

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



CCNP Enterprise Hands-On Troubleshooting v2.0

Patrick Gargano, Lead Content Advocate
@PatrickGargano
LTRCRT-2002

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#LTRCRTC-2002>

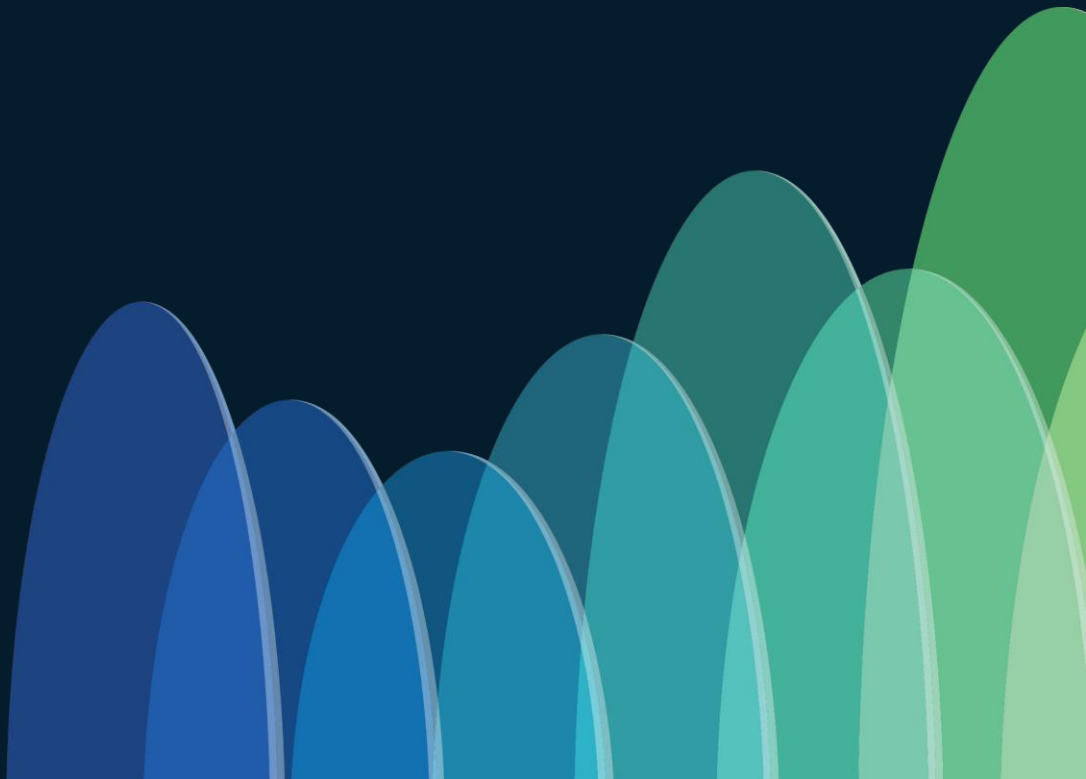




Agenda

- Introduction
- Lab Setup
- Troubleshooting Challenge
- Cisco Press Prizes
- Conclusion

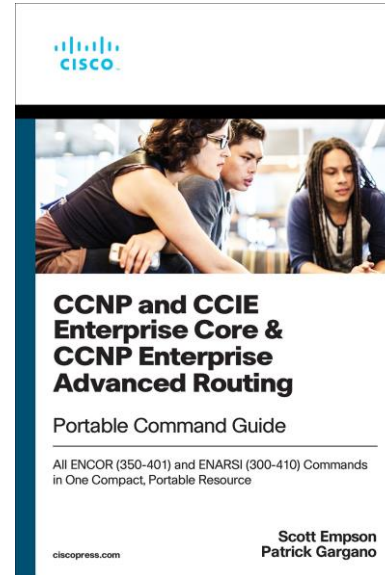
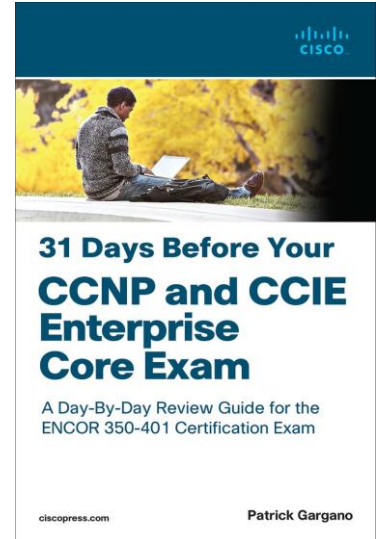
Introduction



Presenter

Patrick Gargano 🇨🇦

- Instructor and Lead Content Advocate with Learning & Certifications
- CCNP Enterprise (SD-WAN | Adv Routing | Cloud Connectivity | Design)
- CCNA CyberOps
- CCSI
- Cisco Networking Academy Instructor
- Cisco Press Author
- Cisco Live Distinguished Speaker



Housekeeping

- Restrooms
- Breaks/Drink – at your discretion (AM Beverage Service: 10:00 AM – 10:30 AM – Luxor Egyptian H)
- Session Survey

