# Workbook Overview

Troubleshooting becomes integral part of the updated CCIE R&S lab exam. The new section is a group of loosely correlated trouble tickets. Every ticket has a point value associated with it, and the candidate must obtain 80% of the total section score in order to succeed in this section. Troubleshooting scenario uses a topology separate from the configuration part of the exam and has its own L2 configuration and IP addressing. Section grading is based on the automatic script along with a human hand to confirm the script results. From this information, one may conclude that mastering troubleshooting techniques becomes vital for succeeding in the new exam.

In this new IEWB-RS VOL4 workbook we present you with ten troubleshooting scenarios, each having ten trouble tickets. This amount should be approximately equal to the number of the troubleshooting tasks you will encounter in the actual exam. The topology used for every scenario is the same that we use for all our RS products, including VOL1 (technology-focused labs), VOL2 (configuration mock lab scenarios) and VOL3 (core technologies scenarios).

However, unlike our previous workbooks, we **restrict** access to some of the devices in the lab topology. For every scenario this “restricted” set may be different and it is clearly outlined in the scenario’s baseline. Using this technique we increase the scenario complexity by allowing candidates to see only “one” side of the problem. When looking at the lab diagram, you will clearly see routers not under your control as being displayed in orange color. Also, when you log onto the “restricted” device, it will warn you using a banner message.

In addition to the above restriction, we highly encourage you not using the **`show running-configuration`**, **`show startup-configuration`** commands or any other command that shows you the textual representation of the router’s configuration. This requirement makes you focus on using the show and debugging commands, which is invaluable when troubleshooting the real-world scenarios.

Our ultimate goal is not only prepare you for passing the Troubleshooting section of the CCIE R&S lab exam, but also to teach you a structured troubleshooting approach. As opposed to simple guessing and peeking at the routers running configurations you should learn using the debugging commands and interpreting various show commands output. For every ticket, we are going to follow the same structured procedure to resolve the issue. Here is an outline of this procedure:

1. Build and Analyze the Baseline
2. Analyze the Symptoms (propose hypothesis)
3. Isolate the issue (gather more symptoms)
4. Fix the Issue (by comparing to the Baseline)

We are now going to discuss all these steps in details to give you the basic understanding of the fundamental procedure.

# Structured Troubleshooting

## Build and Analyze the Baseline.

Since all tickets in a scenario share the same topology, you need to perform this step only once per the whole scenario. Baseline is essentially a picture of the healthy network, which serves as the starting point of any troubleshooting process. In real life, your baseline is the snapshot of your network under "normal" conditions – stable topology, interfaces under normal utilization, devices responding to management requests, users happy etc. In the lab, all you have is the diagram and possibly some additional network description. Additional information might be provided in the trouble ticket itself, but the initial starting point is the diagram.

We recommend making your own diagrams, including the following information:

- IP addressing + IGPs.
- Layer 2 topology.
- BGP diagram.
- IPv6 topology.
- Multicast and Redistribution diagram.

You may enhance your diagrams with any extra information provided, e.g. hints on the network pre-configuration and applications deployed, such as WWW, FTP, SMTP, VoIP and so on. This will help you analyzing symptoms later. You goal at this stage is to get clear picture of the network and discover any potential caveats. Try not using any IOS commands at this point, as this may consume your valuable time and add unneeded information. Overall, don't spend too much time building the baseline – the goal is to spend around 20 minutes. By the end of the baseline analysis phase, you should have clear understanding of the protocols and applications deployed in your network.

When you finished with building the baseline, take a quick look over all tickets in sequence. See if you can make any conclusions based on the ticket information, like marking the potentially broken links or missing information flows. Sometimes this may be obvious from the ticket text and give you extra

