**360RSW05-WKB-TA08**

# Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Exercise Workbook contains 20 challenging scenarios at the CCIE level that can be used for rigorous self-paced practice.

Each lab provides an extensive answer key, Mentor Guide support, and verification tables and is designed to maximize learning by providing practical experience. Also, self-paced learning resources such as the Cisco 360 CCIE R&S Reference Library and Cisco 360 CCIE R&S lessons supplement the Exercise Workbook scenarios.

**https://t.me/learningnets**

# Cisco 360 CCIE R&S Exercise Workbook Lab 8 Troubleshooting Section

COPYRIGHT 2013, CISCO SYSTEMS, INC. ALL RIGHTS RESERVED. ALL CONTENT AND MATERIALS, INCLUDING WITHOUT LIMITATION, RECORDINGS, COURSE MATERIALS, HANDOUTS AND PRESENTATIONS AVAILABLE ON THIS PAGE, ARE PROTECTED BY COPYRIGHT LAWS. THESE MATERIALS ARE LICENSED EXCLUSIVELY TO REGISTERED STUDENTS FOR THEIR INDIVIDUAL PARTICIPATION IN THE SUBJECT COURSE. DOWNLOADING THESE MATERIALS SIGNIFIES YOUR AGREEMENT TO THE FOLLOWING: (1) YOU ARE PERMITTED TO PRINT THESE MATERIALS ONLY ONCE, AND OTHERWISE MAY NOT REPRODUCE THESE MATERIALS IN ANY FORM, OR BY ANY MEANS, WITHOUT PRIOR WRITTEN PERMISSION FROM CISCO; AND (2) YOU ARE NOT PERMITTED TO SAVE ON ANY SYSTEM, MODIFY, DISTRIBUTE, REBROADCAST, PUBLISH, TRANSMIT, SHARE OR CREATE DERIVATIVE WORKS OF ANY OF THESE MATERIALS. IF YOU ARE NOT A REGISTERED STUDENT THAT HAS ACCEPTED THESE AND OTHER TERMS OUTLINED IN THE STUDENT AGREEMENT OR OTHERWISE AUTHORIZED BY CISCO, YOU ARE NOT AUTHORIZED TO ACCESS THESE MATERIALS.



https://t.me/learningnets

# Table of Contents






**https://t.me/learningnets**

# Activity Objectives

When performing any Practice Lab, it is recommended that you formulate a test-taking strategy that includes the following activities. Some of these activities should be conducted in the actual lab:

- Download the latest copy of a Practice Lab, then print it and read it carefully from beginning to end.
- Create a strategy for how to perform a Practice Lab.
- Draw diagrams if necessary.
- Create a checklist of general best practices to follow during the Practice Lab.
- Develop skill in finding issues in the lab so that you are able to uncover the hidden and complex internetworking issues.
- Carefully track your time so that you can develop good time-management techniques.
- Estimate the points that you have gained or lost to see where you are in your overall goal.

# General Lab Instructions

Read the following instructions carefully. It is important to remember that if you misinterpret any directions, you could lose points. After you have read the "General Lab Instructions" section, read through the entire lab and look for connections between the tasks. Pay close attention to the "Restrictions and Goals" section because the information may reduce the configuration options that are available to you.

- Your pod should be cabled according to the example in the "Ethernet Switched Cabling Topology" figure and the IPv4 diagram.
- Each router should have an initial IP configuration loaded.
- You should be able to access all devices on your learner virtual pod via Telnet.
- To begin, check the following base configuration for each router and switch:
  - Configure a hostname on each device.
  - If a DNS server is being used in your pod, disable the DNS lookups.
  - Familiarize yourself with any Cisco IOS Software shortcuts.
  - Remember that some Cisco IOS command parameters and regular expressions are case-sensitive.
- Verify the following information on each router and switch:
  - Determine the Cisco IOS Software versions that are being used for the routers and the virtual switches.
  - Verify that all the software on the routers and switches sees all physical interfaces.
- Review all the tasks in the scenario.

 © 2013 Cisco Systems, Inc.

https://t.me/learningnets

# Difficulty Levels

Tasks are categorized as follows:

- **Basic:** These fundamental tasks are generally those that are needed to provide the basic functions of the protocol or feature. You must complete these tasks to provide reachability and to move forward in the lab.
- **Intermediate:** These tasks include protocol features like routing optimization, route filtering, optimal path selection, load sharing, and summarization. Failure to complete these tasks will usually not affect later lab sections.
- **Advanced:** This category includes new Cisco IOS Software features and IP services, complex optimizations, and fine-tuning.