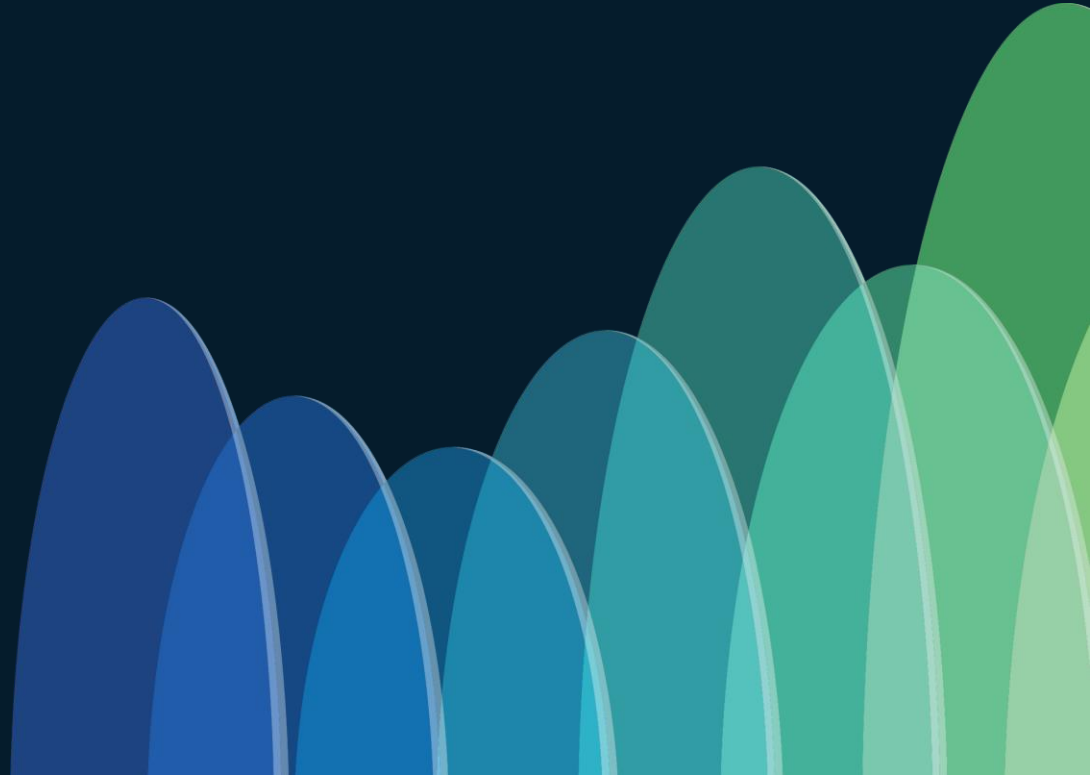
3) Please rate the above Instructor on the following:

Reachability for any questions during the Lab (troubleshooting , explanation etc..)

Technical Knowledge

*This session will make you
stronger at troubleshooting
network issues.*

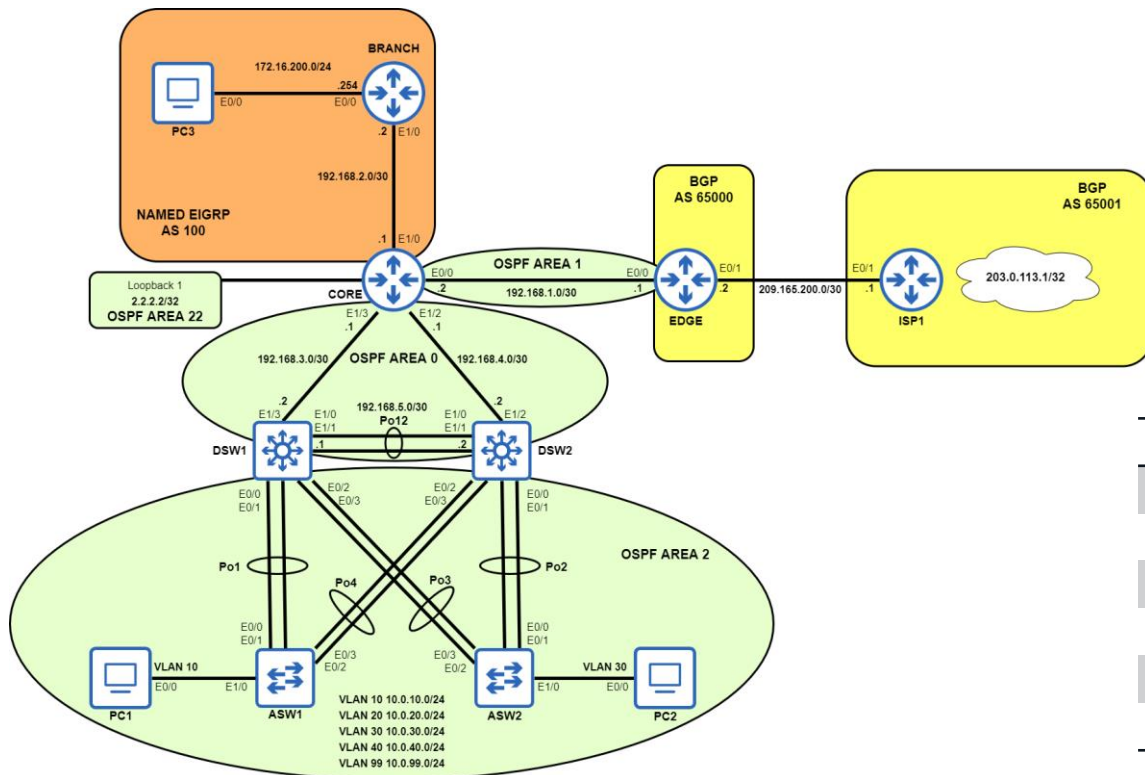
Lab Setup



Lab Overview

- 27 Trouble Tickets
- Similar to the legacy CCNP TSHOOT exam and ENARSI labs
 - Scenario-based
 - Issue has been logged
 - Confirm issue
 - Troubleshoot and fix
 - Document solution on answer sheet
 - Get answer validated by proctor or request a hint
- Prepares you for CCNP Enterprise ENCOR + ENARSI exams
- Stick around until the end for Cisco Press giveaways!