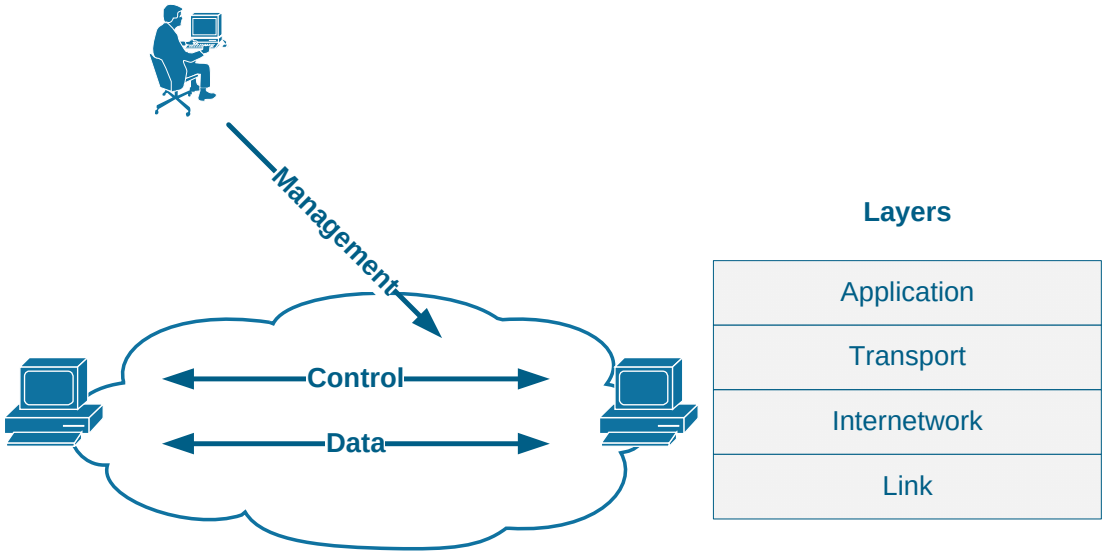
hint and help when dealing with other tickets.

## Analyze the Symptoms.

The ultimate goal of this step is coming up with the initial scope of the problem area and the initial set of hypothesis identifying the root cause. With respect to the CCIE lab, the primary source of the information is trouble ticket itself. The ticket might be formatted in a very simple manner, such as “there is an issue that prevents R1 from communicating with R2” or contain a detailed situation description, for example “at 10:00am this morning customers at Branch 1 site started complaining of poor HTTP performance. Analyzing the NOC action logs, you have noticed that someone was modifying R3’s configuration yesterday, but the change log entry is missing” and so on.

When trying to narrow the initial problem scope, it is helpful to use a reference network model, based on the classic TCP/IP protocol layers. The minimal working network consists of two communicating nodes and communication substrate connecting them. The substrate might be a direct link or a set of other nodes/routers. The network functions in three general planes: data, control and management. The first plane is responsible for forwarding data between the two endpoints, based on the programmed tables. The control plane is responsible for negotiating the data paths and establishing end-to-end connectivity. Example control plane protocols are OSPF, RIP, BGP and so on. The management plane is responsible for enforcing certain policy on the network and monitoring its performance. For example, SNMP and SSH used to carry CLI commands are both management protocols. All planes could be subdivided into four classic layers: Application, Transport, Internetwork and Link.




When analyzing the symptoms, you should select the network elements (e.g nodes, links) that you suspect to belong to the problematic area: e.g. routers on the path between two nodes failing to communicate. At the same time, you should mark the planes and the layers that you suspect to malfunction and possible identify the protocol names at every layer. You need to be aware of the symptoms typical for every layer and remember that an issue at lower layer affects all other overlying layers as well (cascading effect).

Lastly, the most helpful thing to identify the initial problematic area is finding

out what prior changes might have been made to the network, if this is mentioned in the ticket. Remember, every change is a potential problem!

## Isolate the issue.

The goal of this phase is finding the device/devices and the specific configuration area that might be causing the issue(s).This is the core of the troubleshooting process. You start verifying your initial hypothesis, by trying to narrow the problematic area as small as possible. To start with the process, you need to select either of the three approaches:

### Top-down approach

Test application layers across the path that you suspect to be causing the issues. Usually this approach works well when the issue lying in application misconfiguration (e.g. improper IMAP4 settings). This is very helpful in real-life scenarios; however, from the lab perspective this approach is not very useful as most issues will probably be related to the network configuration.