Scenarios are categorized as follows based on task classifications:

- Basic
- Basic to Intermediate
- Intermediate
- Intermediate to Advanced
- Advanced



https://t.me/learningnets

# Exercise Workbook Lab 8 Troubleshooting Section

## Grading and Duration

- Troubleshooting lab duration: 2 hours
- Troubleshooting lab maximum score: 24 points

**Note** You can assess your progress on the self-paced labs in this workbook by adding up the points that are assigned to sections and tasks. Consider taking the full Assessment Labs to assess your readiness level.

## Difficulty Level

- Difficulty: Intermediate

## Restrictions and Goals

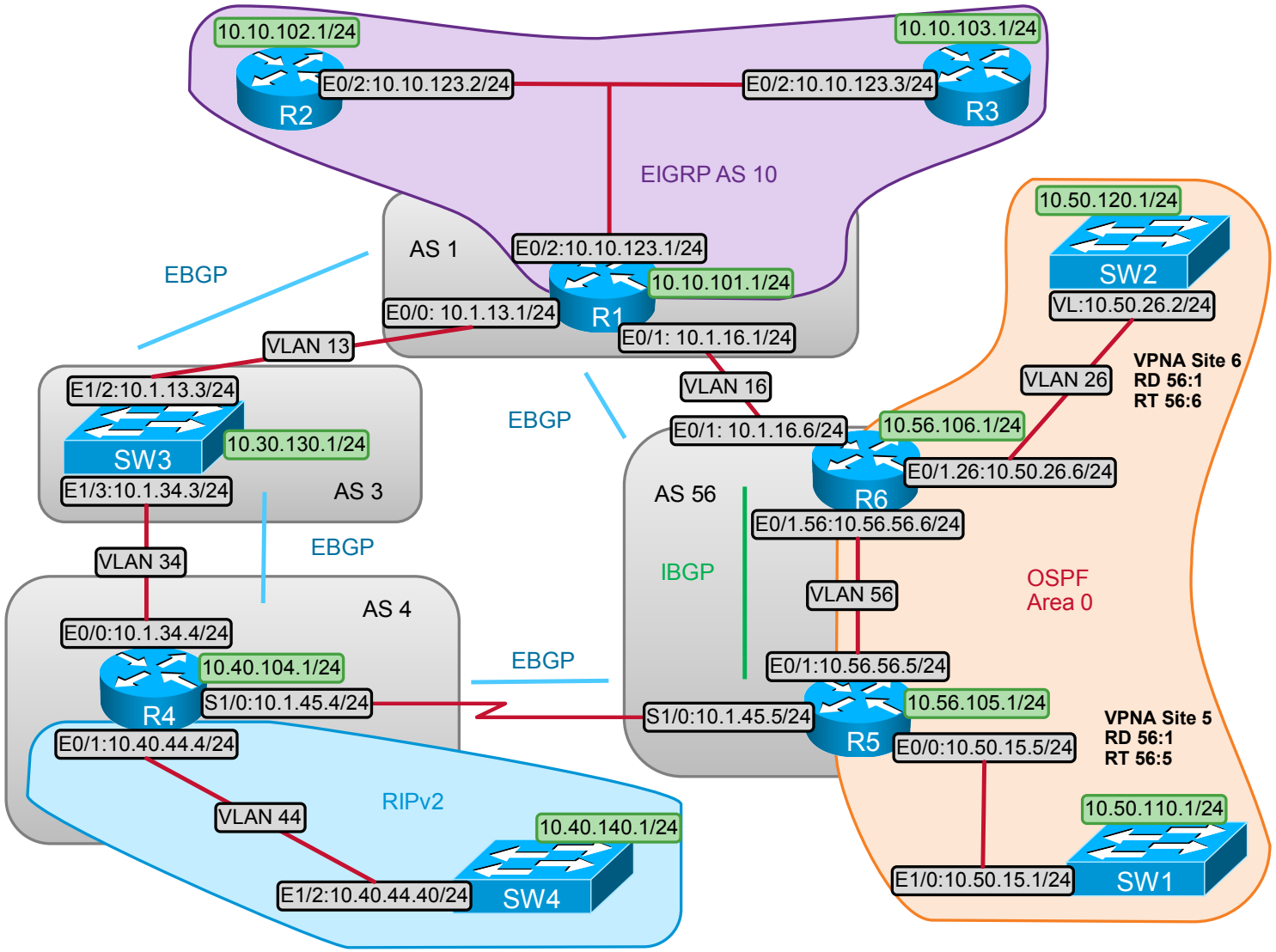
**Note** Read this section carefully.