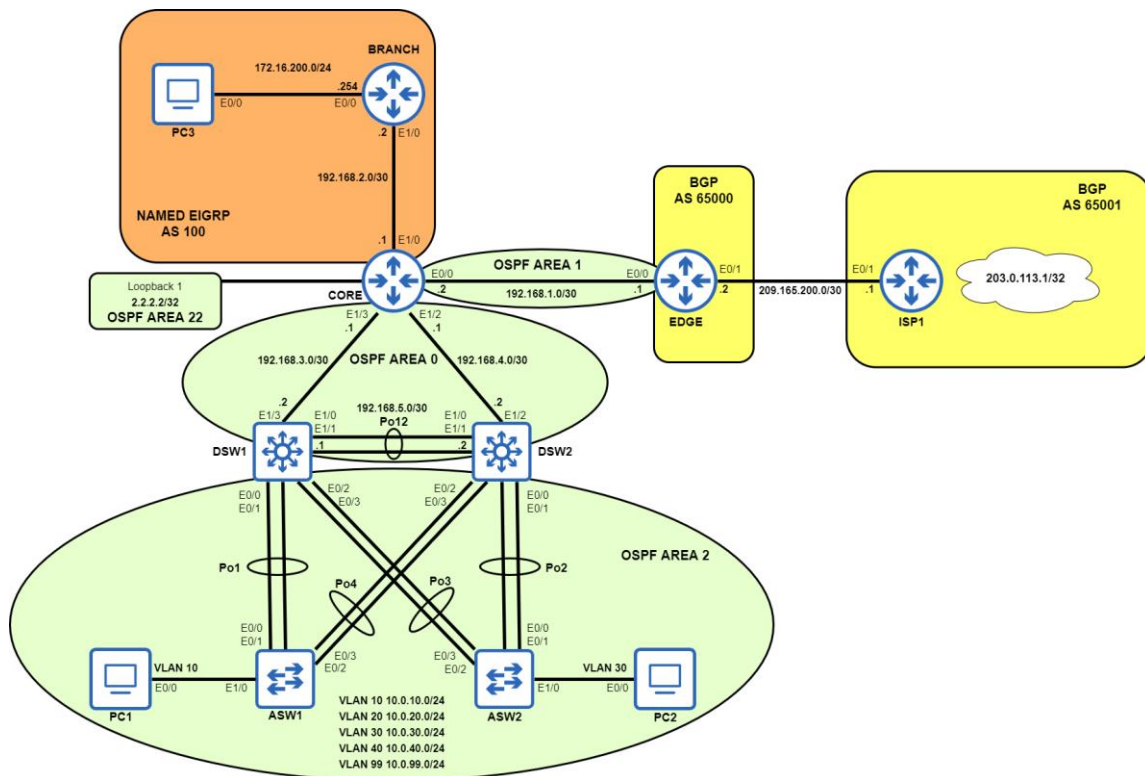
Lab Topology – IPv4 (Tickets 1-21)



RSTP		
VLAN	DSW1	DSW2
10	Root	Backup root
20	Root	Backup root
30	Backup root	Root
40	Backup root	Root
99	Root	Backup root

HSRPv2			
VLAN	DSW1	DSW2	Virtual IP
10	Active	Standby	10.0.10.254
20	Active	Standby	10.0.20.254
30	Standby	Active	10.0.30.254
40	Standby	Active	10.0.40.254
99	Active	Standby	10.0.99.254

Lab Topology – IPv4 (Tickets 1-21)