### Bottom-up approach

You start by testing physical layer issues of every node in the problematic area. If you don't find any issues, you proceed to the next layer (i.e. networking) and see if there are any deviations from the baseline there. This is the most universal approach, as it starts with the fundamental layer and moves up. However, executing bottom-up search might be routine and time consuming, and thus inappropriate for a small issue.

### Divide-and-Conquer approach

This method attempts to reduce the amount of work required by bottom-up search by making a "guess" – picking up the network layer that you suspect to be malfunctioning and testing the devices in the problematic area at this layer. It is common to start with the Internetwork layer and test end-to-end connectivity using the **`ping`** and **`traceroute`** commands. If this layer is healthy, then any underlying layer should be healthy as well, and you may continue searching in the "up" direction. Otherwise, using the above mentioned commands you may further isolate the problematic area and find the specific devices that might be causing the issue.

It is important to remember that during the issue isolating phase you will learn more information and may have to change your initial hypothesis, based on the results. Effectively, the Analyze and Isolate phases are deeply interconnected and depend on each other.

## Fix the Issue

At the end of the previous stage you should be dealing with the "hot" area of the problem – devices/links that are malfunctioning or improperly configured. Of course, you should have facts on hands to prove that your hypothesis/guess was valid. Your next step is developing a plan to resolve the problem. Resist the urge or simply going ahead and changing the running configuration – you may effectively introduce more issues then there originally was. Save the original configuration, and type in your "fixup" in the notepad.

Implement the “fixup” step by step – don’t apply changes to many devices at the same time, if you suspect many devices being affected After every change, run verifications to see if the issue has been eliminated or not.

When you’re done, compare the results to the baseline you have built at the first step. If everything seems to match and the symptoms outlined in the ticket no longer persist you may consider the ticket to be resolved. If not, you should re-analyze the initial symptoms and the additional information gathered during the previous steps. The last step could be named as “Verification” step.

# Workbook Solutions

Every solution document is formatted in structured manner to show you the flow of the actual troubleshooting process. You will find the sections corresponding to the in-depth analysis of the scenario baseline, diagram drawing and detailed step-by-step troubleshooting for every ticket presented in the scenario. Here is an outline for the solution document structure:

**Build and Analyze the Baseline**

Layer 2 Diagram.
BGP Diagram.
Multicast and Redistribution.
    Redistribution Loops Analysis.
    Multicast Propagation Analysis.
IPv6 Diagram
Read over the Lab

**Solutions**

Ticket 1
Analyze the Symptoms
Isolate the Issue
Fix the issue
Verify
...
Ticket 10
Analyze the Symptoms
Isolate the Issue
Fix the issue.
Verify

As you can see, the document follows the exact same path for the troubleshooting process that we outlined before. Every solution is about 50-60 pages long and provides enough details for every ticket, so that you’ll have plenty of material to learn from.

# IEWB-RS VOL4 Lab 1

## Lab Overview:

The following scenario is a practice lab exam designed to test your skills at troubleshooting Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco Systems' CCIE Routing & Switching Lab exam Troubleshooting Section. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab in order to resolve all issues, take the time to apply the structured troubleshooting methodology and improve your strategy.

## Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. For a current copy of these scripts, see the Internetwork Expert members' site at http://members.INE.com

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number. When not explicitly mentioned, a router's IP address on the segment is based off the router number, Y. For example, R1 will have the IP address of 150.X.100.1 on the subnet 150.X.100.0/24, and SW3 will have the IP address 150.X.100.9 on the same subnet.

Use the name **`cisco`** along with the password of **`cisco`** to access the console line of any device used in the topology.

## Lab Do's and Don'ts:

- Do not access the routers that are marked as restricted for your access.
- Do not use the **`show running-config`** or **`show startup-config`** commands or their equivalents when performing troubleshooting.
- Do not change or add any IP addresses from the initial configuration unless required for troubleshooting.
- Do not change any interface encapsulations unless required for troubleshooting.
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified.
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified.
- Save your configurations often.

## Grading:

This practice lab consists of 10 trouble tickets totaling 30 points. A score of 24 points is required to achieve a passing grade. A trouble ticket must be fixed 100% with the requirements given in order to be awarded the points for that ticket. No partial credit is awarded. If a ticket has multiple possible resolutions, choose the solution that best meets the requirements and requires minimal changes. Per the CCIE R&S lab exam requirements, you are required to finish this lab in **two** hours.