- To receive credit for a subsection, you must fully complete the subsection per requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 10.0.0.0/8.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Do not use any static routes.
- Advertise loopback interfaces with their original masks.
- Prefixes displayed in routing tables must have mask lengths between /8 and /24, inclusive.
- Do not use the **ip default-gateway** or **ip default-network** commands.
- Do not introduce any new IP addresses.
- All IP addresses that are involved in this scenario must be reachable from within the same virtual routing and forwarding (VRF) instance. This lab does not require reachability between VPNA IP addresses and the remainder of the pod.
- Use conventional routing algorithms only, unless the instructions specify otherwise.
- Do not create new interfaces to fulfill IGP requirements, and do not summarize unless you are explicitly asked to do so.
- Do not modify the hostname, console, or vty configuration unless you are specifically asked to do so.
- Do not modify the initial interface or IP address numbering.

 © 2013 Cisco Systems, Inc.

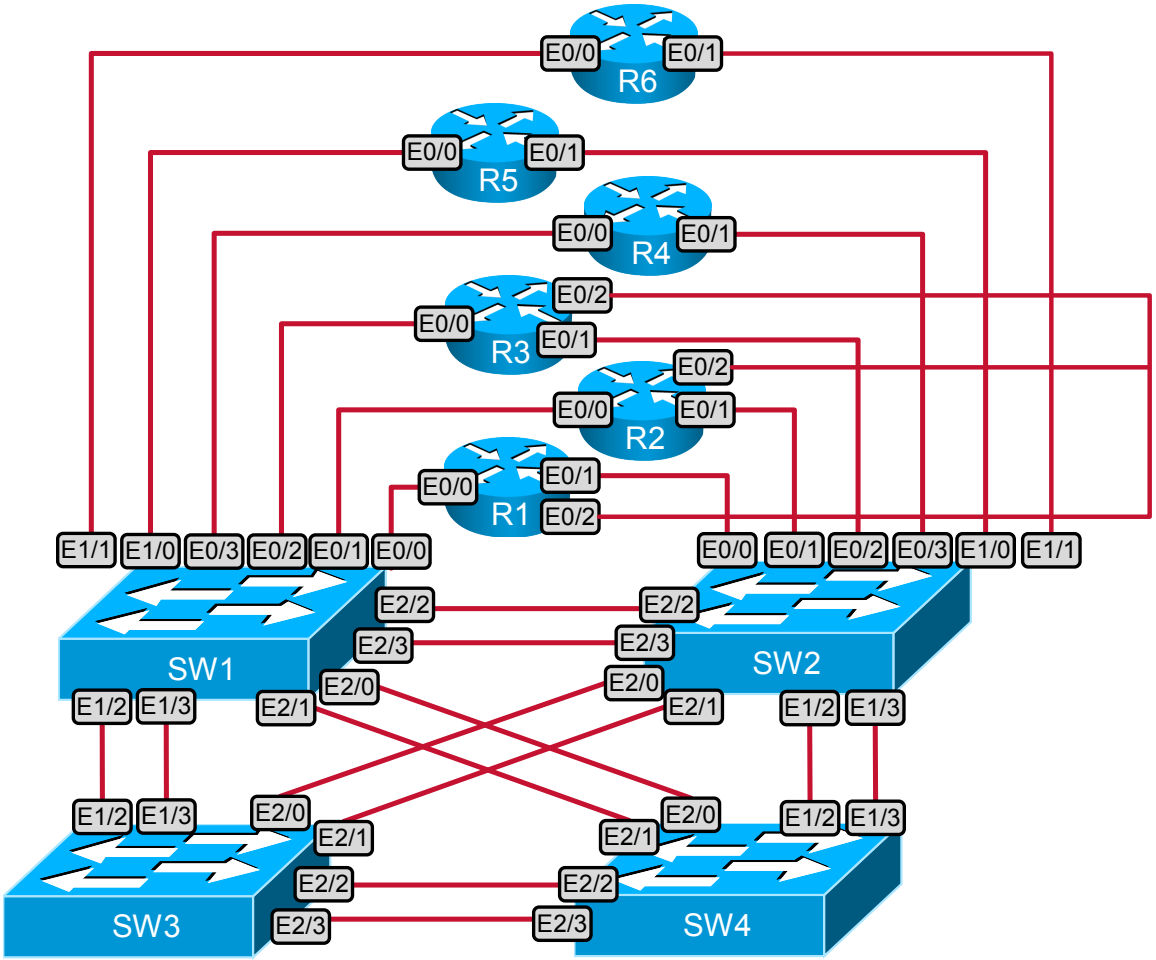
https://t.me/learningnets

# IPv4 IGP Diagram




https://t.me/learningnets

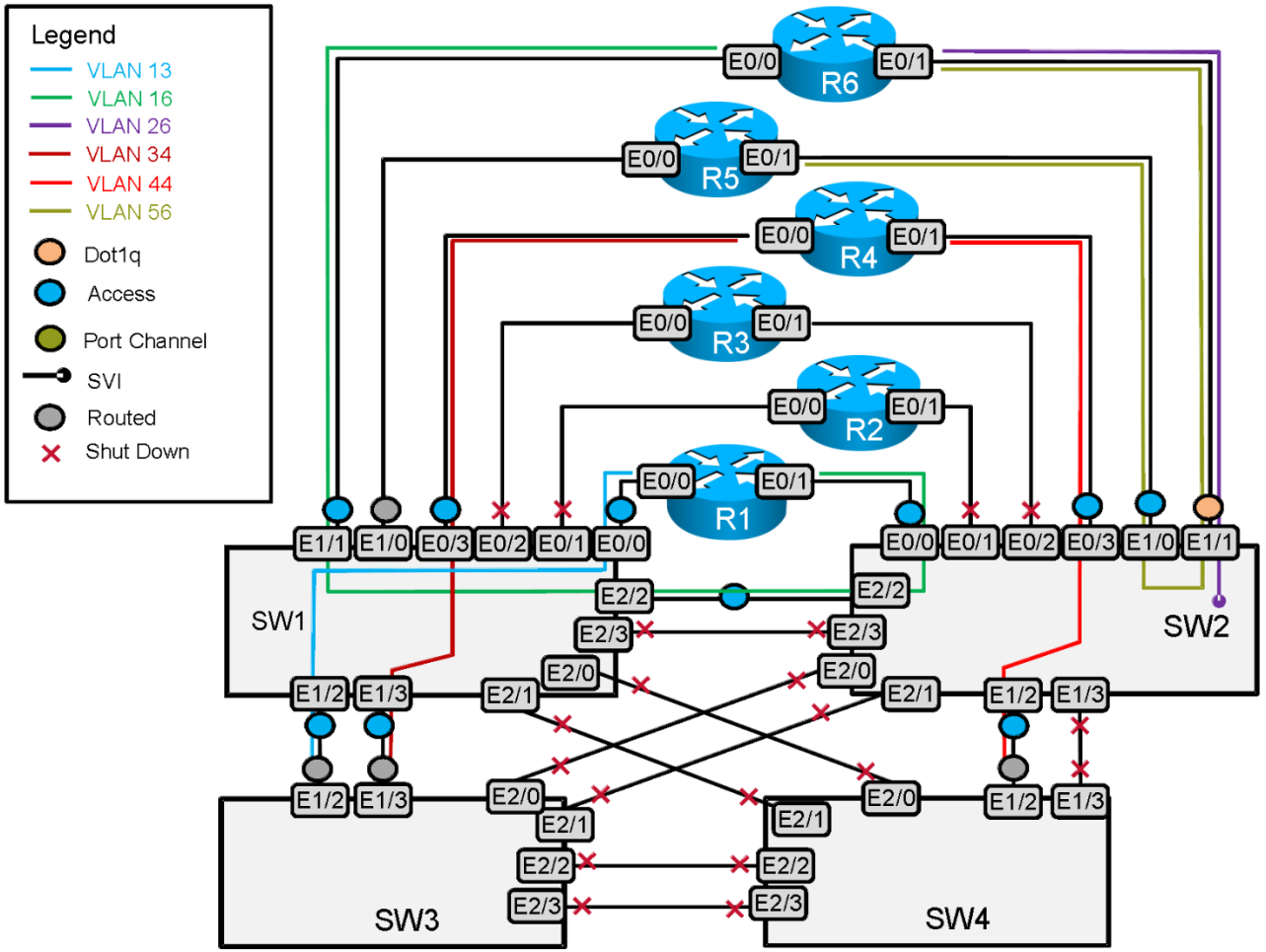
## Ethernet Switched Cabling Topology




 © 2013 Cisco Systems, Inc.

https://t.me/learningnets

## VLAN Propagation Diagram






https://t.me/learningnets

# 1. Switched Network Troubleshooting Section (Total: 3 points)

## 1.1. Troubleshooting Ticket

- Users reported that the switched network does not operate according to the requirements provided in the "Switched Network Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