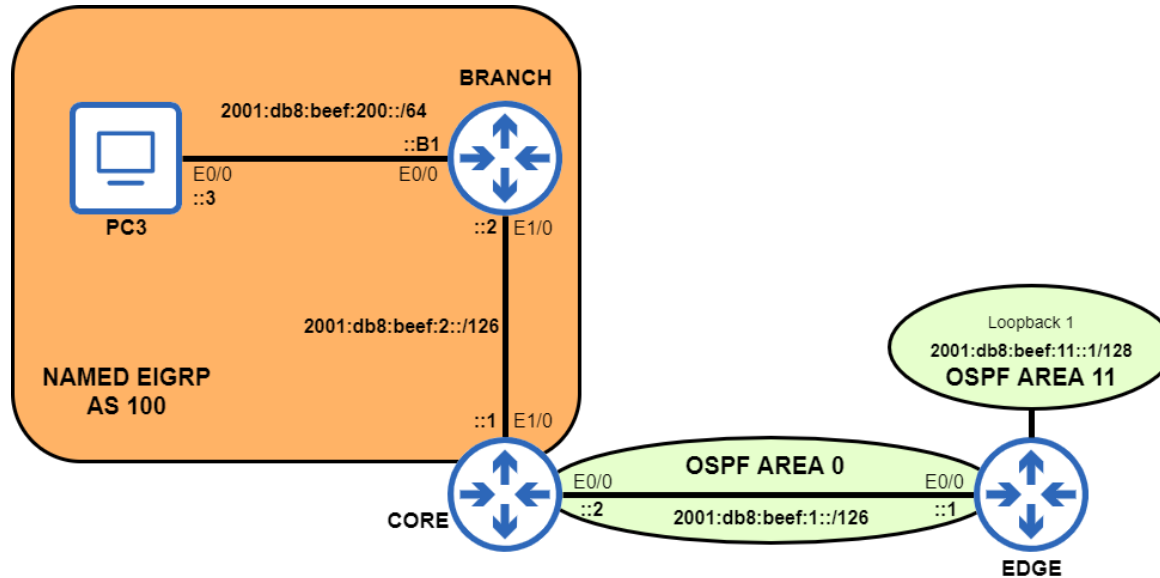


DHCP

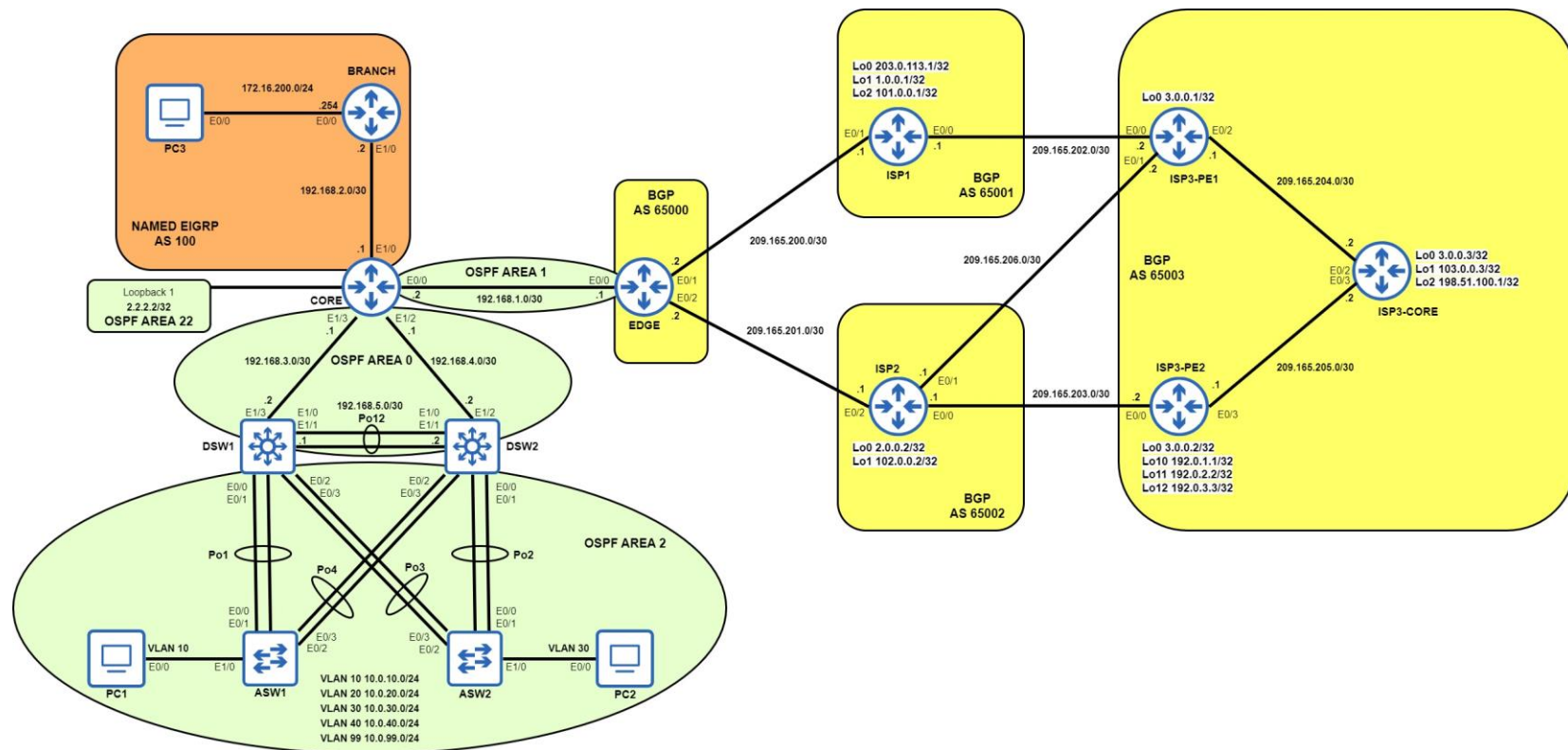
CORE (relay agent 2.2.2.2)

VLAN	Subnet	Gateway
10	10.0.10.0/24	10.0.10.254
20	10.0.20.0/24	10.0.20.254
30	10.0.30.0/24	10.0.30.254
40	10.0.40.0/24	10.0.40.254
BRANCH		
--	172.16.200.0/24	172.16.200.254

Lab Topology – IPv6 (Tickets 1-21)