The tickets generally have no dependencies, unless explicitly stated in the ticket outline, so you may work through them in any order you like. It's up to you to select the tickets that you feel most easy to deal with and manage your time accordingly.

# GOOD LUCK!

# Baseline

All network devices are configured according to the diagram provided with this scenario. The diagram reflects the proper network configuration, including IP address, IGP protocol settings and BGP AS numbers and serves as your primary source of the information. This section provides the scenario-specific configuration information that you may need during troubleshooting process. Notice that not all of the information may be useful during the troubleshooting process; however, all statement made below reflect the correct network configuration.

## Devices under your Control

For this lab, you may only access and modify the configuration of the following devices: R1, R4, R5, R6, SW1 and SW2. Backbone devices BB1, BB2 and BB3 are out of your control per the initial topology configuration. If you refer to the diagram provided, the devices colored in **ORANGE** are out of your control.

## Bridging and Switching

- All switches use VTP domain name of CCIE.
- SW1 is VTP server, SW3 & SW4 are VTP clients and SW2 is in VTP transparent mode.
- L3 Etherchannels and point-to-point links are configured between the switches according to the diagram provided with the scenario.
- The following is the list of the trunk links interconnecting the switches
    - SW1 Fa0/14 to SW2 Fa0/14
    - SW2 Fa0/17 to SW3 Fa0/17
    - SW3 Fa0/19 to SW4 Fa0/19
- SW1 is the STP root bridge for all VLANs. Classic STP (PVST+) is in use.
- The Frame-Relay sub-interfaces of R2 and R3 are configured as point-to-point.

## IGP

- Mutual redistribution is configured between RIP and EIGRP on R6.
- Mutual redistribution is configured between OSPF and EIGRP on R3 and SW2.
- The Serial link between R4 and R5 is slow ISDN and should be used as a backup in the rare conditions of the Frame-Relay links failure.
- The network should not have any additional redistribution points.

- IPv6 is configured on the Frame-Relay links between R1 and R2, R2 and R3 as follows:
  - Network 2001:164:X:12::/64 between R1 and R2
  - Network 2001:164:X:23::/64 between R2 and R3
  - The PPP link between R1 and R3 uses the network 2001:164:X:13::/64.
- RIPng is used as IPv6 routing protocol between R1, R2 and R3.
- R1 prefers to reach R3's Loopback100 IPv6 subnet via R2.
- R2 uses point-to-point Frame-Relay sub-interfaces.

## BGP

- BGP peering sessions are configured according to the following table:

| Device 1 | Device 2 |
|---|---|
| R4 | BB3 |
| R4 | R3 |
| R3 | R1 |
| R3 | R2 |
| R1 | SW2 |
| R1 | R2 |
| R2 | R6 |
| R6 | BB2 |

- R6 and BB2 peering session is authenticated used the password value of "CISCO".
- AS 300 users cannot use AS 200 as transit to any other AS.
- AS 54 and AS 254 receive only a single summary route representing the whole 164.X.0.0 major subnet.

## Multicast

- IP multicast routing is enabled in R2, R3, R4 and SW1.
- PIM is enabled on the following networks:
  - Frame Relay segments between R2 & R3 and R3 & R4.
  - The Ethernet link between R4 and SW1.
  - The VLANs 26, 3, and 7 of R2, R3, and SW1 respectively.
- R3 is the RP for the following multicast groups:
  - 225.10.0.0 - 225.10.255.255
  - 225.26.0.0 - 255.26.255.255
  - 225.42.0.0 - 255.42.255.255

    - 225.58.0.0 - 255.58.255.255
- R4 is the RP for the following multicast groups:
    - 226.37.0.0 - 226.37.255.255
    - 226.45.0.0 - 226.45.255.255
    - 227.37.0.0 - 227.37.255.255
    - 227.45.0.0 - 227.45.255.255
- RP mapping is configured statically through the network.