## 1.2. Description of the Topology

- The switched Ethernet topology for this lab consists of six VLANs and routed interfaces, as shown in the "Ethernet Switched Cabling Topology" and IPv4 IGP diagrams. No additional VLANs or links may be configured or used.
- The link connecting R6 to SW2 is a dot1q trunk. All other switched interfaces are in access or routed mode.

## 1.3. Expected Behavior and Network Policies

- The Ethernet links that are shown in the "IPv4 IGP" diagram must support same-subnet reachability and the routing protocols shown.
- All switches must be in VTP transparent mode.

## 1.4. Special Goals and Restrictions

- Allow only traffic in the required VLANs to cross trunk links.
- Do not create or use any additional Ethernet interfaces. All links that are administratively down must remain so.

# 2. IPv4 EIGRP Troubleshooting Section (Total: 2 points)

## 2.1. Troubleshooting Ticket

- Users reported that the EIGRP routing domain does not operate according to the requirements provided in the "IPv4 EIGRP Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

## 2.2. Description of the Topology

- EIGRP AS 10 should operate exclusively on the links that are shown in the IPv4 IGP diagram. These include only the following:
  - 10.10.101.0/24
  - 10.10.123.0/24
  - 10.10.102.0/24
  - 10.10.103.0/24
- No other networks are internal to EIGRP.

## 2.3. Expected Behavior and Network Policies

- EIGRP must provide stable reachability between internal networks and reachability to required IPv4 addresses in the remainder of the pod.

https://t.me/learningnets

- R1, R2, and R3 must exchange only unicast EIGRP protocol packets. R2 and R3 may not exchange EIGRP protocol traffic. EIGRP should not advertise routes back out the interface it learned them on.

### 2.4. Special Goals and Restrictions

- There must be no EIGRP external routes in any routing table.

## 3. IPv4 RIP Troubleshooting Section (Total: 2 points)

### 3.1. Troubleshooting Ticket

- Users reported that the RIP routing domain does not operate according to the requirements provided in the "IPv4 RIP Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

### 3.2. Description of the Topology

- RIPv2 updates are exchanged between R4 and SW4 across VLAN 44.

### 3.3. Expected Behavior and Network Policies

- Each device sends only one route to the other.

### 3.4. Special Goals and Restrictions

- No configuration changes are permitted under either RIP process.

## 4. BGP Troubleshooting Section (Total: 3 points)

### 4.1. Troubleshooting Ticket

- Users reported that the IPv4 BGP routing domain does not operate according to the requirements provided in the "BGP Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

### 4.2. Description of the Topology

- BGP autonomous systems 1, 3, 4, and 56 are configured and peered as shown on the IPv4 IGP diagram and as described below.

### 4.3. Expected Behavior and Network Policies

- BGP provides reachability between EIGRP, RIP, and OSPF domains.

### 4.4. Special Goals and Restrictions

- All EBGP peering is between external, directly connected interfaces.
- The IBGP peering in AS 56 is between loopback interfaces.
- Do not alter configured unicast BGP policies.



https://t.me/learningnets

## 5. IPv4 Redistribution Troubleshooting Section (Total: 2 points)

### 5.1. Troubleshooting Ticket

- Users reported that the IPv4 IGP routing domain does not operate according to the requirements provided in the "IPv4 Redistribution Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

### 5.2. Description of the Topology

- Redistribute connected routes under all BGP processes.
- On R1, redistribute EIGRP 10 into BGP.
- On R4, redistribute RIP into BGP.

### 5.3. Expected Behavior and Network Policies

- Verify that all IP addresses are reachable, except for those on subnets of 10.50.0.0/16 in VPNA.

### 5.4. Special Goals and Restrictions

- Perform no additional redistribution unless specifically directed.

## 6. MPLS Layer 3 VPN Troubleshooting Section (Total: 4 points)

### 6.1. Troubleshooting Ticket

- Users reported that the MPLS Layer 3 VPN network does not operate according to the requirements provided in the "MPLS Layer 3 VPN Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

### 6.2. Description of the Topology

- OSPF for IPv4 is divided into three processes, as follows:
  - Process 0 on R5 and R6 includes only those links that are subnets of 10.56.0.0/16.
  - Process 50 on R5 and SW1 includes only subnets 10.50.15.0/25 and 10.50.110.0/24.
  - Process 60 on R6 and SW2 includes only subnets 10.50.26.0/24 and 10.50.120.0/24.
- Redistribute connected routes under all BGP processes.
- On R1, redistribute EIGRP 10 into BGP.
- On R4, redistribute RIP into BGP.

 © 2013 Cisco Systems, Inc.

https://t.me/learningnets

### 6.3. Expected Behavior and Network Policies

- SW1 and SW2 may have only connected, OSPF internal, and OSPF interarea routes. All routes in these tables must have /24 masks. No external routes are permitted in these routing tables.
- Verify that all IP addresses are reachable, except for those on subnets of 10.50.0.0/16 in VPNA.

### 6.4. Special Goals and Restrictions

- All VPNA IP addresses (which are all on subnets of 10.50.0.0/16) must be reachable from SW1 and SW2, R5 and R6.
- VPNA IP addresses are not required to reach any IP addresses outside VPNA.
- Perform no additional redistribution unless specifically directed.

## 7. Router Monitoring Troubleshooting Section (Total: 4 points)

### 7.1. Troubleshooting Ticket

- Users reported that router monitoring does not operate according to the requirements provided in the "Router Monitoring Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.

### 7.2. Description of the Topology

- R6 is configured with an Embedded Event Manager (EEM) policy to replace Loopback 106 if its protocol status goes down.

### 7.3. Expected Behavior and Network Policies

- If R6 Loopback 106 goes down, EEM should detect it and configure a loopback interface that duplicates its functions.
- If Loopback 106 goes down, all network protocols should continue to operate as if it was still up.

### 7.4. Special Goals and Restrictions

- If Loopback 106 goes down, the EEM process on R6 should source a syslog message reporting it at severity level 3.

## 8. IP Multicast Troubleshooting Section (Total: 4 points)

### 8.1. Troubleshooting Ticket

- Users reported that the multicast network does not operate according to the requirements provided in the "IP Multicast Troubleshooting" section.
- While resolving this ticket, refer to the "Description of the Topology," the "Expected Behavior and Network Policies," and the "Special Goals and Restrictions" subsections to determine if your solution is appropriate.



https://t.me/learningnets

### 8.2. Description of the Topology

- R1 should be a PIM neighbor with R2, R3, and SW3.
- R4 should be a PIM neighbor with SW3 and SW4.
- R1, SW3, and R4 are statically configured as PIM rendezvous points (RPs). In general, each RP should share source active (SA) information with the other RPs. See below for restrictions.
- The BGP peer relationships have been enabled for the IPv4 multicast address family.

### 8.3. Expected Behavior and Network Policies

- R1 should use the special multicast BGP route information to support reverse path forwarding (RPF) lookups for traffic sourced from subnet 10.40.140.0/24. R4 should use the special multicast BGP route information to support RPF lookups for traffic sourced from subnet 10.10.102.0/24. SW3 should use these special multicast BGP routes to support RPF lookups to either source subnet.
- R3, SW3, and R4 should respond to pings to IP address 224.1.1.1, whether these pings are sourced from IP address 10.10.102.1 or not.

### 8.4. Special Goals and Restrictions

- R5 is not part of multicast routing.

 © 2013 Cisco Systems, Inc.

https://t.me/learningnets