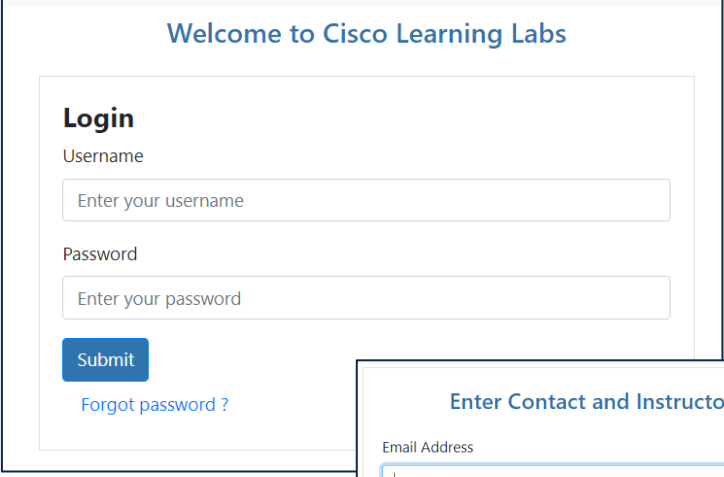


Advanced BGP Tickets (22 to 27)



Steps to Login

- <https://ccl-ng.cisco.com>
- Credentials
- Instructor Token: **medab**
- Click OK in the instructor popup
- Save your credentials for 90 days access!



>Welcome to Cisco Learning Labs

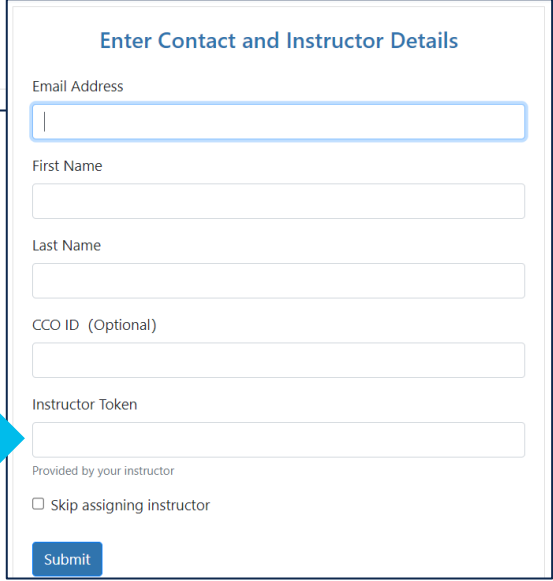
Login

Username

Password

Submit

[Forgot password ?](#)



Enter Contact and Instructor Details

Email Address

First Name

Last Name

CCO ID (Optional)

Instructor Token

Provided by your instructor

☐ Skip assigning instructor

Submit



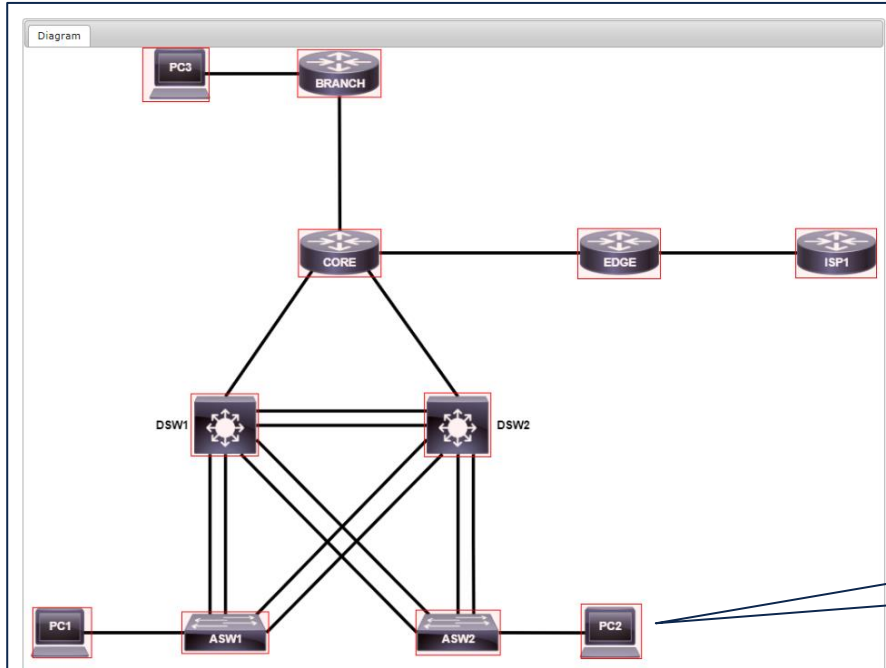
Lab Portal

The screenshot shows the Cisco Lab Portal interface. At the top, there is a blue header with the Cisco logo on the left and the user's account name 'c22tshoot-41-1' on the right. Below the header, the page is titled 'Lab List'. On the right side of the page, there are links for 'Refresh', 'Time Summary', 'Tools', 'Links', and 'Logout'. A 'TIP' box on the left states: 'Click on your account name in the upper-right hand corner of the screen to change your password or access preferences:'. On the right side, there is a dropdown menu for the user 'jsmith999' with options 'Change Password' and 'Preferences'. Below this, there is a table with two columns: 'Labname' and 'Status'. The table lists five labs, all with a status of 'Pending'. Each row has a green 'Start Lab' button. A large blue arrow points to the 'Start Lab' button for the first lab, 'Discovery 1: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 1'.