## QoS

- Cisco Unified CallManager server is deployed on VLAN5 and users on VLAN 7 register their SIP phones with the server.
- The Frame-Relay links of R4 and R5 are provisioned at 256Kbps; All routers are configured for FRTS to accommodate this limitation.
- VoIP traffic is being given priority treatment over WAN links based the best-practice recommendations for low-speed links.

# Trouble Tickets

## Ticket 1: VoIP Quality

- You have received complaints from the users on VLAN7 using their Cisco IP Phones.
- The problem appears to be voice quality degradation when calling the HQ users residing on VLAN 5 subnet.
- According to the corporate QoS policy configuration everything should have been taken care of.
- You looked over the Frame-Relay links and found all of them uncongested.
- To make the problem even harder, users informed you that the voice quality is degraded only one way: from VLAN7 to the HQ.
- Based on the baseline information provide a solution to this problem.

**3 Points**

## Ticket 2: Load-Balancing

- Three switches: SW2, SW3 and SW4 were configured so that traffic from SW1 load-balances to VLAN9 across the links connecting SW2 to SW3 and SW4.
- However, recently you have found that only the path via SW4 is being utilized.
- Accessing the devices under your control only, return the network to the baseline and ensure proper load-balancing.

**3 Points**

## Ticket 3: BGP Peering

- After the security administrator of AS 300 has changed some “security settings” you found that BGP session between R1 and R3 is not coming up anymore. This is the message you keep seeing on your router’s console:

```
%BGP-3-NOTIFICATION: sent to neighbor 164.1.13.3 4/0 (hold time
expired) 0 bytes
```

- You have limited access to the remote router. So far, the only valuable piece of information you were able to get was the following:

```
Rack1R3#show ip bgp neighbors 164.1.13.1
BGP neighbor is 164.1.13.1,  remote AS 300, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = OpenSent
  Last read 00:01:34, last write 00:01:34, hold time is 180,
keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                 26          1
    Notifications:         23          0
    Updates:                0          0
    Keepalives:           157        156
    Route Refresh:          0          0
    Total:                206        157
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0/0
 Output queue size : 0
  Index 2, Offset 0, Mask 0x4
  2 update-group member
  Outbound path policy configured
  Outgoing update AS path filter list is 1
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Total:                              0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 1; dropped 1
```

```
  Last reset 01:25:07, due to BGP Notification sent, hold time
expired
  External BGP neighbor may be up to 1 hop away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 254, Outgoing
TTL 255
Local host: 164.1.13.3, Local port: 44156
Foreign host: 164.1.13.1, Foreign port: 179

Enqueued packets for retransmit: 1, input: 0  mis-ordered: 0 (0
bytes)

Event Timers (current time is 0xECDA36):
Timer          Starts    Wakeups            Next
Retrans             7          5        0xECFCDC
TimeWait            0          0             0x0
AckHold             0          0             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  263956977  snduna:  263956978  sndnxt:  263957023
sndwnd:  16384
irs: 1374337120  rcvnxt: 1374337121  rcvwnd:      16384
delrcvwnd:      0

SRTT: 37 ms, RTTO: 1837 ms, RTV: 1800 ms, KRTT: 58784 ms
minRTT: 20 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: active open, nagle
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 1 (out of order: 0), with data: 0, total data bytes: 0
Sent: 3 (retransmit: 5, fastretransmit: 0, partialack: 0, Second
Congestion: 0), with data: 1, total data bytes: 45
```

- You cannot reach the other admin via the phone, so it's up to you to use the information you have on hand to fix your side of the connection.

**4 Points**

## Ticket 4: Connectivity Issue

- Another ticket from VLAN7 users. They cannot reach any resource on VLAN 5 – all IP Phones have unregistered, and nothing else works.
- However, they are still able to reach the local resources.
- Using the baseline description as your reference, resolve this issue in optimal manner.

**3 Points**

## Ticket 5: Old Backup

- Accidental R6's power supply failure left you with no choice but quickly looking for a spare router.
- While preparing the new box you found that the latest router backup is dated 3 months old. It's about time to think of a change management system.
- However, for now you loaded the old backup file and now trying to find the missing parts of the puzzle.
- Your main goal is make all routers in EIGRP domain reach all RIP routes announced by BB1 and make sure BGP is working properly.

