/124 ms
PC4(tcl)#tclquit

R12#tclsh
R12(tcl)#foreach CCIE {
    }155.84.74.38,
    }155.84.74.34,
    }155.84.74.25,
    }140.60.88.29,
    }155.84.74.22,
    }155.84.74.18,
    }155.84.74.1,
    }192.168.50.5,
    }194.35.252.7,
    }75.6.224.150,
    }60.99.98.150,
    }4.2.2.2,
    }124.13.240.150,
    }117.3.48.150,
    }86.13.117.119,
    }197.0.112.150,
    }63.69.0.150,
    } | ping CCIE ou loo 1 re 10 }
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 24/29/34 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 13/19/39 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 11/14/20 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 23/26/31 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 140.60.88.29, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 23/27/49 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/6 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 152.168.21.12
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/11 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.21.50, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 23/26/35 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 14/17/22 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 75.6.224.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 28/33/41 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 60.99.98.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 24/31/46 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 29/34/42 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 26/30/39 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 4/6/14 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 86.13.117.119, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 17/20/25 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/8 ms
Sending 10, 100-byte ICMP Echoes to 63.69.0.150, timeout is 2 seconds:
Packet sent with a source address of 192.168.21.12
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/11/16 ms
R12(tcl)#tclquit

R21#tclsh
R21(tcl)#foreach CCIE {
   +>155.84.74.38
   +>155.84.74.30
   +>155.84.74.34
   +>155.84.74.25
   +>140.60.88.29
   +>155.84.74.22
   +>155.84.74.18
   +>155.84.74.1
   +>192.168.50.5
   +>194.35.252.7
   +>75.6.224.150
   +>60.99.98.150
   +>4.2.2.2
   +>124.13.240.150
   +>117.3.48.150
   +>96.13.137.119
   +>197.0.112.150
   +>63.69.0.150
} { ping $CCIE re 10 }

Sending 10, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 21/32/76 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.30, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 12/16/25 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.34, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/15/24 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 19/22/26 ms

Sending 10, 100-byte ICMP Echos to 140.60.88.29, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 7/9/13 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.22, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 20/25/32 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.18, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/28/65 ms

Sending 10, 100-byte ICMP Echos to 155.84.74.1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 19/23/29 ms

Sending 10, 100-byte ICMP Echos to 192.168.50.5, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/4 ms

Sending 10, 100-byte ICMP Echos to 194.35.252.7, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/17/30 ms

Sending 10, 100-byte ICMP Echos to 75.6.224.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/13/20 ms

Sending 10, 100-byte ICMP Echos to 60.99.98.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 13/23/34 ms

Sending 10, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 11/13/15 ms

Sending 10, 100-byte ICMP Echos to 124.13.240.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/12/19 ms
Sending 10, 100-byte ICMP Echos to 117.3.48.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 20/29/50 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 86.13.117.119, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 3/7/15 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 197.0.112.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 17/22/30 ms
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 63.69.0.150, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 10/13/24 ms
R21(tcl)#tclquit

Note: Please remove Tunnel 10 and Tunnel 20 interfaces from R19 and R20 to bring down DMVPN tunnel

R19 / R20
no interface tunnel 10
no int tunnel 20

Note: Please ensure R19 and R16 using EIGRP named mode with a name of your choice. R20 should already be using EIGRP 64bit mode configured in one of the previous sections

R19 / R16
router eigrp 250
eigrp upgrade-cli

Note: Based on the BGP section R16 R19 R20 should be able to reach eachother external interfaces of R19 but not be able to reach eachother LAN subnets for instance – Server#3 Server#4 and PC#3

R19#ping 155.84.74.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/20/23 ms
R20#ping 155.84.74.25
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.25, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/20/24 ms
R16#ping 155.84.74.38
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.38, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/19/20 ms
R16#ping 155.84.74.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.41, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/23/43 ms
PC3#ping 192.168.140.100 re 5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SERVER3#ping 192.168.160.100 re 5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CCIEv5 Routing & Switching
Advanced Configuration & Troubleshooting Lab#2
EIGRP OTP

Tom Mark Giembicki
Sean Draper
**Note: EIGRP OTP**

EIGRP Over the Top allows the customer to establish EIGRP adjacencies across the MPLS/VPN provider cloud. An EIGRP targeted adjacency between CEs is created. This EIGRP neighborship is done via unicast packets, using the CE 'WAN' IP address. This "over the top" peering allows EIGRP to exchange customer prefixes directly between CEs. Customer prefixes are NOT injected in the providers VRF routing table.

**Control Plane**

OTP control plane consists in an EIGRP targeted adjacency between CEs. Neighborship is established using the CE WAN address, i.e. address of CE on the PE/CE link, so there is no need for any dynamic routing protocol between the PE/CE. The PE just needs to redistribute the connected routes.

This adjacency is using unicast packets and the CE needs to know the IP of the remote CE. In the first phase of OTP, only static neighbors are allowed. With manual neighbor configuration, it wouldn’t scale to establish full mesh peering between all CEs. Instead, the concept of Route Reflector, i.e. CEs peer with RRs only is used and RRs reflect the routes they receive to other CEs. Each CE is configured with the RRs WAN address and each RR is configured in EIGRP promiscuous mode, i.e. to accept incoming 'connections' (similar to BGP listen feature).

*directly from Cisco website*
Note: EIGRP OTP

Data Plane
Since the customer prefixes are not known in the VRF of provider, customer traffic can't be natively forwarded through the provider cloud, but needs to be encapsulated by CEs before being sent through the provider cloud.
OTP leverages existing LISP encapsulation which:

- Allows dynamic multi-point tunneling
- Provides instance ID field to optionally support virtualization across WAN (see EVN WAN Extension section)

OTP does NOT use LISP control plane (map server/resolver, etc.) instead it uses EIGRP to exchange routes and provide the next-hop, which LISP encapsulation uses to reach remote prefixes.

MTU and Fragmentation Issues
Since OTP adds an extra header (36 bytes), it needs to deal with potential MTU/fragmentation issues. The DF bit is always set in LISP encapsulation. This is to prohibit the re-assembly operation on the egress CE. The idea here is to force fragmentation before encapsulation, so re-assembly is done by end-users. For the ingress CE to be able to perform fragmentation before encapsulation, it needs to know the max MTU that can go through the provider cloud with OTP encapsulation.
This is hopefully done automatically if the MTU of the WAN interface is supported end to end across the provider cloud. If this is not the case (i.e. there are lower MTU links within the provider cloud), change manually the IP MTU of the WAN interface to match the lowest MTU within the provider cloud. Otherwise, the PMTUD is broken for end-users and this may lead to connectivity issues over OTP.

Note: Check the calculated max mtu by looking at the CEF adjacencies on the LISP interface.

In the case below, the WAN-intf gets 1500 MTU, so L3 mtu = 1464 (1500 - 36):

```
CE#show adjacency lisp 0 int | i mtu
L3 mtu 1464
mtu update from interface suppressed
```

Note: EIGRP OTP cont.
The EIGRP Over the Top feature enables a single end-to-end Enhanced Interior Gateway Routing Protocol (EIGRP) routing domain that is transparent to the underlying public or private WAN transport that is used for connecting disparate EIGRP customer sites. When an enterprise extends its connectivity across multiple sites through a private or a public WAN connection, the service provider mandates that the enterprise use an additional routing protocol, typically the Border Gateway Protocol (BGP), over the WAN links to ensure end-to-end routing. The use of an additional protocol causes additional complexities for the enterprise, such as additional routing processes and sustained interaction between EIGRP and the routing protocol to ensure connectivity, for the enterprise. With the EIGRP Over the Top feature, routing is consolidated into a single protocol (EIGRP) across the WAN. Perform this task to configure a customer edge (CE) device in a network to function as an EIGRP Route Reflector:

```
enable
configure terminal
router eigrp virtual-name
  address-family ipv4 unicast autonomous-system as-number
  af-interface interface-type interface-number
  no next-hop-self
  no split-horizon
  exit
remote-neighbors source interface-type interface-number unicast-listen lisp-encap
  network ip-address
  end

Note: Use no next-hop-self to instructs EIGRP to use the received next hop and not the local outbound interface address as the next hop to be advertised to neighboring devices. If no next-hop-self is not configured, the data traffic will flow through the EIGRP Route Reflector.
```

*directly from Cisco website – Reference EIGRP Over the Top*
LAB#2

EIGRP Over The Top (OTP)

Configure EIGRP (OTP) using LISP encapsulation between R16, R19, and R20 using EIGRP AS 250. R19 and R20 should act as spoke routers with R16 acting as a route reflector hub. Routers should not accept connection from each other if they are more than 10 hops away. Locator/ID Separation Protocol should be set to a value of 1. Ensure all remote LAN subnets are able to communicate with each other.

**Configuration:**

**R16**

```plaintext
router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
  af-interface Ethernet0/0
    no next-hop-self
    no split-horizon
    exit-af-interface
    topology base
  exit-af-topology
    remote-neighbors source Ethernet0/0 unicast-listen lisp-encap
    network 155.84.74.25 0.0.0.0
  exit-address-family
```

**R19**

```plaintext
router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
  topology base
  exit-af-topology
    neighbor 155.84.74.25 Multilink1 remote 10 lisp-encap 1
    network 155.84.74.38 0.0.0.0
  exit-address-family
```

**R20**

```plaintext
router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
  topology base
  exit-af-topology
    neighbor 155.84.74.25 Serial1/0 remote 10 lisp-encap 1
    network 155.84.74.41 0.0.0.0
  exit-address-family
```

**Verification:**

```plaintext
R19#sh eigrp address-family ipv4 neighbors detail
EIGRP-Ipv4 VR(SBRO) Address-Family Neighbors for AS(250)
H Address Interface Hold Uptime SRTT RTO Q Seq
( sec) (ms) Cnt Num
0 155.84.74.25 Mul 14 00:03:15 548 3288 0 145
Remote Static neighbor (static multihop) (LISP Encap)
Version 14.0/2.0, Retrans: 0, Retries: 0, Prefixes: 33
Topology-ids from peer - 0
```

```plaintext
R16#sh eigrp address-family ipv4 neighbors detail
EIGRP-Ipv4 VR(SBRO) Address-Family Neighbors for AS(250)
H Address Interface Hold Uptime SRTT RTO Q Seq
( sec) (ms) Cnt Num
5 155.84.74.38 Et0/0 12 00:05:52 51 306 0 25
```
Remote neighbor (unicast-listen) (LISP Encap)
Version 14.0/2.0, Retrans: 5, Retries: 0, Prefixes: 12
Topology-ids from peer – 0

4 155.84.74.41  Et0/0 14 00:05:52 53 318 0 40

Remote neighbor (unicast-listen) (LISP Encap)
Version 14.0/2.0, Retrans: 5, Retries: 0, Prefixes: 17
Topology-ids from peer – 0

3 192.168.110.18 Et2/0 13 01:24:13 5 100 0 64

Version 14.0/2.0, Retrans: 0, Retries: 0, Prefixes: 17
Topology-ids from peer – 0

2 192.168.110.107 Et2/0 11 01:24:13 2 100 0 65

Version 7.0/3.0, Retrans: 0, Retries: 0, Prefixes: 3
Topology-ids from peer – 0

1 192.168.100.106 Et1/0 13 01:24:13 6 100 0 68

Version 7.0/3.0, Retrans: 0, Retries: 0, Prefixes: 2
Topology-ids from peer – 0

0 192.168.100.17 Et1/0 12 01:24:13 7 100 0 72

Version 14.0/2.0, Retrans: 0, Retries: 0, Prefixes: 4
Topology-ids from peer – 0

Note: Hmm… On R19 and R20 R16 Hub show as ‘incomplete’ LISP adjacency with the ‘drop’ as the next chain element towards out hub R16?

R19#sh adjacency lisp 1 detail
Protocol Interface Address
IP LISP1
IP 155.84.74.25(25) (incomplete)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 12
drop packets
LISP
Next chain element: drop

IP 155.84.74.41(22)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 12
Encap length 36
4500000000004000FF11B0F49B544A26
9B544A29000010F7000000080D62A13
00000000
LISP
Next chain element: IP adj out of Multilink

R20#sh adjacency lisp 1 detail
Protocol Interface Address
IP LISP1
IP 155.84.74.25(25) (incomplete)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 16
drop packets
LISP
Next chain element: drop

IP 155.84.74.38(17)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 16
Encap length 36
4500000000004000FF11B0F49B544A29
9B544A26000010F7000000080D66C26B
00000000
LISP
Next chain element:
**Note:** but the R16 Hub itself seems fine?

```
IP adj out of Serial1/0

R16#sh adjacency lisp 1 detail
Protocol Interface  Address
IP    LISP1                      155.84.74.38(17)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 5
Encap length 36
450000000004000FF11B1049B544A19
9B544A26000010F70000000080D3E40C
00000000
LISP
Next chain element:
IP adj out of Ethernet0/0, addr 155.84.74.26
  155.84.74.41(22)
  1 packets, 176 bytes
  epoch 0
  sourced in sev-epoch 5
  Encap length 36
  450000000004000FF11B1049B544A19
  9B544A29000010F70000000080CF4477
  00000000
LISP
Next chain element:
```

**Note:** Let's check our reachability between the spoke sites first:

```
SERVER3#ping 192.168.160.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/19/21 ms

PC3#ping 192.168.150.147
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.147, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/20/22 ms
```

**Note:** And now with the Server#4 - R16 LAN:

```
SERVER3#ping 192.168.140.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

PC3#ping 192.168.140.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```
Note: Looks like none of the spoke sites is able to reach LAN segment behind R16?

R19#sh adjacency lisp 1 link ipv4
Protocol Interface Address
IP LISP1 155.84.74.25(25) (incomplete)
IP LISP1 155.84.74.41(22)

R19#sh adjacency lisp 1 encapsulation
Protocol Interface Address
IP LISP1 155.84.74.25(25) (incomplete)

adjacency is incomplete
IP LISP1 155.84.74.41(22)
Encap length 36
45000000000000000000FF11B0F49B544A26
9B544A290000010F70000000080D62A13
00000000
Provider: LISP
Protocol header count in encaps string: 3
Header no #0: ipv4
Fields with variable content: tos, ttl, ident, tl, chksm
tos : per packet, copy from payload
ttl : per packet, default
ident : per packet, default
df : static 1
tl : per packet, copy from payload
protocol : static 17
chksm : per packet, default
src : static 155.84.74.38
dst : static 155.84.74.41
Header no #1: udp
Fields with variable content: source port, length
Protocol Interface Address
source port : hash of payload, 3-tuple (src, dst, protocol)
destination port : static 4343
length : per packet, default
checksum : static 0
Header no #2: lisp
Fields with variable content: none
nonce present : static 1
LSB enabled : static 0
echo nonce request : static 0
map-versions present : static 0
instance ID present : static 0
reserved flags : static 0x0
nonce : static 0xD62A13
source map-version : N/A
destination map-version : N/A
instance ID : N/A
locator status : N/A

Note: Let's do some troubleshooting

SERVER3#traceroute 192.168.140.100
Type escape sequence to abort.
Tracing the route to 192.168.140.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.150.19 27 msec 5 msec 6 msec
2 * * *
3 *
Note: Now let’s see what is the reason behind 155.84.74.25/24 (incomplete) on both of our hubs and we will focus on R19.
**Note:** That’s a good sign, we are learning EIGRP prefixes including VLAN50 subnet 192.168.140.0/24 where Server#4 resides on and we can see our problem, we’ve got a routing issue inside of R19 CEF table where we are trying to get to the remote end of the Tunnel via the Tunnel itself (similar to GRE), we’ll also check R20

R19#sh ip cef 155.84.74.25 155.84.74.25/32
  nexthop 155.84.74.25 LISP1
R19#sh ip cef 192.168.140.100 192.168.140.0/24
  nexthop 155.84.74.25 LISP1
R20#sh ip cef 155.84.74.25 155.84.74.25/32
  nexthop 155.84.74.25 LISP1
R20#sh ip cef 192.168.140.100 192.168.140.0/24
  nexthop 155.84.74.25 LISP1

**Note:** What about spoke to spoke communication?

R19#sh ip cef 155.84.74.41 155.84.74.41/32
  nexthop 155.84.74.37 Multilink1
R19#sh ip cef 192.168.160.100 192.168.160.0/24
  nexthop 155.84.74.41 LISP1
R20#sh ip cef 155.84.74.38 155.84.74.38/32
  nexthop 155.84.74.42 Serial1/0
R20#sh ip cef 192.168.150.147 192.168.150.0/24
  nexthop 155.84.74.38 LISP1

**Note:** We will apply the following configuration on both spokes, this way blocking the RR prefix from reaching EIGRP RIB

**R19**

```
ip prefix-list PFL seq 5 deny 155.84.74.24/30
ip prefix-list PFL seq 10 permit 0.0.0.0/0 le 32
```

```
router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
topology base
distribute-list prefix PFL in
exit-af-topology
exit-address-family
```
R20
ip prefix-list PFL seq 5 deny 155.84.74.24/30
ip prefix-list PFL seq 10 permit 0.0.0.0/0 le 32

router eigrp SBRO
  address-family ipv4 unicast autonomous-system 250
topology base
distribute-list prefix PFL in
  exit-af-topology
  exit-address-family

**Note:** Another reachability test and all looks good!

SERVER3#ping 192.168.140.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/22 ms

SERVER3#ping 192.168.150.147
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.147, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

PC3#ping 192.168.140.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.140.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/23/37 ms

PC3#ping 192.168.150.147
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.150.147, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 15/23/41 ms

R19#sh ip cef 155.84.74.25
155.84.74.25/32
  nexthop 155.84.74.37 Multilink1

R19#sh ip cef 192.168.140.100
192.168.140.0/24
  nexthop 155.84.74.25 LISPl

R20#sh ip cef 155.84.74.25
155.84.74.25/32
  nexthop 155.84.74.42 Serial1/0

R20#sh ip cef 192.168.140.100
192.168.140.0/24
  nexthop 155.84.74.25 LISPl

**Note:** Please remove configuration from all devices and apply initial configs.
CCIEv5 Routing & Switching
Advanced Configuration & Troubleshooting Lab#3
LAYER 2

Tom Mark Giembicki

Sean Draper
CCIEv5 R&S L2/L3 Topology

Service Provider #9
BGP AS 5934

Service Provider #6
BGP AS 10001

Berlin HQ
Home User

OSPF Area 0
172.31.10/30
Lo0:172.100.X.X/32

EIGRP 200
192.168.50.0/24
Lo0:192.X.X.X/32

Copyright © 2015 CCIE4ALL. All rights reserved
LAB#3

MPLS CORE – Service Provider 9

VLAN TRUNK VTP

Interfaces connecting to other switches should be configured as dot1q trunk interfaces with a native VLAN 11.

All switches should be configured as VTP Version 3 with the following requirements:

- SW5 is the primary switch for the VLAN database
- SW3 and SW4 should be configured as VTP clients
- Domain name should be set to V5

All switches should have a ‘hidden’ password of CCIE-V5

Configuration:

**SW5**

```
vlan 11
name NATIVE

vtp domain V5
vtp version 3
vtp password CCIE-V5 hidden
vtp primary vlan (exec mode configuration)

This system is becoming primary server for feature vlan
Enter VTP Password:CCIE-V5
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
SW5#

interface range Ethernet0/0 - 2, Ethernet1/0 - 2
switchport trunk encapsulation dot1q
switchport trunk native vlan 11
switchport mode trunk
```

**SW3**

```
vtp domain V5
vtp version 3
vtp password CCIE-V5 hidden
vtp mode client

interface range Ethernet0/0 - 2, Ethernet1/0 - 2
switchport trunk encapsulation dot1q
switchport trunk native vlan 11
switchport mode trunk
```

**SW4**

```
vtp domain V5
vtp version 3
vtp password CCIE-V5 hidden
vtp mode client

interface range Ethernet0/0 - 2, Ethernet1/0 - 2
switchport trunk encapsulation dot1q
switchport trunk native vlan 11
switchport mode trunk
```
### Verification:

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
<tr>
<td>Et0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
<tr>
<td>Et0/2</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
<tr>
<td>Et1/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
<tr>
<td>Et1/2</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>11</td>
</tr>
</tbody>
</table>

### Note:

*Use the interface Switchport command to look at more detail at the Switchport including trunk and native VLAN*

```
SW3#show interfaces ethernet 0/1 switch
Name: Et0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 11 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Appliance trust: none
```

**Note:** Creating VTP Primary Vlan in order for other switches to learn about the primary server over the trunk interfaces
SW5#vtp primary vlan
This system is becoming primary server for feature vlan
Enter VTP Password:
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
SW5#

*Jan 3 11:28:19.706: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.3700 has become the primary server for the VLAN VTP feature

SW4(config)#
%SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.3700 has become the primary server for the VLAN VTP feature

SW3(config)#
%SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.3700 has become the primary server for the VLAN VTP feature

SW3#sh vlan id 11
VLAN Name                             Status    Ports
---- ---------------------------------- ----------------------------
11   NATIVE active Et0/0, Et0/1, Et0/2, Et1/0
     - Et1/1, Et1/2, Et1/3, Et2/2
     - Et3/1
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
--- ---- ---------- ----- --------- -------- ------- -------- ------- ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ ------ -------
Note: You can set the VTP password in exec and global configuration. To configure the hidden password you must do it from global configuration mode. By entering the hidden keyword it ensures that the secret key generated from the password string is saved in the nvram: vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password.

To clear the password use the ‘no vtp password’ command in global configuration.

```
SW3#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : V5
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3500
Feature VLAN:

----------------------
VTP Operating Mode : Client
Number of existing VLANs : 30
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 3
Primary ID : aabb.cc00.3700
Primary Description : SW5
MD5 digest : 0x92 0x97 0x5C 0xA3 0xB6 0xE0 0x28 0xF6
0x2F 0x60 0xB2 0x12 0x67 0xB0 0x59 0xB1

Feature MST:

----------------------
VTP Operating Mode : Transparent
Feature UNKNOWN:

----------------------
VTP Operating Mode : Transparent
```

```
SW4#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : V5
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3600
Feature VLAN:

----------------------
VTP Operating Mode : Client
Number of existing VLANs : 30
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 3
Primary ID : aabb.cc00.3700
Primary Description : SW5
MD5 digest : 0x92 0x97 0x5C 0xA3 0xB6 0xE0 0x28 0xF6
0x2F 0x60 0xB2 0x12 0x67 0xB0 0x59 0xB1

Feature MST:

----------------------
VTP Operating Mode : Transparent
Feature UNKNOWN:

----------------------
VTP Operating Mode : Transparent
```
SW5# show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : V5
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3700
Feature VLAN:
--------------
VTP Operating Mode : Primary Server
Number of existing VLANs : 30
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 3
Primary ID : aabb.cc00.3700
Primary Description : SW5
MD5 digest : 0x92 0x97 0x5C 0xA3 0xB6 0xE0 0x28 0xF6
0x2F 0x60 0xB2 0x12 0x67 0xB0 0x59 0xB1
Feature MST:
--------------
VTP Operating Mode : Transparent
Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent

Note: Lastly we will check for neighbouring VTP devices within our VTP domain

SW3# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
----------------- ------------- ------------------- -------------------------
VLAN No 5 aabb.cc00.3700 aabb.cc00.3600 SW4
VLAN No 5 aabb.cc00.3700=aabb.cc00.3700 SW5

SW4# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
----------------- ------------- ------------------- -------------------------
VLAN No 5 aabb.cc00.3700 aabb.cc00.3500 SW3
VLAN No 5 aabb.cc00.3700=aabb.cc00.3700 SW5

SW5# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
----------------- ------------- ------------------- -------------------------
VLAN No 5 aabb.cc00.3700 aabb.cc00.3500 SW3
VLAN No 5 aabb.cc00.3700 aabb.cc00.3600 SW4
ETHERCHANNEL

Configure Cisco-proprietary etherchannel as per the following:

- SW3-SW5 – SW3 should actively initiate. Use group number 35
- SW4-SW5 – SW5 should actively initiate. Use group number 45
- SW3-SW4 – SW4 should passively negotiate. Use number 34. SW3 should only start negotiation once data packets have been received

**Configuration:**

**SW5**

interface range Ethernet0/0 - 2
channel-group 35 mode auto

interface range Ethernet1/0 - 2
channel-group 45 mode desirable

**SW3**

interface range Ethernet0/0 - 2
channel-group 34 mode desirable non-silent

interface range Ethernet1/0 - 2
channel-group 35 mode desirable

**SW4**

interface range Ethernet0/0 - 2
channel-group 34 mode auto

interface range Ethernet1/0 - 2
channel-group 45 mode auto

**Verification:**

SW3#deb etherchannel event
PAGP/LACP Shim Events debugging is on
SW3#config t
SW3(config)#int ran po 34 , po 35
SW3(config-if-range)#sh
SW3(config-if-range)#no sh
FEC: pagp_switch_port_up: Et0/0
FEC: pagp_switch_invoke_port_up: Et0/0
FEC: pagp_switch_port_up: Et0/1
FEC: pagp_switch_invoke_port_up: Et0/1
FEC: pagp_switch_port_up: Et0/2
FEC: pagp_switch_invoke_port_up: Et0/2
FEC: pagp_switch_port_up: Et1/0
FEC: pagp_switch_invoke_port_up: Et1/0
FEC: pagp_switch_port_up: Et1/1
FEC: pagp_switch_invoke_port_up: Et1/1
FEC: pagp_switch_port_up: Et1/2
FEC: pagp_switch_invoke_port_up: Et1/2
FEC: fec_bundle: Et0/1
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 1 [Et0/1]
FEC: fec_bundle: Et1/1
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 1 [Et1/1]
FEC: fec_bundle: Et0/0
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 2 [Et0/0]
FEC: fec.bundle: Et1/2
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 2 [Et1/2]
FEC: fec.bundle: Et1/0
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 3 [Et1/0]
FEC: fec.bundle: Et0/2
FEC: pagp_switch_add_port_to_agport_list: afb->nports++ = 3 [Et0/2]

Note: We will now check SW3 both port-channels 34 and 35

SW3#sh etherc summ | be Group
Group Port-channel Protocol Ports
34 Po34 (SU) PAgP Et0/0 (P) Et0/1 (P) Et0/2 (P)
35 Po35 (SU) PAgP Et1/0 (P) Et1/1 (P) Et1/2 (P)

SW3#sh etherchannel 34 detail
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: PAgP
Minimum Links: 0

Port: Et0/0
---
Port state = Up Mstr In-Bndl
Channel group = 34 Mode = Desirable, NonSl Gcchange = 0
Port-channel = Po34 GC = 002220001 Pseudo port-channel = Po34
Port index = 0 Load = 0x00 Protocol = PAgP
Flags: S - Device is sending slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.

Local information:
<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>IIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>19</td>
</tr>
</tbody>
</table>

Partner's information:
<table>
<thead>
<tr>
<th>Partner</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW4</td>
<td>aabb.cc00.3600</td>
<td>Et0/0</td>
<td>14s</td>
<td>SAC</td>
<td>220001</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:03m:28s

Port: Et0/1
---
Port state = Up Mstr In-Bndl
Channel group = 34 Mode = Desirable, NonSl Gcchange = 0
Port-channel = Po34 GC = 002220001 Pseudo port-channel = Po34
Port index = 0 Load = 0x00 Protocol = PAgP
Flags: S - Device is sending slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.
Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/1</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>19</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/1</td>
<td>SW4</td>
<td>aabb.cc00.3600</td>
<td>Et0/1</td>
<td>11s</td>
<td>SAC</td>
<td>220001</td>
</tr>
</tbody>
</table>

Age of the port in the current state: *0d:00h:03m:28s*

**Port: Et0/2**

---

**Port state** = Up Mstr In-Bndl

**Channel group** = 34

**Port-channel** = Po34

**Port index** = 0

**Load** = 0x00

**Protocol** = PAgP

**Flags:**  
- S - Device is sending Slow hello.  
- C - Device is in Consistent state.  
- A - Device is in Auto mode.  
- P - Device learns on physical port.  
- d - PAgP is down.

**Timers:**  
- H - Hello timer is running.  
- Q - Quit timer is running.  
- S - Switching timer is running.  
- I - Interface timer is running.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/2</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>19</td>
</tr>
</tbody>
</table>

Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/2</td>
<td>SW4</td>
<td>aabb.cc00.3600</td>
<td>Et0/2</td>
<td>18s</td>
<td>SAC</td>
<td>220001</td>
</tr>
</tbody>
</table>

Age of the port in the current state: *0d:00h:03m:28s*

**Port-channels in the group:**

---

**Age of the Port-channel** = *0d:00h:06m:24s*

**Logical slot/port** = 16/1

**GC** = 0x00220001

**HotStandBy port** = null

**Port state** = Port-channel Ag-Inuse

**Protocol** = PAgP

**Port security** = Disabled

**Ports in the Port-channel:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Et0/0</td>
<td>Desirable-NonSl</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Et0/1</td>
<td>Desirable-NonSl</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Et0/2</td>
<td>Desirable-NonSl</td>
<td>0</td>
</tr>
</tbody>
</table>

Time since last port bundled: *0d:00h:03m:28s*  
Time since last port Un-bundled: *0d:00h:04m:39s*
SW3#sh etherchannel 35 detail
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: PAgP
Minimum Links: 0

Ports in the group:

---

**Port: Et1/0**

---

Port state = Up Mstr In-Bndl
Channel group = 35 **Mode = Desirable-Sl** Gcchange = 0
Port-channel = Po35 GC = 0x00230001 Pseudo port-channel = Po35
Port index = 0 Load = 0x00 Protocol = PAgP
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>20</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:05m:01s

**Port: Et1/1**

---

Port state = Up Mstr In-Bndl
Channel group = 35 **Mode = Desirable-Sl** Gcchange = 0
Port-channel = Po35 GC = 0x00230001 Pseudo port-channel = Po35
Port index = 0 Load = 0x00 Protocol = PAgP
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>20</td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:05m:01s

**Port: Et1/2**

---

Port state = Up Mstr In-Bndl
Channel group = 35 **Mode = Desirable-Sl** Gcchange = 0
Port-channel = Po35 GC = 0x00230001 Pseudo port-channel = Po35
Port index = 0 Load = 0x00 Protocol = PAgP
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
A - Device is in Auto mode. P - Device learns on physical port.
d - PAgP is down.
Timers: H - Hello timer is running. Q - Quit timer is running.
S - Switching timer is running. I - Interface timer is running.

Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Count</th>
<th>Priority</th>
<th>Method</th>
<th>Ifindex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1</td>
<td>128</td>
<td>Any</td>
<td>20</td>
</tr>
</tbody>
</table>
Partner's information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Device ID</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/2</td>
<td>SW5</td>
<td>aabb.cc00.3700</td>
<td>Et0/2</td>
<td>20s SAC</td>
<td>230001</td>
<td></td>
</tr>
</tbody>
</table>

Age of the port in the current state: 0d:00h:05m:01s

Port-channels in the group:

Port-channel: Po35

Age of the Port-channel = 0d:00h:07m:48s
Logical slot/port = 16/2  Number of ports = 3
GC = 0x00230001  HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = PAgP
Port security = Disabled

Ports in the Port-channel:

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/0</td>
<td>Desirable-Sl</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/1</td>
<td>Desirable-Sl</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Et1/2</td>
<td>Desirable-Sl</td>
<td>0</td>
</tr>
</tbody>
</table>

Time since last port bundled: 0d:00h:05m:01s  Et1/0
Time since last port Un-bundled: 0d:00h:06m:07s  Et1/2
SPANNING TREE

Configure the switches as per the following:

- All switches should run rapid convergence based on the IEEE 802.1w standard on a per-vlan basis
- SW3 should be the Root Bridge
- SW4 should be the backup Root Bridge
- This should be manually set for all possible VLAN range
- SW5 should use Po45 as its root port for VLAN 12 only. Changes can only be made SW5
- All switches should have a point to point link type

**Configuration:**

**SW5**

spanning-tree mode rapid-pvst

int port35
spanning-tree vlan 12 cost 95

**SW3**

spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 priority 0

**SW4**

spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 root secondary

**Verification:**

```
SW5#sh spanning-tree | in VLAN|Po
VLAN0001
   Port   514 (Port-channel35)
   Po35: Root FWD 47 128.514 Shr
   Po45:  Altn BLK 47 128.515 Shr
VLAN0011
   Port   514 (Port-channel35)
   Po35: Root FWD 47 128.514 Shr
   Po45:  Altn BLK 47 128.515 Shr
   VLAN0012
   Port   514 (Port-channel35)
   Po35: Root FWD 47 128.514 Shr
   Po45:  Altn BLK 47 128.515 Shr
   VLAN0013
   Port   514 (Port-channel35)
   Po35: Root FWD 47 128.514 Shr
   Po45:  Altn BLK 47 128.515 Shr
   VLAN0014
   Port   514 (Port-channel35)
   Po35: Root FWD 47 128.514 Shr
   Po45:  Altn BLK 47 128.515 Shr
<Output omitted>
```
**Note:** SW5 is choosing the path directly to SW3 for all local VLANs based on the lower cost to the root bridge.

SW5#sh spanning-tree vlan 12 detail

VLAN0012 is executing the rstp compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 12, address aabb.cc00.3700
Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
Current root has priority 12, address aabb.cc00.3500

**Root port is 514 (Port-channel35), cost of root path is 47**
Topoogy change flag not set, detected flag not set
Number of topology changes 8 last change occurred 00:04:27 ago
from Port-channel35
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 514 *(Port-channel35) of VLAN0012 is root forwarding*
- Port path cost 47, Port priority 128, Port Identifier 128.514.
- Designated root has priority 12, address aabb.cc00.3500
- Designated bridge has priority 12, address aabb.cc00.3500
- Designated port id is 128.515, **designated path cost 0**
- Timers: message age 15, forward delay 0, hold 0
- Number of transitions to forwarding state: 1
- Link type is shared by default
- BPDU: sent 37, received 172

Port 515 *(Port-channel45) of VLAN0012 is alternate blocking*
- Port path cost 47, Port priority 128, Port Identifier 128.515.
- Designated root has priority 12, address aabb.cc00.3500
- Designated bridge has priority 28684, address aabb.cc00.3600
- Designated port id is 128.515, **designated path cost 47**
- Timers: message age 16, forward delay 0, hold 0
- Number of transitions to forwarding state: 1
- Link type is shared by default
- BPDU: sent 3, received 173

**Note:** The total path cost via SW4 is 47 (local link cost) + 47 (cost to the Root Bridge) = 94. We will now change the path cost on SW5 (Po35) so that the cost is now 95

SW5
```
  int port35
  spanning-tree vlan 12 cost 95
```
SW5#sh spanning-tree vlan 12

VLAN0012
Spanning tree enabled
protocol rstp

Root ID    Priority    12
Address     aabb.cc00.3500
Cost        94
Port        515 (Port-channel45)
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID    Priority    32780  (priority 32768 sys-id-ext 12)
Address     aabb.cc00.3700
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  300 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ----- -------- ---------- --------------
Et1/3       Desg FWD 100 128.36   Shr
Et2/0       Desg FWD 100 128.65   Shr
Et2/1       Desg FWD 100 128.66   Shr
Et2/3       Desg FWD 100 128.68   Shr
Po35        Altn BLK 95  128.514  Shr
Po45        Root FWD 47  128.515  Shr

SW5#sh spanning-tree vl 12 detail
VLAN0012 is executing the rstp compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 12, address aabb.cc00.3700
Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
Current root has priority 12, address aabb.cc00.3500

Root port is 515 (Port-channel45), cost of root path is 94
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 00:01:43 ago from Port-channel45
Times:  hold 1, topology change 35, notification 2
        hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

<Output omitted>

Port 514 (Port-channel35) of VLAN0012 is alternate blocking
Path port cost 95. Port priority 128, Port Identifier 128.514.
Designated root has priority 12, address aabb.cc00.3500
Designated bridge has priority 12, address aabb.cc00.3500
Designated port id is 128.515, designated path cost 0
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is shared by default
BPDU: sent 37, received 384

Port 515 (Port-channel45) of VLAN0012 is root forwarding
Path port cost 47. Port priority 128, Port Identifier 128.515.
Designated root has priority 12, address aabb.cc00.3500
Designated bridge has priority 28684, address aabb.cc00.3600
Designated port id is 128.515, designated path cost 47
Timers: message age 15, forward delay 0, hold 0
Number of transitions to forwarding state: 2
Link type is shared by default
BPDU: sent 22, received 384

Note: SW5 is now choosing PO45 as its root port only for VLAN12
| VLAN0001 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0011 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0012 | Port | 515 (Port-channel45) | Po35 | Altn BLK 95 | 128.514 | Shr | Po45 | Root FWD 47 | 128.515 | Shr |
| VLAN0013 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0014 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0015 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0016 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0017 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0023 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0024 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0035 | Port | 514 (Port-channel35) | Po35 | Root FWD 47 | 128.514 | Shr | Po45 | Altn BLK 47 | 128.515 | Shr |
| VLAN0046 | Port | 514 (Port-channel35) | <Output omitted> |
San Francisco Group HQ

VLAN TRUNK VTP

Interfaces connecting to other switches should be configured as dot1q trunk interfaces.
All switches should be configured as VTP Version 2 with the following requirements:

- SW1 is the Server
- SW2 is the Client
- Domain name should be set to SFHQ
- Authenticated with a password of "SanFranHQ?" (including question mark without the quotes)
- VTP pruning enabled
- VLAN 100 with a name of CCIE-PRUNED-VLAN. This should be pruned off the links between the switches
- Ethernet1/2 on each switch should have VTP disabled

**Configuration:**

**SW1**

```
vlan 100
  name CCIE-PRUNED-VLAN

vtp mode server
vtp version 2
vtp domain SFHQ
vtp pruning
vtp password SFHQ?

interface range Ethernet1/0 - 1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switch trunk pruning vlan 100

interface Ethernet1/2
  no vtp

interface Ethernet1/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switch trunk pruning vlan 100
```

**SW2**

```
vtp mode client
vtp version 2
vtp domain SFHQ
vtp password SFHQ?

interface range Ethernet1/0 - 1
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switch trunk pruning vlan 100

interface Ethernet1/2
  no vtp

interface Ethernet1/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switch trunk pruning vlan 100
```
Verification:

SW1#show interface trunk
Port          Mode    Encapsulation  Status       Native vlan
Et1/0         on       802.1q         trunking     1
Et1/1         on       802.1q         trunking     1
Et1/3         on       802.1q         trunking     1

SW2#show interface trunk
Port          Mode    Encapsulation  Status       Native vlan
Et1/0         on       802.1q         trunking     1
Et1/1         on       802.1q         trunking     1
Et1/3         on       802.1q         trunking     1

SW1#show vtp password
VTP Password: SanFranHQ?

SW2#show vtp password
VTP Password: SanFranHQ?

SW1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name : SFHQ
VTP Pruning Mode    : Enabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3300
Configuration last modified by 192.168.10.6 at 12-14-14 21:40:05
Local updater ID is 192.168.10.6 on interface Vl118 (lowest numbered VLAN interface found)
Feature VLAN:
--------------
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 11
Configuration Revision : 11
MD5 digest : 0xE1 0xCF 0xE9 0xAF 0x53 0xFE 0xC5 0x06 0xF3 0x96 0x53 0x14 0xF8 0x77 0x08

SW2#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name : SFHQ
VTP Pruning Mode : Enabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3400
Configuration last modified by 192.168.10.6 at 12-14-14 21:40:05
Feature VLAN:
--------------
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 11
Configuration Revision : 11
MD5 digest : 0xE1 0xCF 0xE9 0xAF 0x53 0xFE 0xC5 0x06 0xF3 0x96 0x53 0x14 0xF8 0x77 0x08
**Note: We will check the trunk before VTP pruning has been enabled and then after the feature has been enabled**

**SW1#show vlan id 100**

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 CCIE-PRUNED-VLAN</td>
<td>active</td>
<td>Et1/0, Et1/1, Et1/3</td>
</tr>
</tbody>
</table>

**SW2#show vlan id 100**

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 CCIE-PRUNED-VLAN</td>
<td>active</td>
<td>Et1/0, Et1/1, Et1/3</td>
</tr>
</tbody>
</table>

**Note: The same outputs will be identical on SW2**

**SW1#show int trunk (before pruning has been enabled)**

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/3</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1,100,111,118-119,999</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1,100,111,118-119,999</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1,100,111,118-119,999</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1,100,111,119</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1,100</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1,100</td>
</tr>
</tbody>
</table>

**SW1#show int trunk (after pruning has been enabled)**

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et1/3</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed on trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1-4094</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1-4094</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans allowed and active in management domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1,100,111,118-119,999</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1,100,111,118-119,999</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1,100,111,118-119,999</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlans in spanning tree forwarding state and not pruned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et1/0</td>
<td>1,111,118-119,999</td>
</tr>
<tr>
<td>Et1/1</td>
<td>1,111,118-119,999</td>
</tr>
<tr>
<td>Et1/3</td>
<td>1,111,118-119,999</td>
</tr>
<tr>
<td>Interface</td>
<td>VTP Status</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Ethernet0/0</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet0/3</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/0</td>
<td>enabled</td>
</tr>
<tr>
<td>Ethernet1/1</td>
<td>enabled</td>
</tr>
<tr>
<td><strong>Ethernet1/2</strong></td>
<td><strong>disabled</strong></td>
</tr>
<tr>
<td>Ethernet1/3</td>
<td>enabled</td>
</tr>
</tbody>
</table>
ETHERCHANNEL

Switches should be configured with a port-channel which forces a port to join an EtherChannel without negotiation.

User number 12 on both switches

SW1 should allocate its internal VLAN’s in a descending manner

**Configuration:**

**SW1**

interface range Ethernet1/0 – 1, Ethernet1/3
channel-group 12 mode on

vlan internal allocation policy descending

**SW2**

interface range Ethernet1/0 – 1, Ethernet1/3
channel-group 12 mode on

vlan internal allocation policy descending

**Verification:**

SW1# sh run | in policy
vlan internal allocation policy **ascending**

SW2# sh run | in policy
vlan internal allocation policy **ascending**

**Note**: Layer 3 LAN ports, WAN interfaces and subinterfaces, and some software features use internal VLANs in the extended range. You cannot use an extended range VLAN that has been allocated for internal use.

To verify that the internal policy has changed create a test port-channel interface.

We can see that the newly created port-channel 1 interface has been allocated VLAN1007 in the ascending manner

SW1# conf t
SW1(config)# interface port-channel 1
SW1(config-if)# ^Z

SW1# sh vlan internal usage

VLAN Usage
--- -------------------
1006 Ethernet0/0
1007 **Port-channel**
Note: Now let’s change the policy to descending and create another test port-channel interface.
We can see that the newly created port-channel 2 interface has been allocated VLAN1007 in the descending manner.

SW1 – SW2
vlan internal allocation policy descending

SW1#sh run | in policy
vlan internal allocation policy descending

SW1#conf t
SW1(config)#int port-channel 2

SW1#sh vlan internal usage
VLAN Usage
----- -----------------
1006 Ethernet0/0
1007 Port-channel1
4094 Port-channel2

Note: Now let’s perform etherchannel checks

SW1#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------- -----------------------------------------------
12 Po12(SU) - Et1/0(P) Et1/1(P) Et1/3(P)

SW2#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------- -----------------------------------------------
12 Po12(SU) - Et1/0(P) Et1/1(P) Et1/3(P)
SW1#sh etherchannel port
  Channel-group listing:
  ----------------------
  Group: 12
  ----------
  Ports in the group:
  ----------------------

Port: Et1/0
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:04s

Port: Et1/1
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:04s

Port: Et1/3
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:37s

SW2#sh etherchannel port
  Channel-group listing:
  ----------------------
  Group: 12
  ----------
  Ports in the group:
  ----------------------

Port: Et1/0
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:37s

Port: Et1/1
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:37s

Port: Et1/3
  ----------------------
  Port state = Up Mstr In-Bndl
  Channel group = 12  Mode = On  Gcchange = -
  Port-channel = Po12  GC = -  Pseudo port-channel = Po12
  Port index = 0  Load = 0x00  Protocol = -
  Age of the port in the current state: 0d:00h:03m:37s
**SPANNING TREE**

Configure the switches as per the following:

- All switches should be configured with IEEE 802.1s
- SW1 should be manually set as the Root Bridge for all odd VLANs with an instance of 1
- SW2 should be the backup Root Bridge for all even VLANs with an instance of 2
- SW1 should be manually set as the Backup Root Bridge for all odd VLANs with an instance of 2
- SW2 should be the backup Root Bridge for all even VLANs with an instance of 2
- All other VLANs should remain in the default instance
- All switches should be in the SFHQ named region
- The hello time should be set to 1 seconds
- The forward delay should be set to 4 seconds
- The maximum age should be set to 12 seconds

**Configuration:**

**SW1**

```yaml
spanning-tree mode mst

spanning-tree mst configuration
name SFHQ
  instance 0 vlan 1-4094
  instance 1 vlan 1, 111, 119, 811, 999
  instance 2 vlan 100, 118

spanning-tree mst 1 priority 0
spanning-tree mst 2 priority 28672

spanning-tree mst max-age 12
spanning-tree mst forward-time 4
spanning-tree mst hello-time 1
```

**SW2**

```yaml
spanning-tree mode mst

spanning-tree mst configuration
name SFHQ
  instance 0 vlan 1-4094
  instance 1 vlan 1, 111, 119, 811, 999
  instance 2 vlan 100, 118

spanning-tree mst 1 priority 28672
spanning-tree mst 2 priority 0

spanning-tree mst max-age 12
spanning-tree mst forward-time 4
spanning-tree mst hello-time 1
```
Verification:

```
SW1#sh spanning-tree mst 1
##### MST1 vlans mapped: 1,111,111,999,999
Bridge address aabb.cc00.3300 priority 1 (0 sysid 1)
Root this switch for MST1
Interface Role Sts Cost Prio.Nbr Type
-------------- ---- ---- ----- ------------
Et0/1        Desg FWD 2000000 128.2    Shr
Et0/3        Desg FWD 2000000 128.4    Shr
Et1/2        Desg FWD 2000000 128.35   Shr
Po12         Desg FWD 666660 128.514  Shr
```

```
SW1#sh spanning-tree mst 2
##### MST2 vlans mapped: 100,118
Bridge address aabb.cc00.3300 priority 28674 (28672 sysid 2)
Root address aabb.cc00.3400 priority 2 (0 sysid 2)
Interface Role Sts Cost Prio.Nbr Type
-------------- ---- ---- ----- ------------
Et0/2        Desg FWD 2000000 128.3    Shr
Po12         Root FWD 666660 128.514  Shr
```

```
SW2#sh spanning-tree mst 1
##### MST1 vlans mapped: 1,111,111,999,999
Bridge address aabb.cc00.3400 priority 28673 (28672 sysid 1)
Root address aabb.cc00.3300 priority 1 (0 sysid 1)
Interface Role Sts Cost Prio.Nbr Type
-------------- ---- ---- ----- ------------
Et0/1        Desg FWD 2000000 128.2    Shr
Et0/2        Desg FWD 2000000 128.3    Shr
Et0/3        Desg FWD 2000000 128.35   Shr
Et1/2        Desg FWD 2000000 128.35   Shr
Po12         Root FWD 666660 128.514  Shr
```

```
SW2#sh spanning-tree mst 2
##### MST2 vlans mapped: 100,118
Bridge address aabb.cc00.3400 priority 2 (0 sysid 2)
Root this switch for MST2
Interface Role Sts Cost Prio.Nbr Type
-------------- ---- ---- ----- ------------
Po12          Desg FWD 666660 128.514  Shr
```

Note: Everything looks as expected
**Note:** With MSTP you can show the configuration before applying the new configuration by using the 'show pending' command within the MST configuration

```
SW1(config)#spanning-tree mst configuration
SW1(config-mst)#show pending

**Pending MST configuration**
Name      [SFHQ]  Revision  0  Instances configured 3

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2-99,101-110,112-117,120-810,812-998,1000-4094</td>
</tr>
<tr>
<td>1</td>
<td>1,111,119,811,999</td>
</tr>
<tr>
<td>2</td>
<td>100,118</td>
</tr>
</tbody>
</table>

SW1(config-mst)#
```

```
SW2(config)#spanning-tree mst configuration
SW2(config-mst)#show pending

**Pending MST configuration**
Name      [SFHQ]  Revision  0  Instances configured 3

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2-99,101-110,112-117,120-810,812-998,1000-4094</td>
</tr>
<tr>
<td>1</td>
<td>1,111,119,811,999</td>
</tr>
<tr>
<td>2</td>
<td>100,118</td>
</tr>
</tbody>
</table>

SW2(config-mst)#
```

**Note:** And now the timers (defaults)

```
SW1#sh spanning-tree  | in MST | Hello | Max | Forward
MST0                 | Hello Time | 2 sec | Max Age 20 sec | Forward Delay 15 sec
MST1                 | Hello Time | 2 sec | Max Age 20 sec | Forward Delay 15 sec
MST2                 | Hello Time | 2 sec | Max Age 20 sec | Forward Delay 15 sec
```
**Note: And after the change**

<table>
<thead>
<tr>
<th>MST0</th>
<th>MST1</th>
<th>MST2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Time</td>
<td>1 sec</td>
<td>Max Age 12 sec</td>
</tr>
<tr>
<td>Hello Time</td>
<td>1 sec</td>
<td>Max Age 12 sec</td>
</tr>
<tr>
<td>Hello Time</td>
<td>1 sec</td>
<td>Max Age 12 sec</td>
</tr>
<tr>
<td>Hello Time</td>
<td>1 sec</td>
<td>Max Age 12 sec</td>
</tr>
</tbody>
</table>

 SWI#sh spanning-tree | in MST| Hello| Max| Forward Delay
 MST0
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |

 MST1
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |

 MST2
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |
 Hello Time  | 1 sec | Max Age 12 sec | Forward Delay 4 sec |
CCIEv5 R&S L2 Topology

BGP AS 64799

SW6 E0/3 E0/2 E1/0 E1/2 E2/0

R17

SW7 E0/3 E0/0 E0/1 E1/1 E2/0 E1/0

R18

Sydney Business Model HQ

Printer

Multicast Server#4 (R84)

Copyright © 2015 CCIE4ALL. All rights reserved
Sydney Business Model

VLAN TRUNK VTP

Interfaces connecting to other switches should be configured as dot1q trunk interfaces.
All switches should be configured as VTP Version 3 with the following requirements:

- SW6 is the primary switch for the VLAN database
- SW7 and should be configured as the backup
- Domain name should be set to SYDNEY

All switches should have an encrypted password of 2C46B5155E3A36D893761CB99D46C320
All switches should store the VLAN database in flash with a filename of SYDNEY-VLANS

**Configuration:**

**SW6**
```
vtp domain SYDNEY
vtp version 3
vtp password 2C46B5155E3A36D893761CB99D46C320 secret
vtp primary vlan (exec mode configuration)
vtp file SYDNEY-VLANS

interface range Ethernet0/0 - 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

**SW7**
```
vtp domain SYDNEY
vtp version 3
vtp password 2C46B5155E3A36D893761CB99D46C320 secret
vtp file SYDNEY-VLANS

interface range Ethernet0/0 - 1
switchport trunk encapsulation dot1q
switchport mode trunk
```

**Verification:**

**SW6#sh interface trunk**
```
<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>E0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>
```

**SW7#sh interface trunk**
```
<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0/0</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>E0/1</td>
<td>on</td>
<td>802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>
SW6# show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : SYDNEY
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3800
Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
               0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Feature MST:
--------------
VTP Operating Mode : Transparent
Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent

SW7# show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : SYDNEY
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : aabb.cc00.3900
Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
               0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Feature MST:
--------------
VTP Operating Mode : Transparent
Feature UNKNOWN:
--------------
VTP Operating Mode : Transparent

SW6# show vtp password
VTP Password: 2C46B5155E3A36D893761CB99D46C320

SW7# show vtp password
VTP Password: 2C46B5155E3A36D893761CB99D46C320
SW6#dir flash:/SYDNEY-VLANS
Directory of unix:/SYDNEY-VLANS
41874  -rw-  10236  Dec 15 2014 20:04:02 +01:00  SYDNEY-VLANS
2147479552 bytes total (2147479552 bytes free)

SW7#dir flash:/SYDNEY-VLANS
Directory of unix:/SYDNEY-VLANS
41873  -rw-  10236  Dec 15 2014 20:03:30 +01:00  SYDNEY-VLANS
2147479552 bytes total (2147479552 bytes free)
ETHERCHANNEL

Configure the switches with 802.3ad etherchannel as per the following:

- SW6 should actively negotiate the channel with a number of 1
- SW7 should passively negotiate the channel with a number of 1
- SW6 with the lowest possible system priority
- SW7 with the highest possible system priority
- Set the channel protocol manually
  Both switches should only ever be allowed a maximum of 2 bundled active ports in the channel-group

Configuration:

**SW6**

```
interface range Ethernet0/0 - 1
  channel-group 1 mode active
  channel-protocol lacp

interface port-channel 1
  lacp max-bundle 2
  lacp system-priority 1
```

**SW7**

```
interface range Ethernet0/0 - 1
  channel-group 1 mode passive
  channel-protocol lacp

interface port-channel 1
  lacp max-bundle 2
  lacp system-priority 65535
```

Verification:

**Note:** When the channel-group command is applied to the physical switchport a logical port-channel interface is created automatically

```
SW6(config)#int range eth 0/0-1
SW6(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

SW7(config)#int range eth 0/0-1
SW7(config-if-range)#channel-group 1 mode passive
Creating a port-channel interface Port-channel 1
```
**Note:** The port channel will go into a suspended state if only one end of the link is configured for LACP

SW7

*Dec 16 18:18:47.099: %EC-L3DONTBNDL2: Et0/1 suspended: LACP currently not enabled on the remote port.

*Dec 16 18:18:47.227: %EC-L3DONTBNDL2: Et0/0 suspended: LACP currently not enabled on the remote port.

`SW7#show etherchannel summary`

**Flags:**
- D - down
- P - bundled in port-channel
- I - stand-alone
- s - suspended
- H - Hot-standby (LACP only)
- R - Layer3
- S - Layer2
- U - not in use
- f - failed to allocate aggregator
- u - unsuitable for bundling
- w - waiting to be aggregated
- d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SD)</td>
<td>LACP</td>
<td>Et0/0(a) Et0/1(a)</td>
</tr>
</tbody>
</table>

**Note:** Once the configuration has been done on SW6 the port-channel interface on both switches comes up

SW6#

*Dec 16 18:19:47.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

SW7

*Dec 16 18:19:47.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

`SW7#show etherchannel summary`

**Flags:**
- D - down
- P - bundled in port-channel
- I - stand-alone
- s - suspended
- H - Hot-standby (LACP only)
- R - Layer3
- S - Layer2
- U - in use
- f - failed to allocate aggregator
- M - not in use, minimum links not met
- u - unsuitable for bundling
- w - waiting to be aggregated
- d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Po1(SU)</td>
<td>LACP</td>
<td>Et0/0(P) Et0/1(P)</td>
</tr>
</tbody>
</table>
**Note:**

**LACP system priority:**
A LACP system priority is configured on each router running LACP. The system priority can be configured automatically or through the CLI. LACP uses the system priority with the router MAC address to form the system ID and also during negotiation with other systems.

The LACP system ID is the combination of the LACP system priority value and the MAC address of the router.

**LACP port priority:**
A LACP port priority is configured on each port using LACP. The port priority can be configured automatically or through the CLI. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

SW6
SW6#show lacp sys-id
1, aabb.cc00.3800

SW7
SW7#show lacp sys-id
65535, aabb.cc00.3800

SW6#show lacp 1 neighbor
Flags:  S - Device is requesting Slow LACPDU
        F - Device is requesting Fast LACPDU
        A - Device is in Active mode       P - Device is in Passive mode

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>key</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>SP</td>
<td>32768</td>
<td>aabb.cc00.3900</td>
<td>11s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x1</td>
<td>0x3C</td>
<td></td>
</tr>
<tr>
<td>Et0/1</td>
<td>SP</td>
<td>32768</td>
<td>aabb.cc00.3900</td>
<td>24s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x2</td>
<td>0x3C</td>
<td></td>
</tr>
</tbody>
</table>

SW7#show lacp 1 neighbor
Flags:  S - Device is requesting Slow LACPDU
        F - Device is requesting Fast LACPDU
        A - Device is in Active mode       P - Device is in Passive mode

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
<th>Dev ID</th>
<th>Age</th>
<th>key</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>SA</td>
<td>32768</td>
<td>aabb.cc00.3800</td>
<td>24s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x1</td>
<td>0x3D</td>
<td></td>
</tr>
<tr>
<td>Et0/1</td>
<td>SA</td>
<td>32768</td>
<td>aabb.cc00.3800</td>
<td>11s</td>
<td>0x0</td>
<td>0x1</td>
<td>0x2</td>
<td>0x3D</td>
<td></td>
</tr>
</tbody>
</table>
SPANNING TREE

Configure the switches with spanning-tree according to the 802.1d standard.
Manually set SW6 as the root for ALL VLANS and SW7 as the backup root – use the most optimal values.
Configure all access ports do not wait for the forwarding delay – use a single command.
The HR VLAN should have the following timers applied:
- Hello = 4 seconds
- Forward Delay = 10 seconds
- Max Age = 30 seconds
Ethernet0/2 on SW6 should never receive spanning-tree packets and the port should transition into an err-disabled state if this is violated.
The timeout for the CAM table on SW7 should be set to a minimum possible value.

**Configuration:**

**SW6**

```plaintext
spanning-tree mode pvst
spanning-tree portfast default

spanning-tree vlan 1-4094 priority 0
spanning-tree vlan 10 hello-time 4
spanning-tree vlan 10 forward-time 10
spanning-tree vlan 10 max-age 30

interface Ethernet0/2
  spanning-tree bpduguard enable
```

**SW7**

```plaintext
spanning-tree mode pvst
spanning-tree portfast default

mac address-table aging-time 10
```

**Verification:**

```
SW6#sh spanning-tree | in VLAN|Et|Po
VLAN0001
  Et1/2  Desg FWD 100   128.35  Shr Edge
  Et1/3  Desg FWD 100   128.36  Shr Edge
  Po1   Desg FWD 56    128.514 Shr
VLAN0010
  Et1/1  Desg FWD 100   128.34  Shr Edge
  Po1   Desg FWD 56    128.514 Shr
VLAN0020
  Po1   Desg FWD 56    128.514 Shr
VLAN0050
  Po1   Desg FWD 56    128.514 Shr
VLAN0078
  Et1/0  Desg FWD 100   128.33  Shr Edge
  Po1   Desg FWD 56    128.514 Shr
VLAN0567
  Et0/2  Desg FWD 100   128.3  Shr Edge
  Et0/3  Desg FWD 100   128.4  Shr Edge
  Po1   Desg FWD 56    128.514 Shr
VLAN0668
  Po1   Desg FWD 56    128.514 Shr
```
**Note:** *The Shr Edge* port type indicates that portfast is enabled, these are the ports that connect to the routers in the topology

SW6#sh spanning-tree summary
Switch is in pvst mode
**Root bridge for:** VLAN0001, VLAN0010, VLAN0020, VLAN0050, VLAN0078, VLAN0567

| VLAN0001 | 0 | 0 | 0 | 3 | 3 |
| VLAN0010 | 0 | 0 | 0 | 2 | 2 |
| VLAN0020 | 0 | 0 | 0 | 1 | 1 |
| VLAN0050 | 0 | 0 | 0 | 1 | 1 |
| VLAN0078 | 0 | 0 | 0 | 2 | 2 |
| VLAN0567 | 0 | 0 | 0 | 3 | 3 |
| VLAN0668 | 0 | 0 | 0 | 1 | 1 |

**Note:** When the channel-group command is applied to the physical switchport a logical port-channel interface is created automatically

SW6#show spanning-tree interface ethernet 1/2 portfast
VLAN0001  **enabled**

SW6#show spanning-tree interface ethernet 1/3 portfast
VLAN0001  **enabled**

SW6#show spanning-tree interface port-channel 1 portfast
VLAN0001  disabled
VLAN0010  disabled
VLAN0020  disabled
VLAN0050  disabled
VLAN0078  disabled
VLAN0567  disabled
VLAN0668  disabled
Note: The key output here is the Root ID and the Root Cost. Below output tells us that SW6 is the root bridge for all VLANs.

### SW6#sh spanning-tree root

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Root ID</th>
<th>Root Cost</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>1 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VLAN0010</td>
<td>10 aabb.cc00.3800</td>
<td>0</td>
<td>4</td>
<td>30</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>VLAN0020</td>
<td>20 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VLAN0050</td>
<td>50 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VLAN0078</td>
<td>78 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VLAN0567</td>
<td>567 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>VLAN0668</td>
<td>668 aabb.cc00.3800</td>
<td>0</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

Note: The timers - In legacy ieee spanning-tree the root bridge controls the timers for the spanning tree domain. The timers only need to be set on the root bridge. SW7 in this case receives the updated hello-time, forward-time and max-age from SW6 - for VLAN 10 in this case as per the question. We will compare the timers it with for example VLAN78.

### SW7#sh spanning-tree root

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Root ID</th>
<th>Root Cost</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
<th>Root Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>1 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0010</td>
<td>10 aabb.cc00.3800</td>
<td>56</td>
<td>4</td>
<td>30</td>
<td>10</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0020</td>
<td>20 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0050</td>
<td>50 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0078</td>
<td>78 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0567</td>
<td>567 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
<tr>
<td>VLAN0668</td>
<td>668 aabb.cc00.3800</td>
<td>56</td>
<td>2</td>
<td>20</td>
<td>15</td>
<td>Po1</td>
</tr>
</tbody>
</table>

### SW6#sh spanning-tree vl 10 | in Hello|Max|Forward|Root|Bridge

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>4 sec</td>
<td>30 sec</td>
<td>10 sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10 (priority 0 sys-id-ext 10)</td>
<td>4 sec</td>
<td>30 sec</td>
<td>10 sec</td>
</tr>
</tbody>
</table>

### SW6#sh spanning-tree vl 78 | in Hello|Max|Forward|Root|Bridge

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>78</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge ID</th>
<th>Priority</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>78 (priority 0 sys-id-ext 78)</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>
```
SW7#sh spanning-tree root hello-time
VLAN0001 2
VLAN0010 4
VLAN0020 2
VLAN0030 2
VLAN0078 2
VLAN0078 2
VLAN0668 2

SW7#sh spanning-tree root forward-time
VLAN0001 15
VLAN0010 10
VLAN0020 15
VLAN0030 15
VLAN0078 15
VLAN0078 15
VLAN0668 15

SW7#sh spanning-tree root max-age
VLAN0001 20
VLAN0010 30
VLAN0020 20
VLAN0030 20
VLAN0078 20
VLAN0078 20
VLAN0668 20

Note: We will now simulate a BPDU being received on ethernet0/2 from R17

```

```text
R17
  bridge 1 protocol ieee

  interface Ethernet1/0
  bridge-group 1

SW6#*Dec 19 20:10:57.184: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/2 with BPDU Guard enabled. Disabling port.*
*Dec 19 20:10:57.184: %RM-4-BPD_G: bpduguard error detected on Et0/2, putting Et0/2 in err-disable state
*Dec 19 20:10:58.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down

SW6#show interfaces status | include Et0/2
Et0/2  err-disabled 567  auto  auto unknown

Note: In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

Once a port is in err-disabled you need to manually shutdown and no shutdown the interface, however as R17 is still sending BPDU’s the port goes back into an err-disabled state
```
SW6(config)#interface ethernet 0/2
SW6(config-if)#shut
*Dec 19 20:15:12.226: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
SW6(config-if)#no shut
SW6(config-if)#a all
*Dec 19 20:15:16.794: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et0/2 with BPDU Guard enabled. Disabling port.
*Dec 19 20:15:16.794: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/2, putting Et0/2 in err-disable state
SW6(config-if)#int et 0/2
*Dec 19 20:15:20.114: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to down
SW6(config-if)#end

SW6#show interfaces status | include Et0/2
Et0/2 err-disabled 567 auto auto unknown

Note: Once the BPDU's have stopped being received the port can come up after a shutdown/no shutdown

R17
bridge 1 protocol ieee
interface Ethernet1/0
  bridge-group 1 spanning-disabled

Note: Or remove the bridging entirely from R17 to disable spanning tree BPDUs

SW6(config)#interface ethernet 0/2
SW6(config-if)#shut
*Dec 19 20:17:37.574: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
SW6(config-if)#no shut
SW6#
*Dec 19 20:17:40.819: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Dec 19 20:17:41.824: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
SW6#show interfaces status | in Et0/2
Et0/2 connected 567 auto auto unknown

SW6#sh spanning-tree interface et 0/2 detail
Port 3 (Ethernet0/2) of VLAN0567 is designated forwarding
  Port path cost 100, Port priority 128, Port Identifier 128.3.
  Designated root has priority 567, address aabb.cc00.3800
  Designated bridge has priority 567, address aabb.cc00.3800
  Designated port id is 128.3, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode by default
  Link type is shared by default
  Bpdu guard is enabled
  BPDU: sent 3, received 0
**Note:** To set the timeout for MAC address table entries, use the `mac-address-table aging-time` command in global configuration mode. The default value is 5 minutes.

Let's choose the port where R17 Ethernet2/0 connects to – refer to the diagram.

```
SW7#show mac address-table aging-time
Global Aging Time: 10
Vlan   Aging Time
----   ---------

SW7#sh mac address-table interface et 1/0
Mac Address Table
-------------------------------
Vlan  Mac Address       Type        Ports
----  ---------------       -------      ----
78    aabb.cc00.1102    DYNAMIC     Et1/0
Total Mac Addresses for this criterion: 1
```

```
SW7# sh clock
*15:50:23.110 CET Sat Jan 3 2015
```

**Note:** We now shut the port on R17 down to flush out the CAM table.

```
R17(config-if)#int et 2/0
R17(config-if)#no shu
R17(config-if)#
*Jan 3 14:49:13.629: %LINK-3-UPDOWN: Interface Ethernet2/0, changed state to up
*Jan 3 14:49:14.638: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to up
R17(config-if)#shut
R17(config-if)#
*Jan 3 14:50:36.316: %LINK-5-CHANGED: Interface Ethernet2/0, changed state to administratively down

SW7#sh clock
*15:50:40.870 CET Sat Jan 3 2015
```

```
SW7#sh mac address-table interface et 1/0
Mac Address Table
-------------------------------
Vlan  Mac Address       Type        Ports
----  ---------------       -------      ----
```

```
SW7#sh clock
*15:50:40.870 CET Sat Jan 3 2015
```
Troubleshooting Guidelines

This section is comprised of a set of troubleshooting scenarios. You have a maximum of 2 hours to complete the section. The final score of this section is combined with the Configuration sections to comprise your final Pass or Fail status on the given lab exam. A candidate is required to pass both sections to achieve Cisco CCIE certification. You will be presented with preconfigured routers and Frame-Relay switches in the topology. DO NOT change the following configuration on the devices.

- Hostname
- Enable password "cisco"
- Console line configuration
- For all of the authentication configuration in the lab, password is "cisco" unless changed to introduce a break. Do NOT change AAA configuration unless explicitly stated in a question.
- Points are awarded for finding AND fixing inserted faults in the presented fully configured topology. An inserted fault is an introduced break for a scenario that was previously working. Depending on the scenario, fixing the inserted faults could require multiple command lines on the same or multiple devices.
- The resolution of one incident may depend on the resolution of previous incident(s). The dependency will not be visible if the tickets are resolved in sequence.
- There are NO physical faults introduced in the presented topology.
- Do NOT change any routing protocol boundaries. Refer to the provided diagram.
- DO NOT REMOVE ANY FEATURE CONFIGURED IN ORDER TO RESOLVE AN INCIDENT, YOU MUST RESOLVE MISCONFIGURATION RATHER THAN REMOVING IT ALL (examples: Access-lists, PBR, CoPP, MQC, etc.)
- Static and default routes are NOT permitted unless preconfigured. These restrictions include floating static and those generated by routing protocols. Routes to Null0 that are generated by a dynamic routing protocol solution are permitted.
- Tunneling and policy-routing are NOT permitted unless preconfigured.
- Dynamic Frame Relay mappings are NOT permitted.
- Points will be deducted for every incident in which candidate uses a prohibited solution.
- Candidates have control of all required devices in the topology.
- If required to verify the reachability from a host machine during the lab exam, use the ping command with source option on the router that is shown connected to the subjected host in the diagram.
CCIEv5 Routing & Switching
MPLS Troubleshooting Lab#4
Questions & Solutions

Tom Mark Giembicki
Sean Draper
LAB#4

Incident#1

R8 Loopback0 is not able to ping R10 Loopback0
This incident contains six separate faults
Do not make any configuration changes on R8
While you are resolving this issue, you are not allowed to create any new interfaces
Refer to the Troubleshooting guidelines to determine if your solution is appropriate

R8#ping 192.10.10.10 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.10.10.10, timeout is 2 seconds:
Packet sent with a source address of 192.8.8.8
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/7 ms

Configuration:

```
SW1
  interface Ethernet0/2
    switchport port-security mac-address dabc.aaaa.bbcc exchange-switchport port-security mac-address dabc.aaaa.bbcc

R10
  router ospf 20001
    network 192.10.10.8 0.0.0.3 area 1
    network 192.10.10.10 0.0.0.0 area 0

  interface Loopback0
    ip ospf prefix-suppression exchange ip ospf prefix-suppression disable

  Extended IP access list 112
    10 permit tcp any any precedence network
    20 permit tcp any any precedence internet
    30 permit tcp any any
    40 permit udp any any precedence network
    50 permit udp any any precedence internet
    60 permit ip any host 224.0.0.5 exchange deny ip any host 224.0.0.5
    70 permit tcp any any
    80 permit udp any any

  interface Ethernet1/0
    ip ospf message-digest-key 78 md5 CISCO
```
Incident#2

R9 and R11 are not able to establish LDP Adjacency
This incident contains four separate faults
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification.

R9#
Dec 31 14:05:02.080: %LDP-5-NBRCHG: LDP Neighbor 192.11.11.11 (1) is UP

Configuration:

R9
Extended IP access list MPLSLDP
  10 permit udp host 192.11.11.11 eq 646 host 224.0.0.2 eq 646
  20 permit tcp host 192.11.11.1 host 192.9.9.9 eq 646
  30 deny tcp any eq 646
  40 deny tcp any eq 646 any
  50 permit ip any any
no 20
  20 permit tcp host 192.11.11.1 host 192.9.9.9 eq 646

R11
Extended IP access list MPLSLDP
  10 permit udp host 192.9.9.9 eq 646 host 224.0.0.2 eq 646
  20 permit tcp host 192.9.9.9 eq 645 host 192.11.11.11
  30 deny tcp any eq 646
  40 deny tcp any eq 646 any
  50 permit ip any any
no 20
  20 permit tcp host 192.9.9.9 eq 646 host 192.11.11.11

mpls ldp router-id Loopback1
mpls ldp router-id Loopback0 force

SW2
interface Ethernet0/2
  switchport access vlan 119
  switchport mode access
Incident#3

R91 in Service Provider#5 can not ping PC#1 in San Francisco Group Remote Site#1
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification
Ensure R12 BGP output matches
This incident contains six separate faults

R91#sh ip cef vrf San-Francisco 192.168.20.100
192.168.20.0/24
nexthop 155.84.74.18 Ethernet0/0

R91#ping vrf San-Francisco 192.168.20.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms

R12#sh ip bgp | be Network
<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric LocPrf Weight Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 0.0.0.0</td>
<td>155.84.74.17</td>
<td>0 15789 i</td>
</tr>
<tr>
<td>*&gt; 192.12.12.12/32</td>
<td>0.0.0.0</td>
<td>0 32768 t</td>
</tr>
<tr>
<td>*&gt; 192.168.20.0</td>
<td>0.0.0.0</td>
<td>0 32768 t</td>
</tr>
</tbody>
</table>

Configuration:

PC1
no ip route 0.0.0.0 0.0.0.0 192.168.20.122
ip route 0.0.0.0 0.0.0.0 0.0.0.0 192.168.20.12
R12
policy-map LAN-POLICY
class LAN-CLASS
  police cir 8000 conform-action drop exceed-action drop violate-action drop
  police cir 8000 conform-action transmit exceed-action transmit violate-action transmit
router eigrp 150
  no network 192.168.12.0
  network 192.168.20.0

R91
no ip route vrf San-Francisco 192.168.20.100 255.255.255.255 155.84.74.81
router bgp 15789
  address-family ipv4 vrf San-Francisco
    no neighbor 155.84.74.18 shutdown
    neighbor 155.84.74.18 default-originate
Incident #4

R93 can not ping Global DNS Server 4.2.2.2

Fix problem so the following ping results in 100% success

While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification

This incident contains three separate faults

R93#sh ip bgp 4.2.2.2

BGP routing table entry for 4.2.0.0/28, version 4
Paths: (1 available, best #1, table default)
Advertised to update-groups:
  1        4
Refresh Epoch 1
18657
140.60.88.33 from 140.60.88.33 (172.15.15.15)
  Origin IGP, metric 0, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0

R93#ping 4.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
**Configuration:**

R93
no ip route 4.2.2.2 255.255.255.255 Null0
access-list 50 deny 0.0.0.0 /0
access-list 50 permit 0.0.0.0 /0

R15
no ip as-path access-list 100 deny *
ip as-path access-list 100 permit *
ip cef
Incident#5

R7 can not ping R3 Loopback 0 IP Address
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification
This incident contains five separate faults

R7#ping 172.100.3.3 source 172.100.7.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.100.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.100.7.7
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/6 ms

Configuration:

SW3
interface Port-channel54
  switchport trunk allowed vlan remove 13,17
  switchport trunk allowed vlan add 13,17
  vtp

interface Port-channel43
  switchport trunk allowed vlan remove 13,17
  switchport trunk allowed vlan add 13,17
  vtp

R3
interface Loopback0
  no ip ospf shutdown
Incident#6

R20 is not able to establish EIGRP adjacency with R95.

While you are resolving this issue, you are not allowed to create any new interfaces.

Refer to the Troubleshooting guidelines to determine if your solution is appropriate.

Ensure R95 produces following outputs:

This incident contains eight separate faults.

R20#sh ip eigrp
EIGRP-IPv4 VR(Sydney) Address-Family Neighbors for AS(250)

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>155.84.74.42</td>
<td>Se1/0</td>
<td>11 01:01:54</td>
<td>21</td>
<td>126</td>
<td>0</td>
<td>28</td>
</tr>
</tbody>
</table>

R95#sh ip eigrp vrf New-York-Sydney neighbors
EIGRP-IPv4 VR(VRF-EIGRP) Address-Family Neighbors for AS(250) VRF(New-York-Sydney)

<table>
<thead>
<tr>
<th>H</th>
<th>Address</th>
<th>Interface</th>
<th>Hold Uptime</th>
<th>SRTT</th>
<th>RTO</th>
<th>Q</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>155.84.74.41</td>
<td>Se3/0</td>
<td>12 01:02:24</td>
<td>18</td>
<td>108</td>
<td>0</td>
<td>27</td>
</tr>
</tbody>
</table>

R95#ping vrf New-York-Sydney 155.84.74.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 155.84.74.41, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
**R95#sh ip pim vrf New-York-Sydney neighbor**

**PIM Neighbor Table**

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Interface</th>
<th>Uptime/Expires</th>
<th>Ver</th>
<th>DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.84.74.41</td>
<td>Serial3/0</td>
<td>00:02:08/00:01:34</td>
<td>v2</td>
<td>1 / S P G</td>
</tr>
</tbody>
</table>

**Configuration:**

```
R95
no username R20EAP password 0 CISCO

username R20EAP password 0 CISCO

no ip route vrf New-York-Sydney 155.84.74.41 255.255.255.255 null 0

R20
interface Serial1/0
ip pim sparse-mode
encapsulation ppp
ppp authentication eap
ppp eap identity R20EAP
ppp eap password 0 CISCO
ppp eap local

Extended IP access list 170
10 deny eigrp any 224.0.0.0 0.0.0.31
20 deny pim any any
30 deny ip any any

Extended IP access list 170
10 permit eigrp any 224.0.0.0 0.0.0.31
20 permit pim any any
30 permit ip any any
```
Incident#7

From R3, when you use command: \textbf{GetR7Hostname}, you must produce exactly same output
This incident contains three separate faults
While you are resolving this issue, you are not allowed to create any new interfaces
Refer to the Troubleshooting guidelines to determine if your solution is appropriate

\textit{R3}\#GetR7Hostname
SNMP Response: reqid 12, errstat 0, erridx 0
\texttt{system.5.0 = R7}

Configuration:

\texttt{R3}

no alias exec GetR7Hostname snmp get v2c 172.100.77.77 cisco oid system.4.0
alias exec GetR7Hostname snmp get v2c 172.100.7.7 cisco oid system.5.0

\texttt{R7}

no access-list 20 permit 172.100.3.3
access-list 20 permit 172.31.10.9
ip access-list extended 101
no 10 deny udp host 172.31.10.9 host 172.100.7.7 range snmp snmptrap
10 permit udp host 172.31.10.9 host 172.100.7.7 range snmp snmptrap
Incident #8

PC#1 should be able to ping and telnet on port 80 to www.google.com (86.55.171.197)
Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification
This incident contains five separate faults
While you are resolving this issue, you are not allowed to create any new interfaces.

PC1#ping www.google.com
Translating "www.google.com"...domain server (4.2.2.2) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 86.55.171.197, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/11/14 ms

PC1#telnet www.google.com 80
Trying www.google.com (86.55.171.197, 80)... Open sd
HTTP/1.1 400 Bad Request!
Date: Wed, 31 Dec 2014 14:36:12 GMT
400 Bad Request
[Connection to www.google.com closed by foreign host]

PC1#traceroute www.google.com
Translating "www.google.com"...domain server (4.2.2.2) [OK]
Type escape sequence to abort.
Tracing the route to www.google.com (86.55.171.197)
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.20.12 5 msec 5 msec 5 msec
  2 155.84.74.17 1 msec 1 msec 1 msec
  3 155.84.74.13 0 msec 0 msec 1 msec
  4 192.168.11.9 6 msec 2 msec 5 msec
  5 155.84.74.6 6 msec 9 msec 6 msec
  6 86.191.16.1 11 msec * 13 msec

Configuration:

SERVER2(Global DNS)
  ip dns server
R96
  ip http server
R11
  router bgp 10784
      address-family ipv4
      neighbor 192.168.9.9 next-hop-self
      exit-address-family

R91
  no route-map VRF-TABLE deny 10
  match ip address prefix-list VRF-TABLE
  set mpls-label
  set vrf San-Francisco
  set interface Ethernet0/0 Ethernet1/0 Null0
  route-map VRF-TABLE permit 10
  match ip address prefix-list VRF-TABLE

R92
  router bgp 25432
      address-family ipv4
      neighbor 192.168.93.93 route-reflector-client
      exit-address-family
Incident#9

PC#1 is not able to reach Web Server#1 (New York DC) and New Warehouse User

While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate.

This incident contains four separate faults.
Configuration:

**R91**

```
router bgp 15789

   address-family ipv4 vrf New-York-Sydney
      no redistribute ospf 200 metric 4294967295 route-map ROUTE-CHANGE
      redistribute ospf 200 match internal external 1 external 2
      exit-address-family

   vrf definition San-Francisco
      address-family ipv4
         route-target import 200:250
         exit-address-family

R13

   no class-map match-all ICMP
      match protocol icmp
      match access-group 155

   no policy-map ICMP
      class ICMP
         police cir 8000
            conform-action drop

      class-map match-any ICMP
      match protocol icmp
      match access-group 155

      policy-map ICMP
         class ICMP
            police cir 1000000
               conform-action transmit

   interface Ethernet0/0
      service-policy input ICMP
```
Incident#10

PC#3 in Sydney has lost ICMP reachability to Web Server#1 (New York DC) and New Warehouse User
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the
Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you
disconnected the telnet session after verification
This incident contains three separate faults

PC3#ping 192.168.30.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.100, timeout is 2 seconds:

!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/33 ms

PC3#traceroute 192.168.30.100
Type escape sequence to abort.
Tracing the route to 192.168.30.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.160.20 3 msec 5 msec 4 msec
2 155.84.74.42 11 msec 12 msec 9 msec
3 66.171.14.13 [MPLS: label 29 Exp 0] 29 msec 33 msec 27 msec
4 66.171.14.10 [MPLS: label 30 Exp 0] 29 msec 32 msec 32 msec
5 86.191.16.10 [MPLS: labels 17/25 Exp 0] 28 msec 33 msec 32 msec
6 86.191.16.3 [MPLS: label 25 Exp 0] 24 msec 32 msec 27 msec
7 155.84.74.5 [MPLS: Label 23 Exp 0] 31 msec 29 msec 29 msec
8 192.168.11.10 [MPLS: Label 23 Exp 0] 28 msec 32 msec 29 msec
9 155.84.74.21 28 msec 28 msec 31 msec
10 155.84.74.22 31 msec 31 msec 34 msec
11 192.168.30.100 36 msec * 31 msec

PC3#ping 10.1.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/37 ms

PC3#traceroute 10.1.0.100
Type escape sequence to abort.
Tracing the route to 10.1.0.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.160.20 5 msec 4 msec 4 msec
2 155.84.74.42 24 msec 9 msec 10 msec
4 66.171.14.10 [MPLS: Label 27 Exp 0] 110 msec 31 msec 29 msec
5 86.191.16.10 [MPLS: Labels 17/22 Exp 0] 34 msec 27 msec 28 msec
6 86.191.16.5 [MPLS: Label 22 Exp 0] 27 msec 40 msec 27 msec
7 155.84.74.5 [MPLS: Label 20 Exp 0] 30 msec 30 msec 35 msec
8 192.168.11.10 [MPLS: Label 20 Exp 0] 26 msec 36 msec 25 msec
9 155.84.74.21 29 msec 30 msec 27 msec
10 155.84.74.22 32 msec * 30 msec

Configuration:

R94
interface Ethernet0/0
mpls bgp forwarding

PC1
no ip route 10.1.0.0 255.255.255.0 192.168.160.120
ip route 10.1.0.0 255.255.255.0 192.168.160.20
ip route 0.0.0.0 0.0.0.0 192.168.160.20

R93
router bgp 25432
no bgp default route-target filter
**Incident #11**

Users in Sydney Business Remote Office R20 has lost Multicast Stream Video access coming from New York DC R13

R96 is not receiving any prefixes for the VRF 'New York Sydney'

While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification

This incident contains three separate faults
Configuration:

R20
  interface Serial1/0
  ip pim sparse-mode

R95
  ip pim vrf New-York-Sydney rp-address 95.95.95.95
  interface Loopback0
    vrf forwarding New-York-Sydney
    ip address 95.95.95.95 255.255.255.255
    ip pim sparse-mode
Incident#12
PC#4 in San Francisco Group Remote Site#2 needs to be able to reach PC#1 PC#3 New York Warehouse User and Web Server#1
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you disconnected the telnet session after verification
This incident contains five separate faults

PC4#ping 192.168.20.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 21/22/23 ms

PC4#ping 192.168.30.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/22/25 ms

PC4#ping 10.1.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.100, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/24 ms

PC4#ping 192.168.160.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.100, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/13/15 ms

PC4#traceroute 192.168.20.100
Type escape sequence to abort.
Tracing the route to 192.168.20.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 3 msec 1 msec 5 msec  
2 140.60.88.73 6 msec 6 msec 5 msec  
3 172.31.10.10 [MPLS: Labels 17/35 Exp 0] 24 msec 23 msec 22 msec  
4 172.31.10.34 [MPLS: Label 35 Exp 0] 24 msec 24 msec 22 msec  
5 140.60.88.65 [MPLS: Label 32 Exp 0] 29 msec 30 msec 27 msec  
6 86.191.16.10 [MPLS: Labels 17/27 Exp 0] 22 msec 23 msec 46 msec  
7 86.191.16.5 [MPLS: Label 27 Exp 0] 23 msec 24 msec 34 msec  
8 155.84.74.5 [MPLS: Label 25 Exp 0] 24 msec 23 msec 22 msec  
9 192.168.11.10 [MPLS: Label 25 Exp 0] 24 msec 23 msec 24 msec  
10 155.84.74.17 [MPLS: Label 18 Exp 0] 21 msec 33 msec 28 msec  
11 155.84.74.18 20 msec 21 msec 27 msec  
12 192.168.20.100 21 msec * 23 msec

PC4#traceroute 192.168.30.100
Type escape sequence to abort.
Tracing the route to 192.168.30.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 3 msec 1 msec 5 msec  
2 140.60.88.73 6 msec 6 msec 8 msec  
3 172.31.10.10 [MPLS: Labels 17/33 Exp 0] 22 msec 28 msec 23 msec  
4 172.31.10.34 [MPLS: Label 33 Exp 0] 23 msec 23 msec 23 msec  
5 140.60.88.65 [MPLS: Label 30 Exp 0] 27 msec 22 msec 21 msec  
6 86.191.16.10 [MPLS: Labels 17/25 Exp 0] 20 msec 26 msec 22 msec  
7 86.191.16.5 [MPLS: Label 25 Exp 0] 17 msec 21 msec 23 msec  
8 155.84.74.5 [MPLS: Label 23 Exp 0] 24 msec 21 msec 25 msec  
9 192.168.11.10 [MPLS: Label 23 Exp 0] 28 msec 24 msec 25 msec  
10 155.84.74.21 21 msec 22 msec 27 msec  
11 155.84.74.22 23 msec 22 msec 21 msec  
12 192.168.30.100 23 msec * 25 msec

PC4#traceroute 10.1.0.100
Type escape sequence to abort.
Tracing the route to 10.1.0.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 5 msec 4 msec 7 msec  
2 140.60.88.73 6 msec 8 msec 8 msec  
3 172.31.10.10 [MPLS: Labels 17/20 Exp 0] 49 msec 29 msec 21 msec  
4 172.31.10.34 [MPLS: Label 20 Exp 0] 23 msec 25 msec 22 msec  
5 140.60.88.65 [MPLS: Label 27 Exp 0] 27 msec 22 msec 23 msec  
6 86.191.16.10 [MPLS: Labels 17/22 Exp 0] 23 msec 24 msec 24 msec  
7 86.191.16.5 [MPLS: Label 22 Exp 0] 21 msec 23 msec 25 msec  
8 155.84.74.5 [MPLS: Label 20 Exp 0] 25 msec 23 msec 22 msec  
9 192.168.11.10 [MPLS: Label 20 Exp 0] 22 msec 24 msec 23 msec  
10 155.84.74.21 22 msec 22 msec 23 msec  
11 155.84.74.22 29 msec * 24 msec

PC4#traceroute 192.168.160.100
Type escape sequence to abort.
Tracing the route to 192.168.160.100
VRF info: (vrf in name/id, vrf out name/id)
1 192.168.50.21 6 msec 5 msec 4 msec
2 140.60.88.73 1 msec 1 msec 1 msec
3 172.31.10.10 [MPLS: Labels 17/24 Exp 0] 2 msec 7 msec 3 msec
4 172.31.10.34 [MPLS: Label 24 Exp 0] 3 msec 9 msec 8 msec
5 140.60.88.65 [MPLS: Label 23 Exp 0] 7 msec 8 msec 16 msec
6 66.171.14.9 [MPLS: Label 23 Exp 0] 7 msec 7 msec 7 msec
7 155.84.74.42 7 msec 9 msec 8 msec
8 155.84.74.41 15 msec 16 msec 16 msec
9 192.168.160.100 17 msec * 12 msec

R7
interface Ethernet0/0.95
mpls bdp forwarding

R3
no ip route 192.168.50.0 255.255.255.0 140.60.88.74
ip route vrf San-Francisco 192.168.50.0 255.255.255.0 140.60.88.74

vrf definition San-Francisco
address-family ipv4
route-target import 500:500
exit-address-family

R91
vrf definition San-Francisco
address-family ipv4
route-target import 64784:12
exit-address-family

R21
access-list 100 deny ip 192.168.30.0 0.0.0.255 any
access-list 100 permit ip any any
access-list 100 permit ip 192.168.30.0 0.0.0.255 any
access-list 100 permit ip any any
Incident#13

MPLS IPv4 Traceroute from R92 R96 and R97 sourced from each device Loopback 0 towards R93
Loopback 0 has stopped working
Fix the problem so that traceroute is successful
While you are resolving this issue, you are not allowed to create any new interfaces. Refer to the
Troubleshooting guidelines to determine if your solution is appropriate. Make sure that you
disconnected the telnet session after verification
This incident contains a single fault

R92#ping mpls ipv4 192.168.93.93/32 source 192.168.92.92 repeat 10
Sending 10, 100-byte MPLS Echos to 192.168.93.93/32,
timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, 'L' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'M' - FEC mismatch,
'M' - malformed request, 'N' - no label entry,
'P' - no rx intf label prot, 'R' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 32/106/137 ms

R96#ping mpls ipv4 192.168.93.93/32 source 192.168.96.96 repeat 10
Sending 10, 100-byte MPLS Echos to 192.168.93.93/32,
timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, 'L' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'M' - FEC mismatch,
'M' - malformed request, 'N' - no label entry,
'P' - no rx intf label prot, 'R' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 61/113/150 ms

R97#ping mpls ipv4 192.168.93.93/32 source 192.168.97.97 repeat 10
Sending 10, 100-byte MPLS Echos to 192.168.93.93/32,
timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, 'L' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'M' - FEC mismatch,
'M' - malformed request, 'N' - no label entry,
'P' – no rx intf label prot, 'p' – premature termination of LSP,
'R' – transit router, 'r' – unknown upstream index,
'X' – unknown return code, 'x' – return code 0
Type escape sequence to abort.

Success rate is 100 percent (10/10), round-trip min/avg/max = 82/122/163 ms

R92#traceroute mpls ipv4 192.168.93.93/32 source 192.168.92.92 ttl 100
Tracing MPLS Label Switched Path to 192.168.93.93/32, timeout is 2 seconds
Codes: '!' – success, 'Q' – request not sent, '.' – timeout,
'L' – labeled output interface, 'B' – unlabeled output interface,
'D' – DS Map mismatch, 'F' – no FEC mapping, 'f' – FEC mismatch,
'M' – malformed request, 'm' – unsupported tlv's, 'N' – no label entry,
'P' – no rx intf label prot, 'p' – premature termination of LSP,
'R' – transit router, 'r' – unknown upstream index,
'X' – unknown return code, 'x' – return code 0
Type escape sequence to abort.
0 86.191.16.10 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 86.191.16.9 36 ms

R96#traceroute mpls ipv4 192.168.93.93/32 source 192.168.96.96 ttl 100
Tracing MPLS Label Switched Path to 192.168.93.93/32, timeout is 2 seconds
Codes: '!' – success, 'Q' – request not sent, '.' – timeout,
'L' – labeled output interface, 'B' – unlabeled output interface,
'D' – DS Map mismatch, 'F' – no FEC mapping, 'f' – FEC mismatch,
'M' – malformed request, 'm' – unsupported tlv's, 'N' – no label entry,
'P' – no rx intf label prot, 'p' – premature termination of LSP,
'R' – transit router, 'r' – unknown upstream index,
'X' – unknown return code, 'x' – return code 0
Type escape sequence to abort.
0 86.191.16.5 MRU 1500 [Labels: 16 Exp: 0]
! 1 86.191.16.6 MRU 1504 [Labels: implicit-null Exp: 0] 23 ms
! 2 86.191.16.9 68 ms

R97#traceroute mpls ipv4 192.168.93.93/32 source 192.168.97.97
Tracing MPLS Label Switched Path to 192.168.93.93/32, timeout is 2 seconds
Codes: '!' – success, 'Q' – request not sent, '.' – timeout,
'L' – labeled output interface, 'B' – unlabeled output interface,
'D' – DS Map mismatch, 'F' – no FEC mapping, 'f' – FEC mismatch,
'M' – malformed request, 'm' – unsupported tlv's, 'N' – no label entry,
'P' – no rx intf label prot, 'p' – premature termination of LSP,
'R' – transit router, 'r' – unknown upstream index,
'X' – unknown return code, 'x' – return code 0
Type escape sequence to abort.
0 86.191.16.3 MRU 1500 [Labels: 16 Exp: 0]
! 1 86.191.16.6 MRU 1504 [Labels: implicit-null Exp: 0] 66 ms
! 2 86.191.16.9 27 ms

ip access-list extended 100
no 95 deny udp any any eq 3503
95 permit udp any any eq 3503
CCIEv5 Routing & Switching
Advanced Configuration Lab#5
Questions & Solutions - Incomplete

Coming Soon

Tom Mark Giembicki          Sean Draper
**LAB#5**

**Layer 2 Technologies**

**Section 1.1**

Configure London HQ Office network as per the following requirements:

- **Enable VTP Version 2 on SW1 SW2 SW3 SW4**
- **VTP domain must be set to CCIE**
- **VTP updates must be secured with MD5 of ASCII string “CCIErocks!”**
- **SW1 should be responsible for sending VTP updates throughout the domain**
- **SW2 SW3 and SW4 should be configured as VTP clients**
- **London HQ switches must retain VTP configuration after reboot**
- **Configure SW1 SW2 SW3 and SW4 to avoid unicast flooding for all the VLANs by retaining dynamic entries for 3 hrs before refresh**
- **SW1 and SW2 must have dot1q trunks that do not rely on negotiation however SW3 and SW4 should negotiate dot1q trunk on all relevant interface – see example output from SW3**
- **Do not configure any etherchannel**
- **Do not forget to allocate VLANs to Server1 and PC100**
- **SW3 and SW4 should be assigned MGMT VLAN IP Address 172.16.103.xx where X is the switch number**

At the end of this task you should have connectivity between all relevant SVIs and P2P links

Refer to the Main Diagram

```markdown
<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Native vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et2/1</td>
<td>desirable</td>
<td>n-802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et2/2</td>
<td>desirable</td>
<td>n-802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et2/3</td>
<td>desirable</td>
<td>n-802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
<tr>
<td>Et3/0</td>
<td>desirable</td>
<td>n-802.1q</td>
<td>trunking</td>
<td>1</td>
</tr>
</tbody>
</table>

Port | Vlans allowed on trunk
|-----|---------------- -------
| Et2/1 | 1-4094
| Et2/2 | 1-4094
| Et2/3 | 1-4094
| Et3/0 | 1-4094

Port | Vlans allowed and active in management domain
|-----|--------------------------------------
| Et2/1 | 1,12,100-102,111,201-202,501-502,999
| Et2/2 | 1,12,100-102,111,201-202,501-502,999
| Et2/3 | 1,12,100-102,111,201-202,501-502,999
| Et3/0 | 1,12,100-102,111,201-202,501-502,999
```
**Configuration:**

**SW1**

```
  vtp ver 2
  vtp dom CCIE
  vtp pass CCIErocks!!
  vtp mo ser

  mac address-table aging-time 7200

  interface range et 1/0 - 1 , et2/1 - 2 , et2/3 , et 3/0
  switchport trunk encapsulation dot1q
  switchport mode trunk

  interface Ethernet0/0
  switchport access vlan 101
  switchport mode access

  interface Ethernet0/1
  switchport access vlan 102
  switchport mode access

  interface Ethernet0/2
  switchport access vlan 12
  switchport mode access
```

**SW2**

```
  vtp ver 2
  vtp dom CCIE
  vtp pass CCIErocks!!
  vtp mo cli

  mac address-table aging-time 7200

  interface range et 1/0 - 1 , et2/2 - 3 , et3/0 - 1
  switchport trunk encapsulation dot1q
  switchport mode trunk

  interface Ethernet0/0
  switchport access vlan 202
  switchport mode access

  interface Ethernet0/1
  switchport access vlan 201
  switchport mode access

  interface Ethernet0/2
  switchport access vlan 12
  switchport mode access
```
Section 1.2

Configure London Remote Office and London DC site network as per the following requirements:

Enable VTP Version 2 on all switches
Use CCIE as the VTP domain
In the future there might be additional switches added to the network
SW6 and SW7 must not advertise their VLAN config but must forward VTP advertisement that they receive out their trunk ports
VTP updates must be secured with MD5 of ASCII string “CCIErocks!!?”

Configuration:

**SW6 – SW7**
- vtp version 2
- vtp domain CCIE
- vtp pass CCIErocks!!
- vtp mode transparent
Section 1.3

Configure India Cisco Reseller Office network as per the following requirements:

Enable VTP Version 3 on SW8
SW8 must be the primary switch for the VLAN database
Domain name should be set to CCIE
Configure VTP hidden password of CCIErocks!
Your solution must match below output on SW8

Configuration:

```
SW8#sh vtp status
VTP Version capable : 1 to 3
VTP version running  : 3
VTP Domain Name     : CCIE
VTP Pruning Mode    : Disabled
VTP Traps Generation: Disabled
Device ID           : aabb.cc00.1c00

Feature VLAN:
-------------------
VTP Operating Mode : Primary Server
Number of existing VLANs : 6
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision : 1
Primary ID           : aabb.cc00.1c00
Primary Description  : SW8
MD5 digest           : 0xE8 0x6F 0x89 0x20 0x53 0x95 0xA4 0x1C
                      0xA9 0x26 0x77 0x5A 0xEF 0xF0 0x38 0x12

Feature MST:
-------------
VTP Operating Mode : Transparent

Feature UNKNOWN:
----------------
VTP Operating Mode : Transparent
```

```
SW8
vtp domain CCIE
vtp version 3
vtp password CCIErocks!!
vtp primary vlan force
```
Section 1.4

Configure Service Provider Switch network as per the following requirements:

Most of the VLANs on SP-SW switch should already be pre-configured
Complete the config of all VLANs so that all relevant routers can ping their directly connected neighbors, see below ICMP test over the Sham Link R1 – R6
Ensure that the following unused ports are shutdown and configured as access ports in VLAN 999
- E2/0 – E2/3 are unused on SW-SP
- E3/0 – E3/3 are unused on SW-SP
- E0/2 are unused on SW-SP

R6#ping 192.168.16.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.16.0, timeout is 2 seconds:
!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms

Configuration:

**SW-SP**

```
vlan 999
  name UNUSED

interface Ethernet1/1
  switchport trunk encapsulation dot1q
  switchport mode trunk

int range et0/2 , et2/0 - 3 , et3/0-/ 3
  switchport mode access
  switchport access vlan 999
  shutdown
```
Section 1.5

Configure London HQ Office network as per the following requirements:

SW1 must be the root switch for all odd vlans and must be the backup for all even vlans
SW2 must be the root switch for all even vlans and must be the backup for all odd vlans
Explicitly configure the root and backup roles, assuming that other switches with default configuration may eventually be added in the network in the future
All switches must maintain one STP instance per vlan
Use the STP mode that has only three possible states
All access ports must immediately transition to the forwarding state upon link up and they must still participate in STP. Use single command per switch to enable this
Access ports must automatically shut down if they receive any BPDU and an administrator must still manually re-enable the port. Use a single command per switch to enable this feature

Configuration:

**SW1**
- spanning-tree mode rapid-pvst
- spanning-tree portfast default
- spanning-tree portfast bpduguard default
- spanning-tree vlan 1,101,111,201,501,999 root primary
- spanning-tree vlan 12,100,102,202,502 root secondary

**SW2**
- spanning-tree mode rapid-pvst
- spanning-tree portfast default
- spanning-tree portfast bpduguard default
- spanning-tree vlan 12,100,102,202,502 root primary
- spanning-tree vlan 1,101,111,201,501,999 root secondary

**SW3**
- spanning-tree mode rapid-pvst
- spanning-tree portfast default
- spanning-tree portfast bpduguard default

**SW4**
- spanning-tree mode rapid-pvst
- spanning-tree portfast default
- spanning-tree portfast bpduguard default
Section 1.6
Configure Global Telecom Service Provider Serial connections towards R2 and R3 as per the following requirements:

The WAN links must rely on a layer 2 protocol that supports link negotiation and authentication.
The Service Provider R90 expects both R2 and R3 to complete three way hand shake by providing the expected response of a challenge that is sent by R90.
R2 must use the username LONDON-R2 and password CCIE.
R3 must use the username INDIA-R3 and password CCIE.

Configuration:

- **R2**
  ```
  interface Serial1/0
  ppp chap hostname LONDON-R2
  ppp chap password CISCO
  ```

- **R3**
  ```
  interface Serial1/0
  encapsulation ppp
  ppp pap sent-username INDIA-R3 password CISCO
  ```

Section 1.7
Configure Global Telecom Service Provider Serial connection towards R1 as per the following requirements:

Ensure that minimum of 2 serial interfaces are required to make the multilink active.
Ensure that CDP is disabled on the connection.
R90 must require R1 to authenticate using CHAP.
Do not use PPP chap hostname on R1.
CHAP password should be “CCIE”.
Make sure that all CHAP passwords are not encrypted in the configuration.

Configuration:

- **R1**
  ```
  service password-encryption
  interface Serial1/0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
  ```

- **R1 (continued)**
  ```
  interface Serial1/0
  no ip address
  encapsulation ppp
  ppp multilink
  ppp multilink group 1
  ```
interface Multilink1
  ip address 145.67.189.1 255.255.255.252
  ppp chap password CISCO
  ppp multilink
  ppp multilink links minimum 2
  ppp multilink group 1
  no cdp enable

R90
  service password-encryption
  username R1 password CISCO

  interface Serial3/0
   no ip address
   encapsulation ppp
   ppp multilink
   ppp multilink group 1

  interface Serial4/0
   no ip address
   encapsulation ppp
   ppp multilink
   ppp multilink group 1

  interface Multilink1
   ip address 145.67.189.2 255.255.255.252
   ppp authentication chap
   ppp multilink
   ppp multilink links minimum 2 mandatory
   ppp multilink group 1
   no cdp enable

Section 1.8
Configure London HQ DHCP as per the following requirements:

Configure DHCP service on R2
Server1 and PC100 must always receive .150 IP address in the last IPv4 octet
Client-ID should be configured as the devices Ethernet interface
Both Server1 and PC100 should send their respective hostnames
DHCP assigned IP address should never expire
Only SW1 should forward DHCP request to Lo0 of R2
DHCP should be configured using the following parameters:

- DNS server 10.2.69.100
- Default gateway PC100 172.16.101.100 and Server1 172.16.102.100
- Infinite lease
- Both DHCP Pools must be named DHCP SERVER and DHCP PC respectively
- Domain Re-solution.london
**Configuration:**

**PC100**

```
interface Ethernet0/0
  ip address dhcp client-id Ethernet0/0 hostname PC100
```

**SERVER1**

```
interface Ethernet0/0
  ip address dhcp client-id Ethernet0/0 hostname SERVER1
```

**SW1**

```
interface Vlan501
  ip helper-address 172.16.2.2

interface Vlan502
  ip helper-address 172.16.2.2
```

**R2**

```
service dhcp

ip dhcp pool DHCP SERVER
  host 172.16.101.150 255.255.255.0
  client-identifier 01aa.bbcc.006e.00
  domain-name Re-solution.london
  default-router 172.16.101.100
  client-name SERVER1
  lease infinite

ip dhcp pool DHCP PC
  host 172.16.102.150 255.255.255.0
  client-identifier 01aa.bbcc.0064.00
  dns-server 10.2.69.100
  domain-name Re-solution.london
  default-router 172.16.102.100
  client-name PC100
```

**Section 1.9**

**Configure Global Telecom Service Provider Serial connection towards R1 as per the following requirements:**

Configure R91 as the PPPoE Server and R92 as the PPPoE Client
Ensure R92 always gets the same IP address XX.XX.120.18 from the PPPoE Server (X=subnet)
You are not allowed to use DHCP
Avoid unnecessary fragmentation on the PPPoE link
The link must be up even when there is no interesting traffic
R91 must authenticate using CHAP but R92 must not require R91 to authenticate
Use the device’s host name as CHAP username and CISCO as password
All password should appear in clear text in the configuration
Refer to the diagram
**Configuration:**

**R91**

username R92 password CISCO

bba-group pppoe CISCO
virtual-template 1

interface Ethernet0/2
  no ip address
  pppoe enable group CISCO

interface virtual-template 1
  ip address 172.31.120.17 255.255.255.248
  peer default ip address pool POOL
  ppp authentication chap

  ip local pool POOL 172.31.120.18

**R92**

interface Ethernet0/2
  no ip address
  pppoe enable
  pppoe-client dial-pool-number 1

interface dialer 1
  ip address negotiated
  mtu 1492
  encapsulation ppp
  dialer pool 1
dialer idle-timeout 0
dialer persistent
  ppp chap hostname R92
  ppp chap password CISCO
Layer 3 Technologies

Section 2.1

Configure OSPFv2 Area 0 in London HQ Office network according to the following requirements:

Configure the OSPF process ID to 200 and set the router ID to interface Lo0 on all OSPF devices

The interface Lo0 on each L3 devices must be seen as an internal OSPF prefix by all other routers

Ensure that OSPF is not running on any interface that is facing another AS

Use any method to accomplish this requirement

SW3 and SW4 must not participate in routing at all

Do not change the default OSPF cost of any interface in AS65100

R1 (Primary) and R2 (Backup) are the DMVPN hub routers, use the pre-config Tunnel 0

At the end of this task Server1 and PC100 should obtain their respective IP Addresses from R2 DHCP and have connectivity to any network within the London HQ OSPF Domain

Do not forget to advertise the back up link on R1

R1 must see the following OSPF routes in the routing table

```
R1#sh ip route ospf | be Gate
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 19 subnets, 3 masks
O 172.16.2.2/32 [110/11] via 172.16.100.18, 00:06:37, Ethernet0/3
O 172.16.11.11/32 [110/11] via 172.16.100.2, 00:19:49, Ethernet0/1
O 172.16.22.22/32 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.100.24/29 [110/11] via 172.16.100.2, 00:19:49, Ethernet0/1
O 172.16.100.32/29 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.100.40/29 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.110.10/24 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/1
O 172.16.101.0/24 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/1
O 172.16.110.10/24 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.110.20/24 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.110.30/24 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.103.8/29 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/1
O 172.16.103.16/29 [110/11] via 172.16.100.10, 00:19:59, Ethernet0/2
O 172.16.105.100/32 [110/11] via 172.16.100.10, 00:14:06, Ethernet0/2
```

```
FC100#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/5 ms

FC100#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/11 ms

SERVER1#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/15 ms

SERVER1#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/7 ms
```
Configuration:

**SW1**
router ospf 200  
router-id 172.16.11.11  
passive-interface default  
no passive-interface Vlan101  
no passive-interface Vlan111  
no passive-interface Vlan201  
network 0.0.0.0 255.255.255.255 area 0

**SW2**
router ospf 200  
router-id 172.16.22.22  
passive-interface default  
no passive-interface Vlan102  
no passive-interface Vlan111  
no passive-interface Vlan202  
network 0.0.0.0 255.255.255.255 area 0

**R1**
router ospf 200  
router-id 172.16.1.1  
passive-interface default  
no passive-interface Ethernet0/0  
no passive-interface Ethernet0/0.16  
no passive-interface Ethernet0/1  
no passive-interface Ethernet0/2  
no passive-interface Ethernet0/3  
network 10.251.1.0 0.0.0.255 area 0  
network 172.16.1.1 0.0.0.0 area 0  
network 172.16.100.0 0.0.0.7 area 0  
network 172.16.100.8 0.0.0.7 area 0  
network 172.16.100.16 0.0.0.7 area 0  
network 172.16.104.100 0.0.0.0 area 0  
network 192.168.16.0 0.0.0.1 area 0

**R2**
router ospf 200  
router-id 172.16.2.2  
passive-interface default  
no passive-interface Ethernet0/1  
no passive-interface Ethernet0/2  
no passive-interface Ethernet0/3  
network 10.251.1.0 0.0.0.255 area 0  
network 172.16.2.2 0.0.0.0 area 0  
network 172.16.100.16 0.0.0.7 area 0  
network 172.16.100.24 0.0.0.7 area 0  
network 172.16.100.32 0.0.0.7 area 0
Section 2.2

Configure OSPFv2 Area 0 in London Remote Office and London DC site network as per the following requirements:

Configure the OSPF process ID to 200 and set the router ID to interface Lo0 on all OSPF devices. The interface Lo0 on each L3 device must be seen as an internal OSPF prefix by all other routers. Ensure that OSPF is not running on any interface that is facing another AS. Use any method to accomplish this requirement.

SW6 and SW7 are L3 devices and must participate in OSPF routing. R5 and R6 are the DMVPN spoke routers, use the pre-config Tunnel 0.

Implement static default route towards the remote end ISP (Serial link) on R5 and R6.

At the end of this task London HQ and London Remote Office all devices should be able to communicate over the back up link.

Configuration:

R6

router ospf 200
router-id 10.2.6.6
passive-interface default
no passive-interface Ethernet0/0.16
no passive-interface Ethernet0/1
network 10.2.6.6 0.0.0.0 area 0
network 10.2.67.1 0.0.0.0 area 0
network 10.251.1.0 0.0.0.255 area 0
network 192.168.16.0 0.0.0.1 area 0
ip route 0.0.0.0 0.0.0.0 4.117.92.17

SW7

router ospf 200
router-id 10.2.77.77
passive-interface default
no passive-interface Vlan67
network 0.0.0.0 255.255.255.255 area 0

PC101

ip route 0.0.0.0 0.0.0.0 10.2.68.77

R5

router ospf 200
router-id 10.3.5.5
passive-interface default
no passive-interface Ethernet0/1
network 10.3.5.5 0.0.0.0 area 0
network 10.3.56.1 0.0.0.0 area 0
network 10.251.1.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 5.118.16.113

SW6

router ospf 200
router-id 10.3.66.66
passive-interface default
no passive-interface vlan 56
network 0.0.0.0 255.255.255.255 area 0
Section 2.3

Configure OSPFv2 in UK Digital Network Provider and Global Telecom Provider networks as per the following requirements:

Configure the OSPF process ID as specified within both provider infrastructures – see diagram
Set the router ID to interface Lo0 on all OSPF devices
The interface Lo0 on each L3 devices must be seen as an internal OSPF prefix by all other routers
Ensure that OSPF is not running on any interface that is facing another AS
Use any method to accomplish the requirement
Do not configure R94 as a stub area router, just make sure R94 won't be a transit router of the traffic
R94 is not source or destination
Advertise all Servers, Laptops and Users Loopback interfaces as shown in the diagram

Configuration:

R51
router ospf 100
router-id 192.168.124.51
passive-interface default
no passive-interface Ethernet0/1	network 192.168.123.6 0.0.0.0 area 0
network 192.168.124.51 0.0.0.0 area 0

R52
router ospf 100
router-id 192.168.124.52
passive-interface default
no passive-interface Ethernet0/1	network 192.168.123.2 0.0.0.0 area 0
network 192.168.124.52 0.0.0.0 area 0

R53
router ospf 100
router-id 192.168.124.53
passive-interface default
no passive-interface Ethernet0/0
no passive-interface Ethernet0/1
no passive-interface Ethernet0/2
network 0.0.0.0 255.255.255.255 area 0

R54
router ospf 100
router-id 192.168.124.54
passive-interface default
no passive-interface Ethernet0/0
no passive-interface Ethernet0/1
no passive-interface Ethernet0/2
network 0.0.0.0 255.255.255.255 area 0

R55
router ospf 100
router-id 192.168.124.55
passive-interface default
no passive-interface Ethernet0/1
network 192.168.123.14 0.0.0.0 area 0
network 192.168.124.55 0.0.0.0 area 0
R56
router ospf 100
  router-id 192.168.124.56
  passive-interface default
  no passive-interface Ethernet0/1
  network 192.168.123.18 0.0.0.0 area 0
  network 192.168.124.56 0.0.0.0 area 0

R90
router ospf 34782
  router-id 172.31.90.90
  passive-interface default
  no passive-interface Ethernet0/0
  no passive-interface Ethernet0/1
  network 172.31.90.90 0.0.0.0 area 0
  network 172.31.120.1 0.0.0.0 area 0
  network 172.31.120.9 0.0.0.0 area 0
  network 172.31.122.100 0.0.0.0 area 0

R91
router ospf 34782
  router-id 172.31.91.91
  passive-interface default
  no passive-interface Ethernet0/0
  no passive-interface Ethernet0/1
  no passive-interface Ethernet0/2
  no passive-interface Virtual-Template
  network 0.0.0.0 255.255.255.255 area 0

R92
router ospf 34782
  router-id 172.31.92.92
  passive-interface default
  no passive-interface Ethernet0/0
  no passive-interface Ethernet0/1
  no passive-interface Ethernet0/2
  no passive-interface Dialer1
  network 0.0.0.0 255.255.255.255 area 0

R93
router ospf 34782
  router-id 172.31.93.93
  passive-interface default
  no passive-interface Ethernet0/0
  no passive-interface Ethernet0/1
  network 172.31.93.93 0.0.0.0 area 0
  network 172.31.120.26 0.0.0.0 area 0
  network 172.31.120.41 0.0.0.0 area 17843

R94
router ospf 34782
  router-id 172.31.94.94
  max-metric router-lsa
  passive-interface default
  no passive-interface Ethernet0/0
  no passive-interface Ethernet0/1
  network 172.31.94.94 0.0.0.0 area 0
  network 172.31.120.34 0.0.0.0 area 0
  network 172.31.120.49 0.0.0.0 area 17843
  network 172.31.124.100 0.0.0.0 area 0
  network 172.31.125.100 0.0.0.0 area 17843
R95
router ospf 34782
  router-id 172.31.95.95
  passive-interface default
  no passive-interface Ethernet0/1
  no passive-interface Ethernet0/2
  network 172.31.95.95 0.0.0.0 area 17843
  network 172.31.120.42 0.0.0.0 area 17843
  network 172.31.120.58 0.0.0.0 area 17843

R96
router ospf 34782
  router-id 172.31.96.96
  passive-interface default
  no passive-interface Ethernet0/1
  no passive-interface Ethernet0/2
  network 172.31.96.96 0.0.0.0 area 17843
  network 172.31.120.50 0.0.0.0 area 17843
  network 172.31.120.57 0.0.0.0 area 17843
Section 2.4

Configure OSPFv2 in UK Voice Provider according to the following requirements:

Configure the OSPF process ID 145
Set the router ID to interface Lo0 on all OSPF devices
Ensure that OSPF is not running on any interface that is facing another AS
Do not use network statement or area 1711 statement anywhere in your configuration
Ensure OSPF networks are reachable across the domain from between all four routers
Refer to the diagram

Configuration:

R57
router ospf 145
  router-id 192.168.145.57
  interface Ethernet0/3
    ip ospf 145 area 0
  interface Loopback0
    ip ospf 145 area 0

R59
router ospf 145
  router-id 192.168.145.59
  area 354 virtual-link 192.168.145.61
  interface Ethernet0/0
    ip ospf 145 area 0
  interface Ethernet0/3
    ip ospf 145 area 354
  interface Loopback0
    ip ospf 145 area 354

R61
router ospf 145
  router-id 192.168.145.61
  area 354 virtual-link 192.168.145.59
  interface Ethernet0/1
    ip ospf 145 area 354
  interface Ethernet0/2
    ip address 192.168.145.30 255.255.255.252
    ip ospf 145 area 0.0.6.175
  interface Loopback0
    ip ospf 145 area 354

R62
router ospf 145
  router-id 192.168.145.62
  interface Ethernet1/0
    ip ospf 145 area 0.0.6.175
  interface Loopback0
    ip ospf 145 area 0.0.6.175
Section 2.5

Configure EIGRP for IPv4 in the India Cisco Reseller office according to the following requirements:

The EIGRP AS is 200
The interface Lo0 must be seen as an internal EIGRP prefix by all EIGRP devices
Ensure the EIGRP is not running on any interface that is facing another AS
Use EIGRP 64-bit version
Do not change the interface bandwidth on any physical interface
SW8 is a Layer 3 switch and must be also configured for EIGRP
Server 3 should be able to reach each device within India Cisco Reseller Office

**Configuration:**

**SW8**

```
router eigrp India-Cisco-Reseller
    address-family ipv4 unicast autonomous-system 200
    topology base
    exit-af-topology
    network 0.0.0.0
    eigrp router-id 10.1.88.88
    exit-address-family

interface Ethernet0/0
    switchport access vlan 601
    switchport mode access
```

**R3**

```
router eigrp India-Cisco-Reseller
    address-family ipv4 unicast autonomous-system 200
    topology base
    exit-af-topology
    network 10.1.3.3 0.0.0.0
    network 10.1.38.1 0.0.0.0
    eigrp router-id 10.1.3.3
    exit-address-family
```

**SERVER3**

```
ip route 0.0.0.0 0.0.0.0 10.1.39.88
```
Section 2.6

Configure EIGRP for IPv4 in the London DR site according to the following requirements:

The EIGRP AS is 200
The interface Lo0 must be seen as an internal EIGRP prefix by all EIGRP devices
The interface Lo100 (External User) must be seen as an external EIGRP prefix by all EIGRP devices
Do not use ACL or Prefix List for your solution
Use EIGRP 32-bit version
SW5 is a Layer 3 switches and must be also configured for EIGRP
Ensure the EIGRP is not running on any interface that is facing another AS
Use any method to accomplish this
Implement static default route towards the remote end ISP (Serial link) on R4

Configuration:

SW5

route-map LOOP10 permit 10
   match interface Loopback100
   set metric 10000 1 255 100 1500

router eigrp 200
   network 10.4.45.5 0.0.0.0
   network 10.4.46.5 0.0.0.0
   network 10.4.47.100 0.0.0.0
   network 10.4.55.55 0.0.0.0
   redistribute connected route-map LOOP10
   passive-interface default
   no passive-interface Ethernet0/0
   no passive-interface Ethernet0/1
   eigrp router-id 10.4.55.55

R4

router eigrp 200
   network 10.4.4.4 0.0.0.0
   network 10.4.45.1 0.0.0.0
   passive-interface default
   no passive-interface Ethernet0/1
   eigrp router-id 10.4.4.4

   ip route 0.0.0.0 0.0.0.0 2.81.106.193

PC102

interface Ethernet0/0
   ip address 10.4.46.100 255.255.255.0

   ip route 0.0.0.0 0.0.0.0 10.4.46.5
Section 2.7

Configure iBGP (12345) in UK Digital Network Provider network according to the following requirements:

All BGP routers must use their int Lo0 as their router-id
All BGP peerings must be established using Lo0 IP Address
Disable the default IPv4 unicast address family for peering session establishment in all BGP routers
Your solution should also carry future MPLS customer traffic
R53 and R54 must reflect prefixes from any PE to any other PE in AS 12345 for both AFs
Communities must be exchanged between the neighbours
Do not use peer groups or dynamic peering for your solution
BGP neighbour changes must be logged

**Configuration:**

**R51**

```
router bgp 12345
bgp router-id 192.168.124.51
bgp log-neighbor-changes
neighbor 192.168.124.53 remote-as 12345
neighbor 192.168.124.53 update-source Loopback0
neighbor 192.168.124.54 remote-as 12345
neighbor 192.168.124.54 update-source Loopback0

address-family ipv4
 neighbor 192.168.124.53 activate
 neighbor 192.168.124.53 send-community
 neighbor 192.168.124.54 activate
 neighbor 192.168.124.54 send-community
exit-address-family

address-family vpnv4
 neighbor 192.168.124.53 activate
 neighbor 192.168.124.53 send-community extended
 neighbor 192.168.124.54 activate
 neighbor 192.168.124.54 send-community extended
exit-address-family

ip bgp-community new-format
```

**R52**

```
router bgp 12345
bgp router-id 192.168.124.52
bgp log-neighbor-changes
neighbor 192.168.124.53 remote-as 12345
neighbor 192.168.124.53 update-source Loopback0
neighbor 192.168.124.54 remote-as 12345
neighbor 192.168.124.54 update-source Loopback0

address-family ipv4
 neighbor 192.168.124.53 activate
 neighbor 192.168.124.53 send-community
 neighbor 192.168.124.54 activate
 neighbor 192.168.124.54 send-community
exit-address-family

address-family vpnv4
 neighbor 192.168.124.53 activate
```
neighbor 192.168.124.53 send-community extended
neighbor 192.168.124.54 activate
neighbor 192.168.124.54 send-community extended
exit-address-family

ip bgp-community new-format

R53

router bgp 12345
  bgp router-id 192.168.124.53
  bgp cluster-id 192.168.124.53
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 192.168.124.51 remote-as 12345
  neighbor 192.168.124.51 update-source Loopback0
  neighbor 192.168.124.52 remote-as 12345
  neighbor 192.168.124.52 update-source Loopback0
  neighbor 192.168.124.54 remote-as 12345
  neighbor 192.168.124.54 update-source Loopback0
  neighbor 192.168.124.55 remote-as 12345
  neighbor 192.168.124.55 update-source Loopback0
  neighbor 192.168.124.56 remote-as 12345
  neighbor 192.168.124.56 update-source Loopback0

  address-family ipv4
  neighbor 192.168.124.51 activate
  neighbor 192.168.124.51 send-community
  neighbor 192.168.124.51 route-reflector-client
  neighbor 192.168.124.52 activate
  neighbor 192.168.124.52 send-community
  neighbor 192.168.124.52 route-reflector-client
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community
  neighbor 192.168.124.54 route-reflector-client
  neighbor 192.168.124.55 activate
  neighbor 192.168.124.55 send-community
  neighbor 192.168.124.55 route-reflector-client
  neighbor 192.168.124.56 activate
  neighbor 192.168.124.56 send-community
  neighbor 192.168.124.56 route-reflector-client
  exit-address-family

  address-family vpnv4
  neighbor 192.168.124.51 activate
  neighbor 192.168.124.51 send-community extended
  neighbor 192.168.124.51 route-reflector-client
  neighbor 192.168.124.52 activate
  neighbor 192.168.124.52 send-community extended
  neighbor 192.168.124.52 route-reflector-client
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community extended
  neighbor 192.168.124.54 route-reflector-client
  neighbor 192.168.124.55 activate
  neighbor 192.168.124.55 send-community extended
  neighbor 192.168.124.55 route-reflector-client
  neighbor 192.168.124.56 activate
  neighbor 192.168.124.56 send-community extended
  neighbor 192.168.124.56 route-reflector-client
  exit-address-family

ip bgp-community new-format
router bgp 12345
  bgp router-id 192.168.124.54
  bgp cluster-id 192.168.124.54
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 192.168.124.51 remote-as 12345
  neighbor 192.168.124.51 update-source Loopback0
  neighbor 192.168.124.52 remote-as 12345
  neighbor 192.168.124.52 update-source Loopback0
  neighbor 192.168.124.53 remote-as 12345
  neighbor 192.168.124.53 update-source Loopback0
  neighbor 192.168.124.55 remote-as 12345
  neighbor 192.168.124.55 update-source Loopback0
  neighbor 192.168.124.56 remote-as 12345
  neighbor 192.168.124.56 update-source Loopback0

address-family ipv4
  neighbor 192.168.124.51 activate
  neighbor 192.168.124.51 send-community
  neighbor 192.168.124.51 route-reflector-client
  neighbor 192.168.124.52 activate
  neighbor 192.168.124.52 send-community
  neighbor 192.168.124.52 route-reflector-client
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community
  neighbor 192.168.124.53 route-reflector-client
  neighbor 192.168.124.55 activate
  neighbor 192.168.124.55 send-community
  neighbor 192.168.124.55 route-reflector-client
  neighbor 192.168.124.56 activate
  neighbor 192.168.124.56 send-community
  neighbor 192.168.124.56 route-reflector-client

exit-address-family

address-family vpnv4
  neighbor 192.168.124.51 activate
  neighbor 192.168.124.51 send-community
  neighbor 192.168.124.51 route-reflector-client
  neighbor 192.168.124.52 activate
  neighbor 192.168.124.52 send-community
  neighbor 192.168.124.52 route-reflector-client
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community
  neighbor 192.168.124.53 route-reflector-client
  neighbor 192.168.124.55 activate
  neighbor 192.168.124.55 send-community
  neighbor 192.168.124.55 route-reflector-client
  neighbor 192.168.124.56 activate
  neighbor 192.168.124.56 send-community
  neighbor 192.168.124.56 route-reflector-client

exit-address-family

ip bgp-community new-format
router bgp 12345
  bgp router-id 192.168.124.55
  bgp log-neighbor-changes
  neighbor 192.168.124.53 remote-as 12345
  neighbor 192.168.124.53 update-source Loopback0
  neighbor 192.168.124.54 remote-as 12345
  neighbor 192.168.124.54 update-source Loopback0

  address-family ipv4
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community
  exit-address-family

  address-family vpnv4
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community extended
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community extended
  exit-address-family

  ip bgp-community new-format

R56

router bgp 12345
  bgp router-id 192.168.124.56
  bgp log-neighbor-changes
  neighbor 192.168.124.53 remote-as 12345
  neighbor 192.168.124.53 update-source Loopback0
  neighbor 192.168.124.54 remote-as 12345
  neighbor 192.168.124.54 update-source Loopback0

  address-family ipv4
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community
  exit-address-family

  address-family vpnv4
  neighbor 192.168.124.53 activate
  neighbor 192.168.124.53 send-community extended
  neighbor 192.168.124.54 activate
  neighbor 192.168.124.54 send-community extended
  exit-address-family

  ip bgp-community new-format
**Section 2.8**

Configure eBGP (12345) in UK Digital Network Provider network according to the following requirements:

R1 and R3 are the CE routers and use eBGP to connect to the manages services that are provided by the UK Digital Network Provider (12345) PE routers R51 and R52.
R1 and R3 BGP routers must use their int Lo0 as their router-id.
Do not disable the default IPv4 unicast address family on R1 or R3.
R1 must establish separate eBGP peerings with R51 on their P2P Global Connection.
R51 and R52 must advertise P2P Global Connections towards R1 and R3 into BGP.
R1 and R3 should only receive a default route from the SP routers and no other prefixes.
Use filter list for your solution.
R3 must appear as if it is coming from AS 65200.
Communities must be exchanged between the neighbours.
Refer to the diagram.

**Section 2.9**

Configure iBGP (10001) in Global Telecom Provider network according to the following requirements:

All BGP routers must use their int Lo0 as their router-id.
All BGP peerings should be configured using GTP peer group.
Disable the default IPv4 unicast address family for peering session establishment in all BGP routers.
R93 and R94 must be the IPv4 route-reflector for BGP AS10001.
No BGP speaker except for the edge routers R90, R95 and R96 must use network statement under the BGP router config at this point – advertise outside prefixes into BGP.
Ensure that all the BGP nexthop is never marked as unreachable as long as interface Lo0 of the remote peer is known via IGP.

**Section 2.10**

Configure eBGP between Global Telecom Provider and all other relevant AS’s:

Establish eBGP neighbourship between Global Telecom Provider (14567) and all remaining BGP Autonomous Systems – AS 20001 R97 should already be preconfigured.
R90 must advertise only a default route to R1 R2 and R3 for the Global BGP connection.
Do not use filter list for your solution.
R95 must be selected as the preferred exit point for traffic destined to remote AS’s.
R96 must selected as the next preferred exit in case R95 fails.
R1 and R2 should always prefer AS 10001 as their preferred exit point out to the internet and only chose AS 12345 if the connection towards AS 10001 fails. Do not configure any SP routers to accomplish this task.
Refer to the diagram.
Section 2.11
Configure iBGP within the UK Voice Provider environment according to the following requirements:

BGP AS 14567 is divided into three separate sub AS’s
Ensure that to the outside world UK Voice Provider appears to be a single AS
All BGP routers must use their int Lo0 as their router-id and to establish BGP peerings
Disable the default IPv4 unicast address family for peering session establishment in all BGP routers
No BGP speaker must use network statement under the BGP router config
Ensure that all the BGP nexthop is never marked as unreachable as long as interface Lo0 of the remote peer is known via IGP
All IP Addresses used for the peerings must pass the bgp’s directly connected check
Your solution should be ready to carry MPLS VPNv4 customer traffic
Configure all BGP peerings AF as per diagram

Section 2.12
Configure eBGP between the following BGP AS’s for AF IPv4 and VPNv4

R58 R60 R63 and Internet router R99 should already be partially pre-configured – see initial configs
R55 AS 12345 – R57 AS 14567
R56 AS 12345 – R58 AS 20058
R62 AS 14567 – Internet R99 AS 30000
R63 AS 20063 – Internet R99 AS 30000
R98 AS 30001 – Internet R99 AS 30000

R55 and R56 should advertise into BGP their outside prefixes
R98 should advertise all its prefixes into BGP. Do not use a network statement
There will be a lot of prefixes exchanged between the BGP peers
At the end of this task you should be able to ICMP ping between R1 R2 R3 R4 R5 and R6 Serial connections also reach any internet services Global DNS, NTP etc....

Section 2.13
eBGP Test between AS’s:

R1 should always route internet traffic via R90 unless the connection goes down. ICMP traffic should match exactly the traceroute output below towards the Global DNS 4.2.2.2:

R1#traceroute 4.2.2.2
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 145.67.189.2 [AS 10001] 8 msec 10 msec 10 msec
2 172.31.120.2 [AS 10001] 9 msec 10 msec 6 msec
3 172.31.120.26 [AS 10001] 18 msec 10 msec 9 msec
4 172.31.120.42 [AS 10001] 11 msec 9 msec 9 msec
5 197.56.6.69 [AS 10001] 10 msec 18 msec 9 msec
R90(config-if)#int mul 1
R90(config-if)#shut

R3 should always route internet traffic via R90 unless the connection goes down. ICMP traffic should
match exactly the traceroute output below towards the Global DNS 4.2.2.2:

R3#traceroute 4.2.2.2
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 137.56.78.2 [AS 12345] 2 msec 6 msec 3 msec
2 192.168.123.10 [AS 12345] 1 msec 1 msec 5 msec
3 192.168.123.10 [AS 12345] 1 msec 1 msec 5 msec
4 192.168.123.18 [AS 12345] 9 msec 6 msec 5 msec
5 9.4.107.26 [AS 12345] 10 msec 27 msec 12 msec
6 7.49.140.18 [AS 12345] 3 msec 2 msec 1 msec
7 85.59.197.42 [AS 12345] 1 msec 11 msec 6 msec
8 179.1.64.41 [AS 12345] 2 msec * 4 msec

R90(config)#int s 1/0
R90(config-if)#shu

R3#traceroute 4.2.2.2
Type escape sequence to abort.
Tracing the route to 4.2.2.2
VRF info: (vrf in name/id, vrf out name/id)
1 87.123.56.17 [AS 12345] 5 msec 5 msec 1 msec
2 192.168.123.10 [AS 12345] 5 msec 5 msec 1 msec
3 192.168.123.10 [AS 12345] 5 msec 12 msec 5 msec
4 192.168.123.18 [AS 12345] 1 msec 1 msec 5 msec
5 9.4.107.26 [AS 12345] 2 msec 1 msec 1 msec
6 7.49.140.18 [AS 12345] 2 msec 5 msec 1 msec
7 85.59.197.42 [AS 12345] 3 msec 2 msec 11 msec
8 179.1.64.41 [AS 12345] 2 msec * 3 msec
Section 2.14
Configure OSPFv3 in the Global Telecom Provider as per the following requirements:

Configure OSPF Process Id 100
Configure Loopback 0 as OSPF router id
R95 must be elected as DR on the connection with R96
R96 must be BDR and ready to take over R95
You are not allowed to use “ipv6 ospf 1 ared”
You are not allowed to use “ipv6 ospf 1 priority”
You are not allowed to use “ipv6 router” anywhere in your configuration
All Lo0 IPv6 Addresses should be reachable between the routers

Section 2.15
Configure BGP for IPv6 between the Global Telecom Provider and the AS 20001 as per the following requirements:

Establish eBGP peering between both BGP AS’s
Advertise IPv6 interfaces on R96 into BGP. Do not use network statement for this task
Configure your network such way that network admin behind R91 can communicate with Facebook server behind R97
Do not explicitly configure any static route or default route
Do not configure iBGP peerings within BGP AS 10001
Ensure that traffic redundancy is in place
Use the following ping to verify your config

R91#ping 2001:DB8:9797::97 so lo 10 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:DB8:9797::97, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:220::91
!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/5 ms

Section 2.16
Configure your network as per the following requirements:

R3 and R4 should only have a default static route towards the internet
Do not configure iBGP peerings within BGP AS 10001
Ensure R3 and R4 external Serial interfaces can communicate
Use the following ping to verify your config

R3#ping 2001:DB8:9704:497::194 re 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2001:DB8:9704:497::194, timeout is 2 seconds:
!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 18/19/23 ms

R3#traceroute 2001:DB8:9704:497::194
Type escape sequence to abort.
Tracing the route to 2001:DB8:9704:497::194
  1 2001:DB8:3390:3390::1 9 msec 10 msec 9 msec
  2 2001:DB8:9999:9999:25 10 msec 6 msec 9 msec
  3 2001:DB8:9193:9193:30 9 msec 10 msec 9 msec
  4 2001:DB8:9395:9395:1 9 msec 9 msec 9 msec
  5 2001:DB8:AAAA:9597::71 9 msec 9 msec 10 msec
  6 2001:DB8:9704:497::194 19 msec 20 msec 17 msec

Section 2.17
IPSec-protected tunnel must be set up between both CE routers R3 and R4 as per the following requirements:

Internal LAN IPv6 Addresses must be able to communicate over the public IPv6 network
The ISP routers have global IPv6 address and should have no knowledge about private subnets present on R3 and R4
IKE negotiations must be protected, each IKE negotiation should begin by agreement of both peers on a common (shared) IKE policy. This following policy security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated
  · The policy should be set to the smallest priority argument
  · Authenticate the tunnel using pre-shared key CCIEVPN
  · Module size for DH group calculation must be 1024bits
  · Use CCIEVSET as transform set name
  · Use CCIEVPOL as IPsec profile name
  · Use IPsec in tunnel mode
  · IPsec protocol ESP and algorithm AES with 128 bits

Finance User PC#1 - R12(LAN) should be able to ICMP to Multicast Receiver User PC#3 - R20 (LAN)
Server# ping 232.1.1.1
reply to request 0 from 10.2.19.1 3ms
reply to request 0 from 10.2.18.1 4ms

Note: The rsa-sig and rsa-encr keywords are not supported in IPv6
Section 2.18

Streaming server is connected directly to SW2. Receivers are located at the DMVPN spokes R5 and R6. Configure the London network as per the following requirements:

Only network segments with active receivers that explicitly require the data must receive the multicast traffic
Interface Lo0 of R1 must be configured as RP
Use a standard method of dynamically distributing the RP
Both R5 and R6 must participate in the multicast routing
To test configure interface Serial0/0 of both R5 and R6 to join group 232.1.1.1

Server# ping 232.1.1.1
reply to request 0 from 10.2.19.1 3ms
reply to request o from 10.2.18.1 4ms

VPN Technologies

Section 3.1

Configure MPLS L3 VPN according to the following requirements

The UK Digital Service Provider network (AS12345) (AS14567) (AS30000) (AS30001) (AS20058) (AS20060) (AS20063) use MPLS L3VPN in order to clearly separate remote site networks
The corporate security policies are centralized and enforced at the London HQ (AS 65100) for the three remote sites
Enable LDP only on required interfaces on the routers within UK Digital Service Provider and the UK Voice Provider
Use the interface Lo0 to establish LDP peerings
Ensure that no mpls interface that belongs to any router inside of AS12345 and AS14567 is visible on a trace route that originates outside of the AS.
END OF WORKBOOK

The creators would like to thank you for taking the time to go through this workbook. It is our hope that you have learnt the core technologies enough to feel confident going into your lab.

If you feel that you can help us improve on the content or have any questions then please get in touch with us.

Technical Verification and Support

For information regarding technical support or any questions please contact Tom Giembicki or Sean Draper using e-mail addresses below

E-Mail – tom.giembicki@gmail.com / sean.draper@gmail.com