Labname	Status	Action
Discovery 1: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 1	Pending	Start Lab
Discovery 2: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 2	Pending	Start Lab
Discovery 3: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 3	Pending	Start Lab
Discovery 4: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 4	Pending	Start Lab
Discovery 5: CCNP Enterprise Hands-On Troubleshooting—Trouble Ticket 5	Pending	Start Lab

Lab Environment

[Introduction](#) [Guidelines](#) [Job Aid](#) [Trouble Ticket 1](#) [Manage Devices](#) [Help & Settings](#) ▾ [Exit](#)



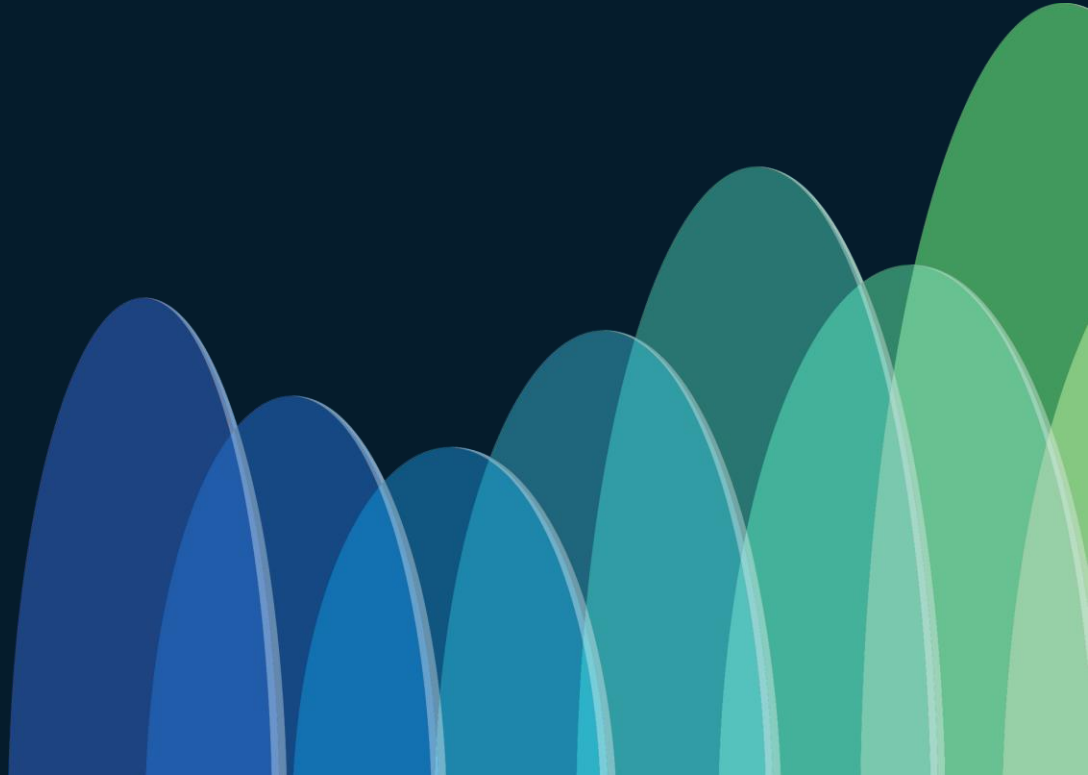
Note:

[Introduction](#), [Guidelines](#), and [Job Aid](#) are identical across all tickets.

Enable secret password: **cisco**

PCs are running IOS router image
no ip routing
ip default-gateway

Troubleshooting Challenge



Trouble Ticket #1

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1** cannot ping 203.0.113.1.

Trouble Ticket #2

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC3** cannot ping 203.0.113.1.

Trouble Ticket #3

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC2** cannot ping 203.0.113.1.

Trouble Ticket #4

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1** is taking a suboptimal path to reach 203.0.113.1.
- Fix the problem so that you can achieve the same output below:

```
PC1# traceroute 203.0.113.1
Type escape sequence to abort.
Tracing the route to 203.0.113.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.10.252 3 msec 4 msec 6 msec
 2 192.168.3.1 1 msec 1 msec 1 msec
 3 192.168.1.1 1 msec 1 msec 1 msec
 4 209.165.200.1 2 msec * 2 msec
```

Trouble Ticket #5

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1 and PC2** cannot reach 203.0.113.1.
- Fix the problem so that you can achieve the same output below:

```
PC1# traceroute 203.0.113.1
Type escape sequence to abort.
Tracing the route to 203.0.113.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.10.252 3 msec 4 msec 6 msec
 2 192.168.3.1 1 msec 1 msec 1 msec
 3 192.168.1.1 1 msec 1 msec 1 msec
 4 209.165.200.1 2 msec * 2 msec
```

```
PC2# traceroute 203.0.113.1
Type escape sequence to abort.
Tracing the route to 203.0.113.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.30.253 9 msec 1 msec 1 msec
 2 192.168.4.1 1 msec 1 msec 1 msec
 3 192.168.1.1 1 msec 1 msec 1 msec
 4 209.165.200.1 2 msec * 2 msec
```

Trouble Ticket #6

- Network requirements state that PC1 should be able to Telnet to all switches.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1** could no longer Telnet to all switches.
- Fix the problem so that you can achieve the same output below:

PC1# telnet 10.0.99.250 Trying 10.0.99.250 ... Open	PC1# telnet 10.0.99.251 Trying 10.0.99.251 ... Open	PC1# telnet 10.0.99.252 Trying 10.0.99.252 ... Open	PC1# telnet 10.0.99.253 Trying 10.0.99.253 .. Open
User Access Verification	User Access Verification	User Access Verification	User Access Verification
Username: admin Password:	Username: admin Password:	Username: admin Password:	Username: admin Password:
ASW2>	ASW2>	DSW1>	DSW2>