**3 Points**

## Ticket 6: BGP Prefixes

- Network administrator from AS 254 called you and complained that they cannot reach any of AS 54 prefixes.
- The administrator claims that AS 200 does not advertise these prefixes to AS 254.
- The problem seems to be related to your network configuration, so it's up to you to fix it.

**3 Points**

## Ticket 7: Security Improvement

- After the security administrator enabled "some" security feature for VLAN 55 users in SW3, the users rebooting their PC started complaining they cannot browse anything.
- You asked on the users to run the **`ipconfig /all`** command and figured that rebooted machines get an IP address in the range 169.254.0.0/16, while they should be auto configured via DHCP.
- The DHCP server is configured in R5 and used to work fine prior to the "security improvement".
- The security admin is out for lunch, and you only have a few minutes to fix the issue and cool down the upset users.

**3 Points**

## Ticket 8: BGP Peering

- After some IP configuration changes on VLAN18 you found that BGP peering sessions between R1 and SW2 is no longer active.
- You looked over the latest configuration changes but found nothing that could potentially affect BGP peering – no changes to BGP configuration, no change of IP addressing or new access-lists.
- Fix the problem so that BGP session works again. You are only allowed to change the configurations of R1 and SW2 for this task.

**3 Points**

## Ticket 9: IPv6

- IPv6 users behind R1 cannot reach the Loopback100 address of R3 anymore.
- Per the baseline, there is a primary and backup path, and there are no alarms signalizing any link problems.
- Accessing the router under you control, fix this issue.

**3 Points**

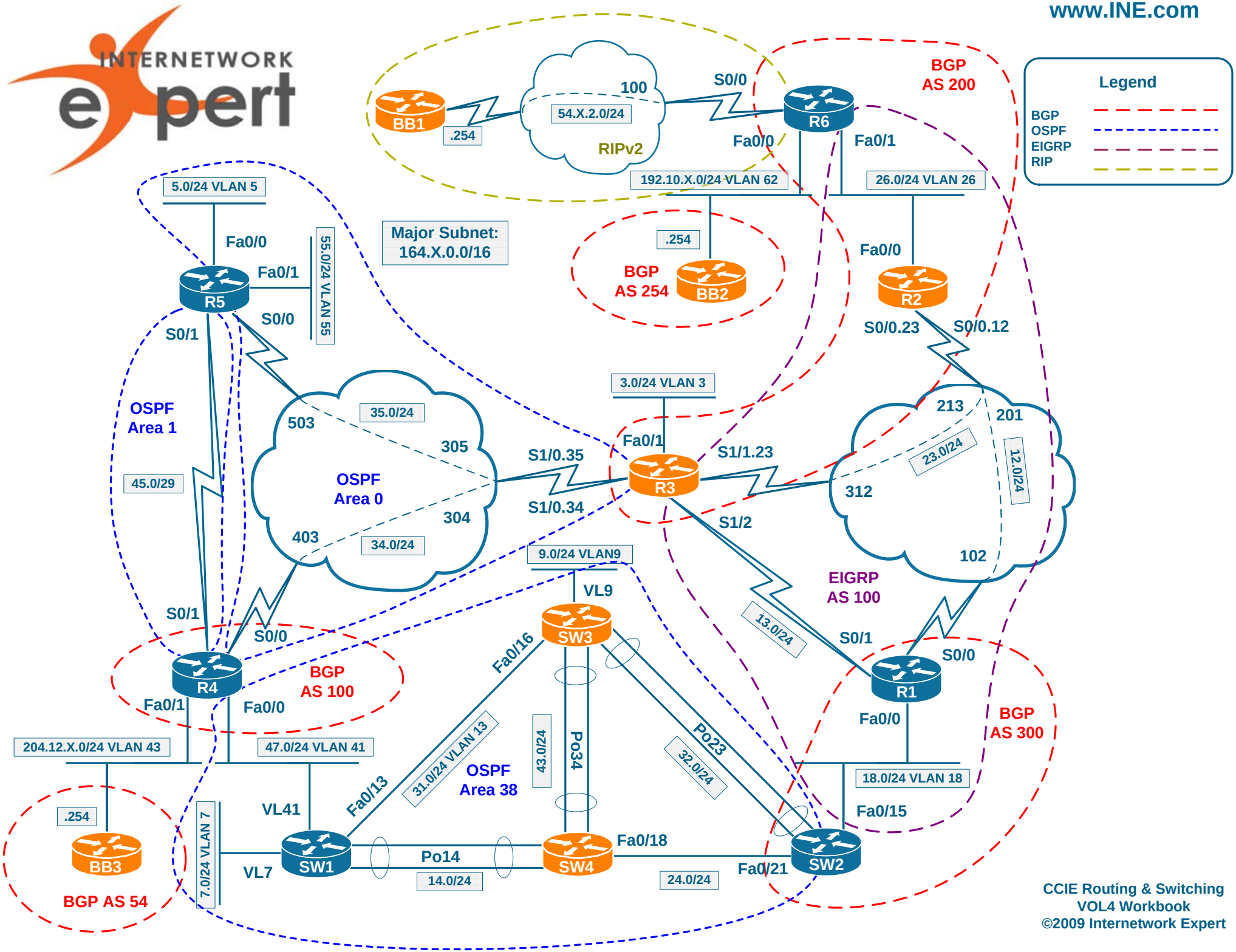
## Ticket 10: Multicast

*Note: Prior to starting with this ticket make sure you resolved Tickets 4 and 5*

- Users on VLAN 41 complain that they cannot receive video feeds from VLAN 26.
- You figured out what channel they are using and found that it maps to the multicast address 226.37.1.1.
- Fix the issue and make sure you can send multicast streams down from R6 to SW1.
- You may use ICMP traffic for testing, as it's open across the network.

**2 Points**


www.INE.com
INTERNETWORK
expert
Legend
BGP
OSPF
EIGRP
RIP
BB1
.254
100
54.X.2.0/24
RIPv2
S0/0
R6
BGP
AS 200
Fa0/0
Fa0/1
192.10.X.0/24 VLAN 62
26.0/24 VLAN 26
5.0/24 VLAN 5
Major Subnet:
164.X.0.0/16
.254
BGP
AS 254
BB2
Fa0/0
R2
S0/0.23
S0/0.12
Fa0/0
Fa0/1
55.0/24 VLAN 55
R5
S0/1
S0/0
3.0/24 VLAN 3
OSPF
Area 1
503
35.0/24
305
OSPF
Area 0
304
403
34.0/24
S1/0.35
S1/0.34
Fa0/1
R3
S1/1.23
S1/2
213
201
23.0/24
12.0/24
312
102
45.0/29
9.0/24 VLAN9
VL9
SW3
EIGRP
AS 100
13.0/24
S0/1
S0/0
R1
S0/1
S0/0
R4
BGP
AS 100
Fa0/1
Fa0/0
Fa0/0
BGP
AS 300
204.12.X.0/24 VLAN 43
47.0/24 VLAN 41
18.0/24 VLAN 18
Fa0/16
Fa0/13
31.0/24 VLAN 13
OSPF
Area 38
43.0/24
Po34
Po23
32.0/24
Fa0/15
.254
BB3
7.0/24 VLAN 7
VL41
VL7
SW1
Po14
14.0/24
SW4
Fa0/18
24.0/24
Fa0/21
SW2
BGP AS 54
CCIE Routing & Switching
VOL4 Workbook
©2009 Internetwork Expert

# IEWB-RS VOL4 Lab 1 Solutions

## Table of Contents



# Build and Analyze the Baseline

When you start with the scenario, all you have is the diagram and some textual information on the network baseline. Your goal at this moment is structuring the available information and making additional diagrams. We recommend extra diagrams to outline the following: L2 connection, BGP Peerings, Multicast & Redistribution and IPv6 Topology. Notice that some of these could be combined in a single diagram – for example you may put the Multicast and Redistribution outlines on the initial L3 diagram. This is probably the best way to save your time during the analysis stage. However, we are going to use separate diagrams for the ease of explanation here.