Trouble Ticket #7

- Network requirements state that PC1 should be able to use TFTP to copy the startup config file from all switches.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1** could no longer copy the startup-config file from all switches.
- Fix the problem so that you can achieve the same output below:

```
PC1# copy tftp://10.0.99.250/startup-config null:
Accessing tftp://10.0.99.250/startup-config...
Loading startup-config from 10.0.99.250 (via Ethernet0/0): !
[OK - 3494 bytes]
```

3494 bytes copied in 0.116 secs (30121 bytes/sec)

```
PC1# copy tftp://10.0.99.251/startup-config null:
Accessing tftp://10.0.99.251/startup-config...
Loading startup-config from 10.0.99.251 (via Ethernet0/0): !
[OK - 3536 bytes]
```

3536 bytes copied in 0.100 secs (35360 bytes/sec)

```
PC1# copy tftp://10.0.99.252/startup-config null:
Accessing tftp://10.0.99.252/startup-config...
Loading startup-config from 10.0.99.252 (via Ethernet0/0): !
[OK - 4719 bytes]
```

4719 bytes copied in 0.153 secs (30843 bytes/sec)

```
PC1# copy tftp://10.0.99.253/startup-config null:
Accessing tftp://10.0.99.253/startup-config...
Loading startup-config from 10.0.99.253 (via Ethernet0/0): !
[OK - 4670 bytes]
```

4670 bytes copied in 0.160 secs (29188 bytes/sec)

Trouble Ticket #8

- Network requirements state that PC2 should have access to the public address 203.0.113.1 via its default gateway DSW2.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that the **PC2** default gateway alternates intermittently between DSW1 and DSW2, as shown below (output may vary):

```
PC2# traceroute 203.0.113.1  
Type escape sequence to abort.  
Tracing the route to 203.0.113.1  
VRF info: (vrf in name/id, vrf out name/id)  
 1 10.0.30.252 3 msec 8 msec 1 msec  
 2 192.168.3.1 1 msec 1 msec 1 msec  
 3 192.168.1.1 1 msec 1 msec 1 msec  
 4 209.165.200.1 2 msec * 2 msec
```

```
PC2# traceroute 203.0.113.1  
Type escape sequence to abort.  
Tracing the route to 203.0.113.1  
VRF info: (vrf in name/id, vrf out name/id)  
 1 10.0.30.253 4 msec 6 msec 11 msec  
 2 192.168.4.1 1 msec 1 msec 1 msec  
 3 192.168.1.1 1 msec 1 msec 1 msec  
 4 209.165.200.1 1 msec * 2 msec
```

- Fix the problem so that you can consistently achieve the output shown on the right.

Trouble Ticket #9

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC2** cannot ping 203.0.113.1.

Trouble Ticket #10

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1** cannot ping 203.0.113.1.

Trouble Ticket #11

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC3** cannot ping 203.0.113.1.

Trouble Ticket #12

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1 and PC2** cannot ping 203.0.113.1.

Trouble Ticket #13

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1, PC2 and PC3** cannot ping 203.0.113.1.

Trouble Ticket #14

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC3** cannot ping 203.0.113.1.

Trouble Ticket #15

- **NOTE:** Please let proctor know when you start this ticket.
- Network requirements state that PC3 should have access to all OSPF IPv6 prefixes.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC3** cannot ping all OSPF IPv6 prefixes.
- Fix the problem so that you can achieve the same output below:

```
PC3# ping 2001:db8:beef:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:BEEF:1::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/37 ms
```

```
PC3# ping 2001:db8:beef:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:BEEF:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
PC3# ping 2001:db8:beef:11::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:BEEF:11::1,
timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 1/1/1 ms
PC3#
```

Trouble Ticket #16

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1, PC2, and PC3** cannot ping 203.0.113.1.

Trouble Ticket #17

- Network requirements specify clear IPv4 and IPv6 routing protocol boundaries.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that the routing boundary on CORE is no longer being observed.
- Fix the problem so that you can achieve the same output below:

```
CORE# show ospfv3 interface brief
```

Interface	PID	Area	AF	Cost	State	Nbrs	F/C
Et0/0	1	0	ipv6	1000	DR	1/1	

```
CORE# show ipv6 eigrp interfaces
```

```
EIGRP-IPv6 VR(EXAM) Address-Family Interfaces for AS(100)
```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Et1/0	1	0/0	0/0	6	0/2	50	0

Trouble Ticket #18

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC2** cannot ping 203.0.113.1.

Trouble Ticket #19

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC3** cannot ping 203.0.113.1.

Trouble Ticket #20

- Network requirements specify that static routing to 203.0.113.1/32 is configured on BRANCH.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that static routing to 203.0.113.1/32 configured on BRANCH is no longer functional.
- Fix the problem so that you can achieve the same output below:

```
BRANCH# show ip route
Gateway of last resort is 192.168.2.1 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/1536000] via 192.168.2.1, 00:20:12, Ethernet1/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.200.0/24 is directly connected, Ethernet0/0
L       172.16.200.254/32 is directly connected, Ethernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/30 is directly connected, Ethernet1/0
L       192.168.2.2/32 is directly connected, Ethernet1/0
      203.0.113.0/32 is subnetted, 1 subnets
S       203.0.113.1 [1/0] via 192.168.2.1
```

Trouble Ticket #21

- Network requirements state that all PCs should have access to the public address 203.0.113.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1, PC2, and PC3** cannot ping 203.0.113.1

Trouble Ticket #22 – Advanced BGP Ticket

- Network requirements state that all PCs should have access to the public address 198.51.100.1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1, PC2, and PC3** cannot ping 198.51.100.1.

Trouble Ticket #23 – Advanced BGP Ticket

- Network requirements state that ISP1 and IPS2 routers should not learn prefixes from AS 65000.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **ISP1 and ISP2** routers are learning prefixes from AS 65000.
- Fix the problem so that you can achieve the same output below:

```
ISP1# show ip bgp summary
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
209.165.200.2	4	65000	8	13	10	0	0	00:05:09	0
209.165.202.2	4	65003	31	36	10	0	0	00:23:36	6

```
ISP2# show ip bgp summary
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
209.165.201.2	4	65000	9	15	13	0	0	00:06:08	0
209.165.203.2	4	65003	31	38	13	0	0	00:24:33	7
209.165.206.2	4	65003	31	33	13	0	0	00:24:36	7

Trouble Ticket #24 – Advanced BGP Ticket

- Network requirements state that all PCs should have access to the public address 198.51.100.1 via ISP1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PCs** are using ISP2 to reach 198.51.100.1.
- Fix the problem so that you can achieve the same output below:

```
PC1# traceroute 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.10.252 1002 msec 0 msec 1 msec
 2 192.168.3.1 2 msec 2 msec 0 msec
 3 192.168.1.1 1 msec 0 msec 1 msec
 4 209.165.200.1 1 msec 1 msec 0 msec
 5 209.165.202.2 1 msec 1 msec 1 msec
 6 209.165.204.2 1 msec 0 msec 1 msec
```

```
PC2# traceroute 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.30.253 1002 msec 1 msec 1 msec
 2 192.168.4.1 1 msec 1 msec 0 msec
 3 192.168.1.1 1 msec 1 msec 1 msec
 4 209.165.200.1 1 msec 1 msec 2 msec
 5 209.165.202.2 2 msec 1 msec 1 msec
 6 209.165.204.2 2 msec 1 msec 1 msec
```

```
PC3# traceroute 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.200.254 1001 msec 1 msec 0 msec
 2 192.168.2.1 1 msec 1 msec 1 msec
 3 192.168.1.1 1 msec 1 msec 0 msec
 4 209.165.200.1 1 msec 1 msec 1 msec
 5 209.165.202.2 1 msec 1 msec 1 msec
 6 209.165.204.2 0 msec 1 msec 0 msec
```

Trouble Ticket #25 – Advanced BGP Ticket

- Network requirements state that all PCs should have access to the public address 2.0.0.2 directly via ISP2.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **PC1, PC2, and PC3** are using a suboptimal path to reach 2.0.0.2.
- Fix the problem so that you can achieve the same output below:

```
PC1# traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.10.252 1 msec 0 msec 0 msec
 2 192.168.3.1 1 msec 1 msec 0 msec
 3 192.168.1.1 1 msec 1 msec 0 msec
 4 209.165.201.1 1 msec 1 msec 0 msec
```

```
PC2# traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2
VRF info: (vrf in name/id, vrf out name/id)
 1 10.0.30.253 0 msec 0 msec 1 msec
 2 192.168.4.1 0 msec 1 msec 0 msec
 3 192.168.1.1 1 msec 1 msec 0 msec
 4 209.165.201.1 2 msec 2 msec 1 msec
```

```
PC3# traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.200.254 0 msec 0 msec 0 msec
 2 192.168.2.1 1 msec 1 msec 0 msec
 3 192.168.1.1 1 msec 1 msec 0 msec
 4 209.165.201.1 1 msec 0 msec 1 msec
```

Trouble Ticket #26 – Advanced BGP Ticket

- Network requirements state that ISP3-CORE should be able to reach prefixes being advertised by ISP1.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that **ISP3** is unable to reach 1.0.0.1 or 203.0.113.1 when sourcing packets from its Loopback 2 interface.
- Fix the problem so that you can achieve the same output below:

```
ISP3-CORE# ping 203.0.113.1 source loopback2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
ISP3-CORE# ping 1.0.0.1 source loopback2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Trouble Ticket #27 – Advanced BGP Ticket

- ISP3-PE2 has recently implemented route summarization of its 192.0.0.0/22 prefixes.
- After several changes to interface status, network addressing, routing schemes and layer 2 connectivity, a trouble ticket was opened indicating that EDGE is still receiving individual /32 prefixes as well as the summary.
- Fix the problem so that you can achieve the same output below:

```
EDGE# show ip bgp
      Network      Next Hop      Metric LocPrf Weight Path
*      1.0.0.1/32      102.0.0.2              0 65002 65003 65001 i
*>              101.0.0.1              0 65001 i
*      2.0.0.2/32      101.0.0.1              0 65001 65003 65002 i
*>              102.0.0.2              0 65002 i
*      192.0.0.0/22      101.0.0.1              0 65001 65003 i
*>              102.0.0.2              0 65002 65003 i
*      198.51.100.0      102.0.0.2              0 65002 65003 i
*>              101.0.0.1              150 0 65001 65003 i
*      203.0.113.1/32      102.0.0.2              0 65002 65003 65001 i
*>              101.0.0.1              0 65001 i
r      209.165.200.0/30      102.0.0.2              0 65002 65003 65001 i
r>              101.0.0.1              0 65001 i
r      209.165.201.0/30      101.0.0.1              0 65001 65003 65002 i
r>              102.0.0.2              0 65002 i
```

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC