

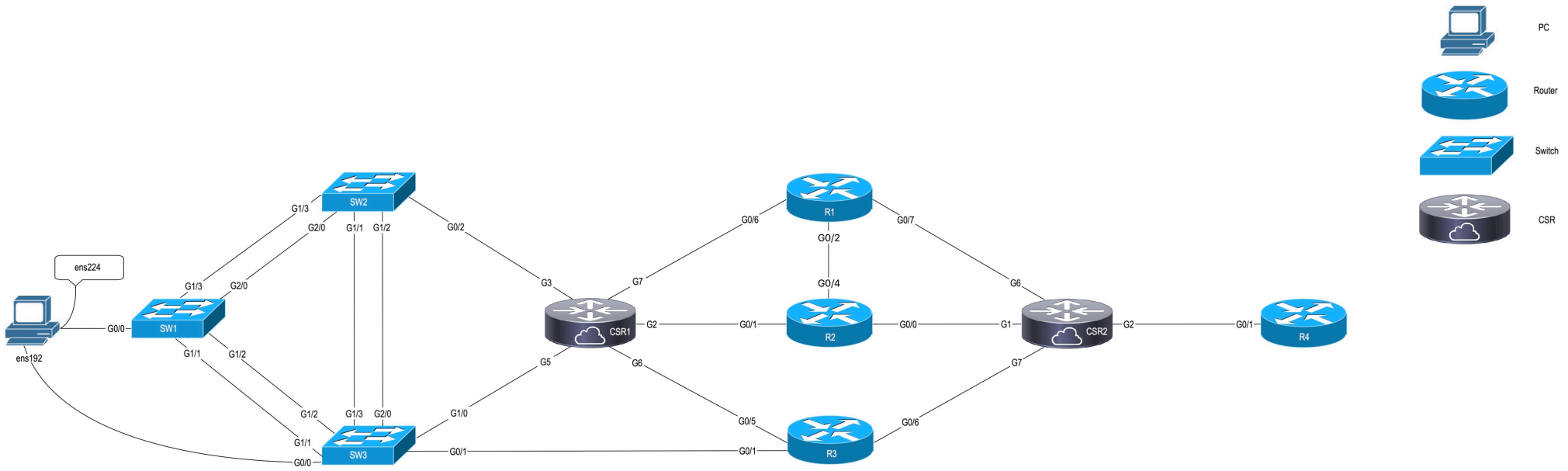


# CCNA 200-301 Bootcamp

Lab Tasks

[ine.com](http://ine.com)

# Base Topology Diagram



## Lab Guidelines

---

- + Refer to videos, notes, or slides to find the commands you need to accomplish the lab tasks.
- + If time permits, feel free to go above-and-beyond what the lab asks you do to:
  - + Experiment by running a variety of “show” commands to view differences in their output.
  - + Experiment with different “debug” commands
- + Unless otherwise stated, passwords will be either “INE” or “Cisco” (with an upper-case or lower-case “C”)
- + It may be helpful to take a screenshot of each topology diagram and have it viewable in a separate window/monitor while reading the lab instructions.



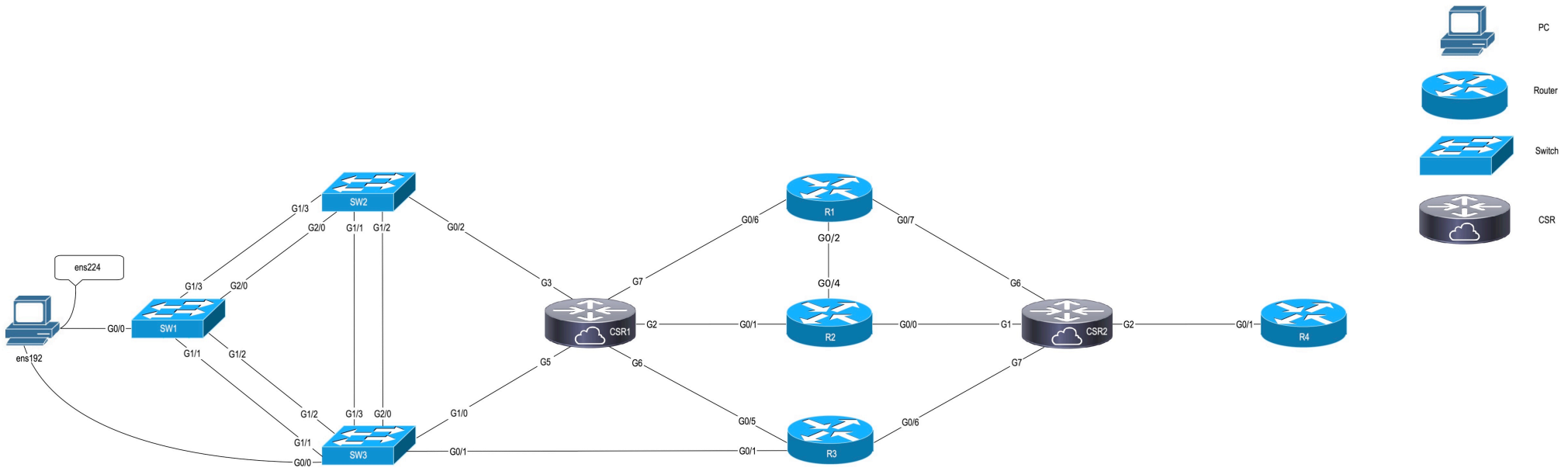


# CCNA 200-301 Bootcamp

Lab Access & Application Familiarization

[ine.com](http://ine.com)

# Base Topology Diagram



## Lab Objectives (Wireshark)

---

- + Familiarization with equipment access
- + Learn how to start-and-stop the following applications:
  - + Terminal
  - + SecureCRT
- + Telnet to topology device from SecureCRT
- + Starting Wireshark from Terminal
  - + Capturing and displaying data
  - + Creating basic display filters

## Lab Tasks (IPv4 Capture & Display)

---

- + Login to Ubuntu host
- + Start Wireshark
- + Capture packets on the ENS-160 interface for 10-15 seconds
- + Stop capture
- + View IPv4 headers and fields
  - + Did you capture any IPv4 fragments?
  - + Create a display filter that displays only packets with the same source IPv4 address



**Thanks For  
Participating!**

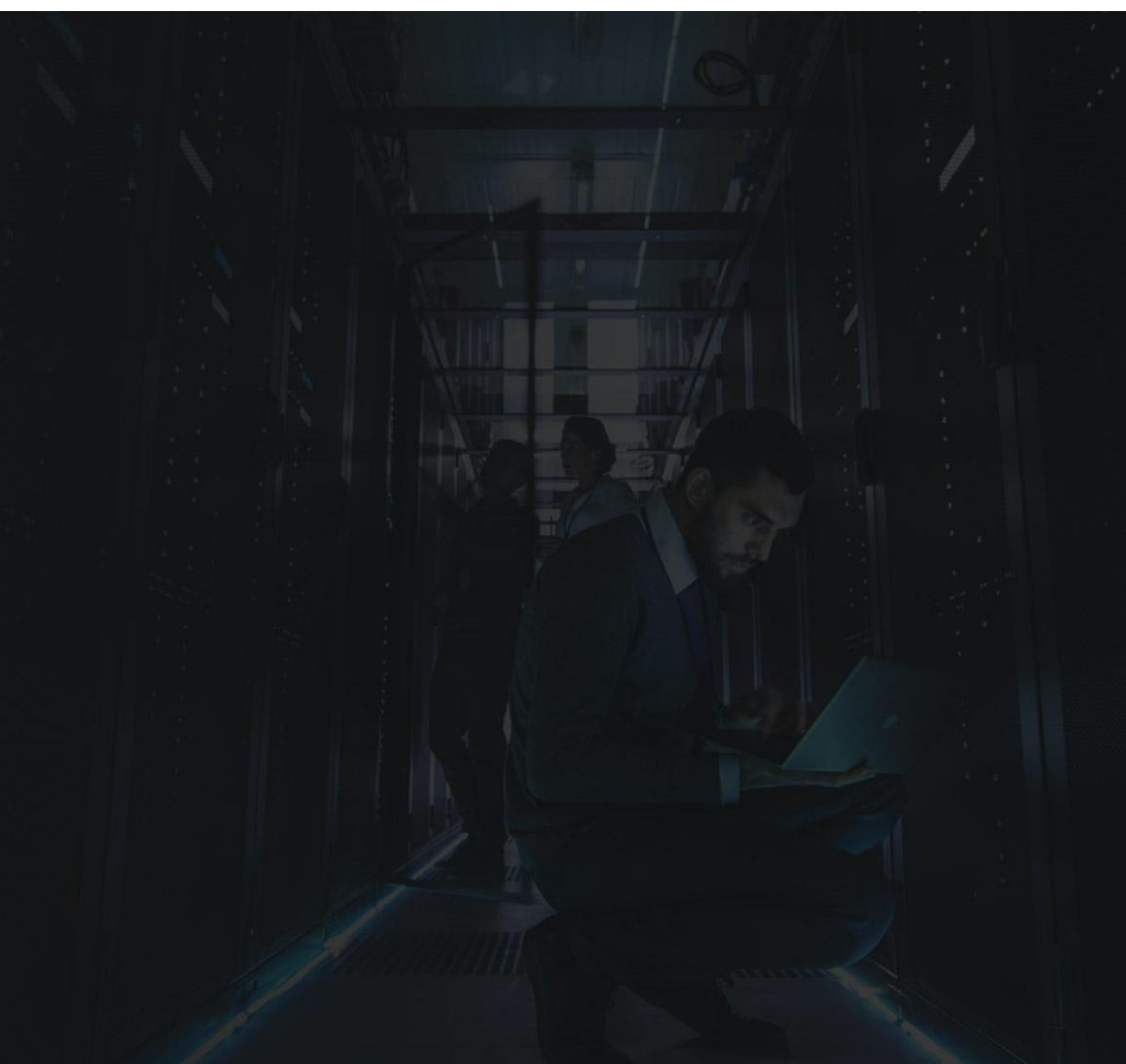




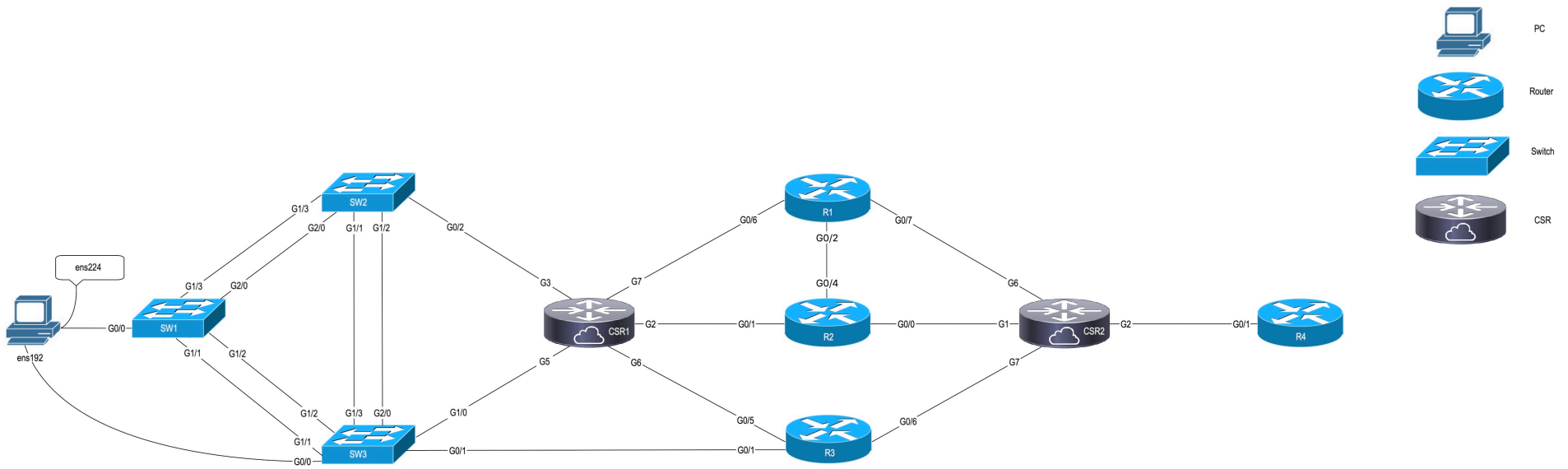
# Lab Task

Viewing TCP Segments

[ine.com](http://ine.com)



# Topology Diagram



## Lab Tasks (TCP Capture & Display)

---

- + Login to Ubuntu host
- + Start Wireshark on the ENS-160 interface
- + Launch the SecureCRT application and telnet to any device in the list
- + Capture packets for 10-15 seconds
- + Stop capture
- + View TCP headers and fields
  - + Can you identify the TCP 3-way handshake?
  - + Can you change Wireshark preferences so that instead of displaying “relative” sequence numbers it displays the actual TCP sequence numbers?



**Thanks For  
Participating!**

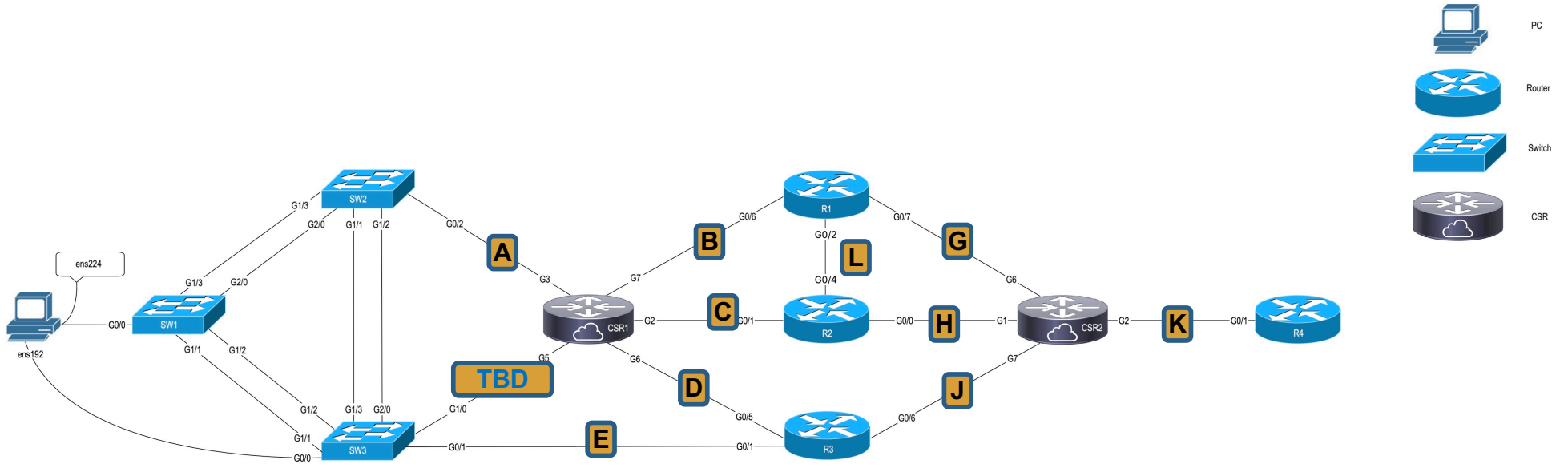


# Lab Task

Introduction To Basic IOS CLI Commands

[ine.com](http://ine.com)

# Topology Diagram



## Lab IPv4 Addressing (Basic IOS Commands)

Network Segment	Prefix	First Host	Second Host
A	1.2.3.0/24	CSR1(Gig3)= .1	None at this time
B	11.11.11.0/24	CSR1(Gig7)= .1	R1(Gig0/6)= .2
C	21.21.21.0/24	CSR1(Gig2)= .1	R2(Gig0/1)= .2
D	31.31.31.0/24	CSR1(Gig6)= .1	R3(Gig0/5)= .2
E	3.3.3.0/24	None at this time	None at this time
G	122.122.122.0/24	CSR2(Gig6)= .1	R1(Gig0/7)= .2
H	22.22.22.0/24	CSR2(Gig1)= .1	R2(Gig0/0)= .2
J	23.23.23.0/24	CSR2(Gig7)= .1	R3(Gig0/6)= .2
K	42.42.42.0/24	CSR2(Gig2)= .1	R4(Gig0/1)= .2
L	112.112.112.0/24	R1(Gig0/2)= .1	R2(Gig0/4)= .2

## Lab Tasks (Cisco IOS Basics)

---

1. Connect to device CSR1 and use the “config replace” command to load the configuration “**IOS-Basics**” from Flash memory.
  - a) To confirm that your “config replace” command worked, issue a command to confirm that at least one interface on this device now has an IPv4 address configured
  - b) Confirm that this device now has an enable-secret password of “**cisco**”
2. Repeat the same steps above on devices R1 and R3
3. Confirm that (from within the CLI of CSR1) you can now ping R1s IP address (on Segment-B) and R3’s IP address (on Segment-D).
4. Save your Running-Config to your Startup-Config on these devices

Note that without IPv4 routing enabled, devices can only ping IPv4 addresses at the other end of their directly-connected cables.





## Lab Tasks (Cisco IOS Basics)

---

5. Login to device **R2** and configure it with the following parameters:
  - a. A “hostname” of R2
  - b. Enable secret of “cisco”
  - c. A command that will prevent DNS lookups of any mistyped commands
  - d. A command that will repeat the last line you’ve typed should any Syslog message interrupt your typing
  - e. Apply relevant IP addresses and subnet masks to interfaces as shown in the diagram and ensure these interfaces are administratively enabled

NOTE: A mask of /24 = 255.255.255.0
6. Verify your configuration by successfully pinging CSR1 and R1 from R2
7. Save your Running-Config to your Startup-Config

Note that without IPv4 routing enabled, devices can only ping IPv4 addresses at the other end of their directly-connected cables.



## Lab Tasks (Cisco IOS Basics)

---

8. Login to device **CSR2** and configure it with the same parameters you used on R2 (except IP addresses and hostname should be different).
9. Configure CSR2 such that it will accept incoming Telnet requests so long as the requestor supplies the following credentials:
  - a. Username = INE
  - b. Password = cisco
10. Verify your configuration by:
  - a. Successfully pinging R1, R2 and R3 from CSR2
  - b. Telnetting to CSR2 from R2
11. Save your Running-Config to your Startup-Config

## Lab Tasks (Cisco IOS Basics)

---

12. Login to device **R4** and configure it with the same parameters you used on R2 & CSR2 (except IP addresses and hostname should be different).
13. Configure R4 such that it will accept incoming SSH requests so long as the requestor supplies the following credentials:
  - a. Username = INE
  - b. Password = cisco

You may use whatever domain-name you wish but ensure your RSA keysize is 1024-bits.

14. Verify your configuration by:
  - a. Successfully pinging CSR2 from R4
  - b. Initiating an SSH session to R4 from CSR2
15. Save your Running-Config to your Startup-Config



## Lab Tasks (Cisco IOS Basics)

---

16. On any IOS-based device in your topology, see if you can issue various IOS commands that:
- a. Display the contents of the configuration file currently in-use
  - b. Display the contents of the saved configuration file that will be loaded upon the next reload of the device
  - c. Display a summary of every interface on the device, the interface naming convention, interface state, and if any IP addresses have been configured



**Thanks For  
Participating!**



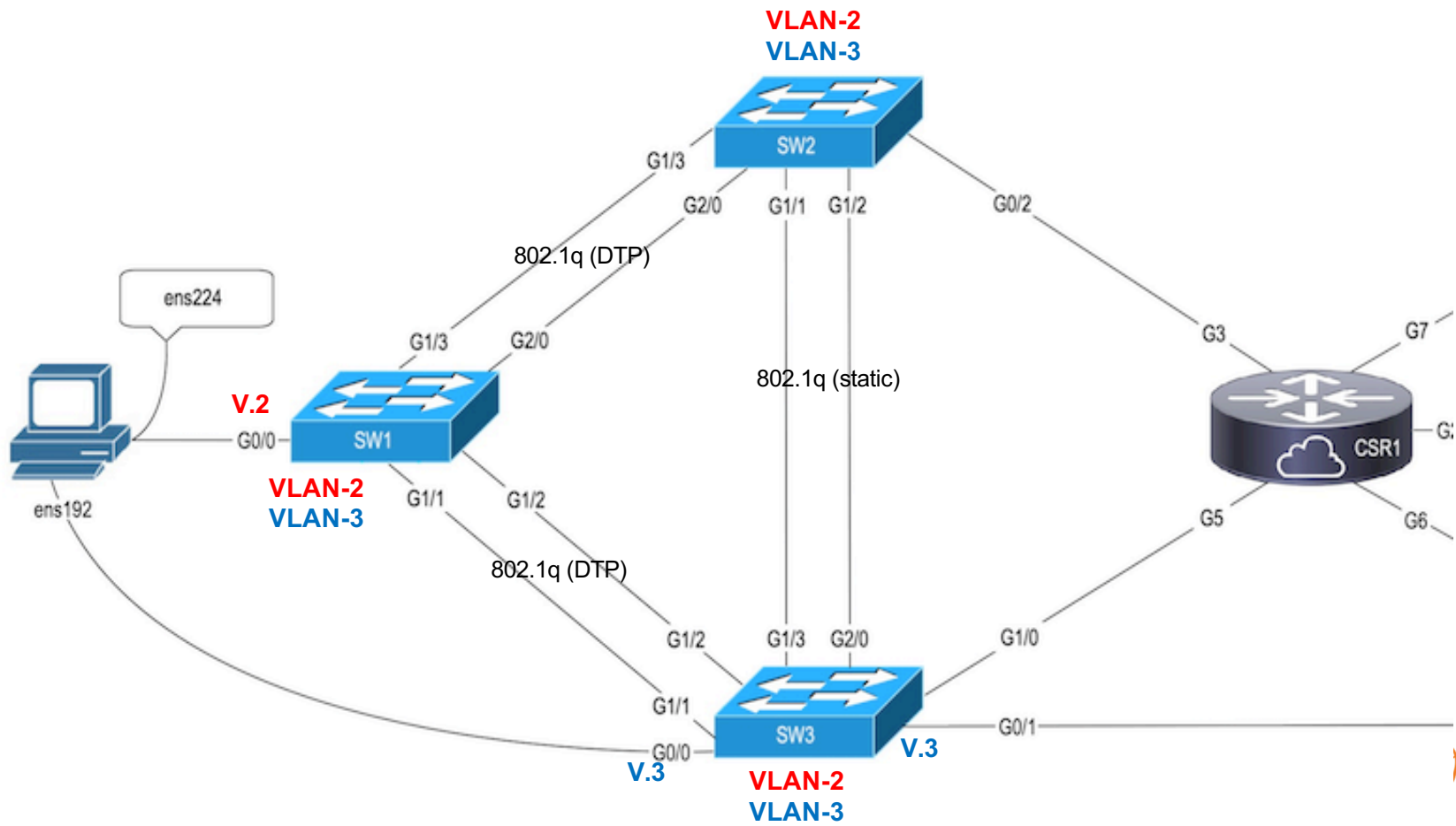
# Lab Task

Introduction To Cisco Switching

[ine.com](http://ine.com)



# Topology Diagram



## Lab Tasks (Intro To Switching)

---

1. Use the “config replace” command to load the configuration “**Switch-Basics**” from Flash memory on Sw1, Sw2 and Sw3
2. From the Ubuntu device, find the MAC address for interface ENS-192
3. Login to Switch-3 and do the following:
  - a. Use the “interface range” command to disable all interfaces that are not displayed in the topology diagram
  - b. View the existing VLANs on this switch
  - c. View the MAC Address Table and locate the MAC address of the Ubuntu device that you discovered in the previous step.
    - i. Within which VLAN was this MAC address learned?
    - ii. Which port of the switch learned this MAC address?



## Lab Tasks (Intro To Switching)

---

4. Create VLAN-2 and VLAN-3 on Sw3
  - a. VLAN-2 should be given a name of “Payroll”
  - b. VLAN-3 should be given a name of “Marketing”
5. Issue the command, “show vlan” to confirm that your new VLANs exist
8. On Sw3, use the “interface range” command to configure interfaces Gigabit0/0 and Gigabit0/1 as Access switchports and put them both into VLAN-3
  - a. View the MAC Address Table on Sw3 again and locate the MAC address of the Ubuntu device that you discovered in a previous step.
    - i. Has the VLAN assignment for this MAC address changed?
7. Issue the following commands and notice the differences in their output:
  - + Show interface Gig1/0
  - + Show interface Gig1/0 switchport

## Lab Tasks (Intro To Switching)

---

8. Login to switches Sw1 and Sw2 and create VLANS-2, and 3 on those switches as well
  - a. Apply the same names to these VLANs as you did on Sw3
  - b. Also disable all interfaces that are not a part of the topology diagram
9. Both Sw2 and Sw3 should have Layer-3 management interfaces (SVIs) for VLAN-2 using the following IPv4 addresses:
  - a. Sw2: 2.2.2.2 255.255.255.0
  - b. Sw3: 2.2.2.3 255.255.255.0
  - c. Ensure these interfaces are administratively “Up”

## Lab Tasks (Intro To Switching)

---

10. Configure all switch-to-switch links shown in the topology diagram as 802.1q VLAN Trunks using the following guidelines:
  - a) Both links between Sw2 and Sw3 should be configured as static VLAN Trunks ("switchport mode dynamic" is NOT allowed)
  - b) Both links between Sw1 and Sw2 should utilize DTP to form their VLAN trunks, with Sw2 being the initiator of the DTP exchange
  - c) Both links between Sw1 and Sw3 should utilize DTP to form their VLAN trunks, with Sw3 being the initiator of the DTP exchange
  - d) Both VLAN Trunks between Sw1 and Sw3 should utilize VLAN-2 as their Native VLAN.
11. Issue the command, "show interface trunk" on Sw1 and Sw2 to confirm that you now have functional 802.1q VLAN trunks
12. On all three switches save your configurations to NVRAM by updating the Startup-Config file



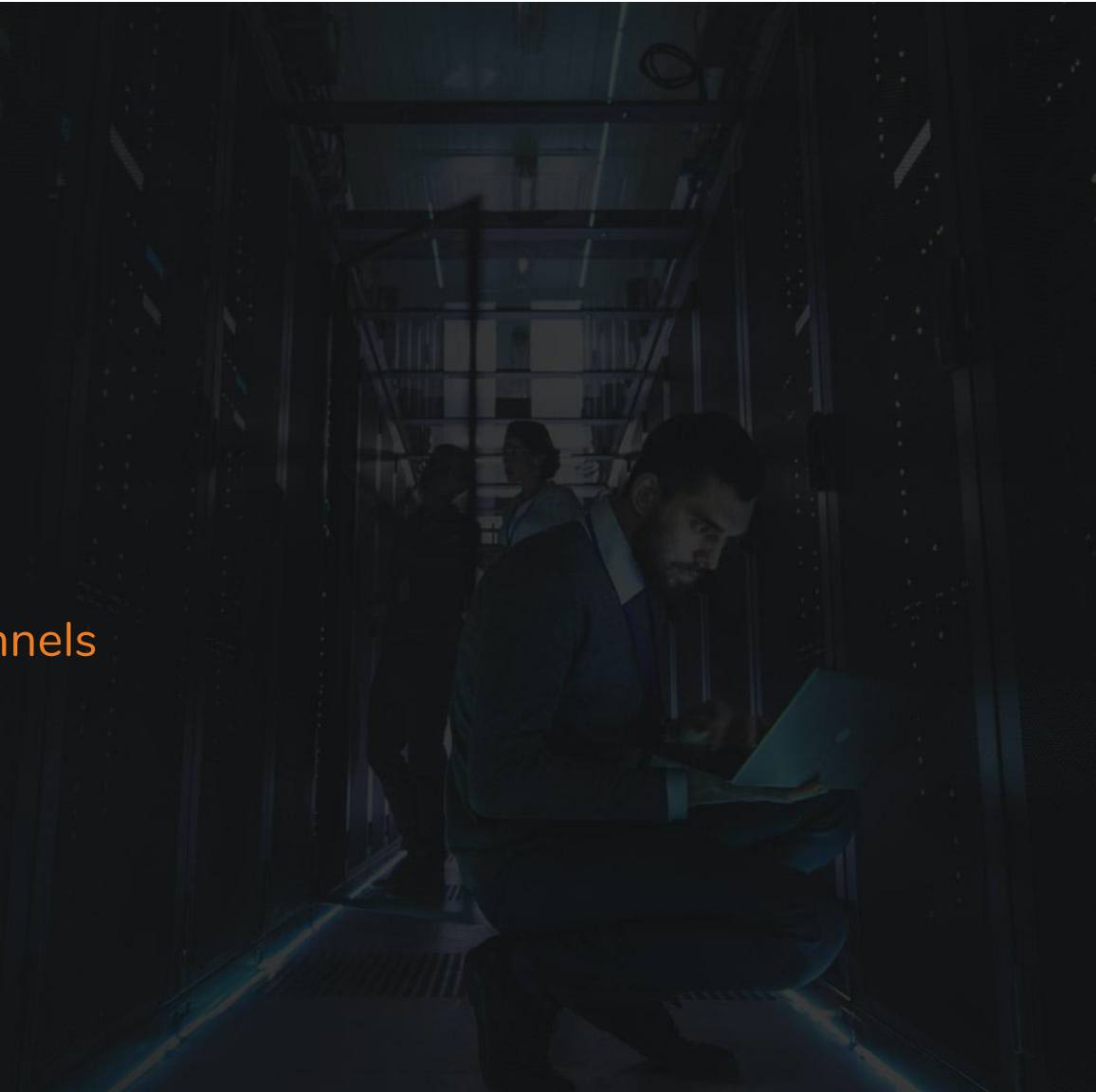
**Thanks For  
Participating!**



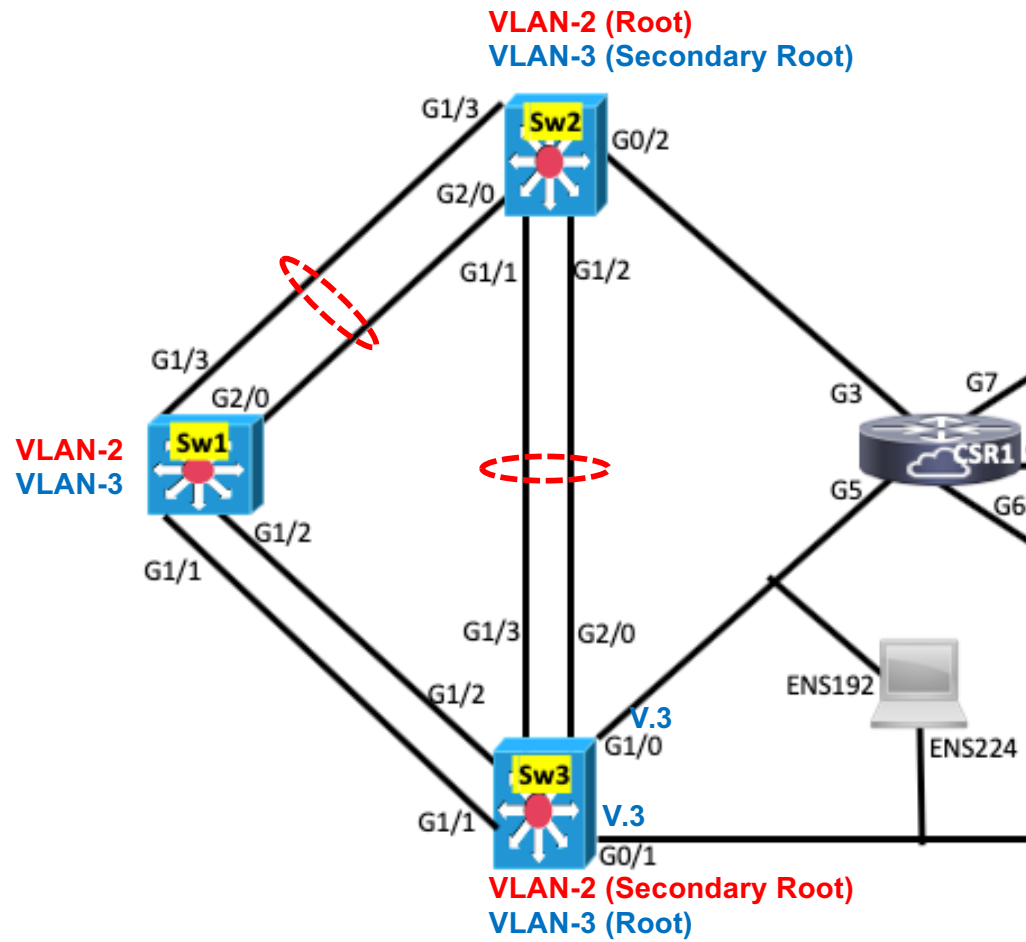
# Lab Task

Working With RSTP & Etherchannels

[ine.com](http://ine.com)



# Topology Diagram



## Lab Tasks (RSTP & Etherchannels)

---

1. Use the “config replace” command to load the configuration “**RSTP-Channel**” from Flash memory on Sw1, Sw2 and Sw3
2. Use Cisco IOS commands to manipulate RSTP in the following ways:
  - a. Issue a command on all of your switches to determine the mode of Spanning-Tree currently in-use. If they are not already running RSTP, issue a command to ensure Sw1, Sw2 and Sw3 are running RSTP (Rapid Spanning-Tree Protocol)
  - b. Issue a command to ensure that Sw2 is the RSTP Root Bridge for VLAN-2, and the Secondary Root Bridge for VLAN-3. The command you select must NOT reference Bridge-Priority values in any way.
  - c. Issue a command to ensure that Sw3 is the RSTP Root Bridge for VLAN-3, and the Secondary Root Bridge for VLAN-2. The command you select must explicitly configure non-default values for Bridge-Priority to accomplish this objective.
  - d. Issue a command starting with “show spanning-tree vlan” to verify your Root Bridge assignments.

## Lab Tasks (RSTP & Etherchannels)

---

3. Configure the following Layer-3 Switched Virtual Interfaces (SVIs) on the following devices:
  - a. SW1:
    - i. Interface vlan 2: 2.2.2.1 255.255.255.0
    - ii. Interface vlan 3: 3.3.3.1 255.255.255.0
  - b. SW2:
    - i. Interface vlan 3: 3.3.3.2 255.255.255.0
  - c. SW3:
    - i. Interface vlan 3: 3.3.3.3 255.255.255.0
4. Ensure these interfaces are administratively “Up”
5. On Sw3, enable the Port-Security feature on interfaces Gigabit 0/1 and 1/0



## Lab Tasks (RSTP & Etherchannels)

---

6. Ensure that from Sw1 you can ping all of the IPv4 addresses on Sw2 and Sw3. If these pings don't work...troubleshoot and resolve the problem(s).
7. Bundle both links connecting Sw1 and Sw2 into a Layer-2 Etherchannel using Cisco's PAgP to form the channel.
  - a. Use channel-group number "1" in your configuration
  - b. Sw1 should initiate the PAgP frame exchange
8. Bundle both links connecting Sw2 and Sw3 into a Layer-2 Etherchannel using the IEEE's LACP to form the channel.
  - a. Use channel-group number "2" in your configuration
  - b. Sw2 should initiate the LACP frame exchange

## Lab Tasks (RSTP & Etherchannels)

9. From Sw1, ping the IPv4 address on Sw2 of 2.2.2.2
- The frames should have gone directly across the Etherchannel between Sw1 and Sw2 to transport those pings.
  - Verify the statement above by:
    - Issuing the command, “show interface vlan 2” on Sw1 and take note of its MAC address
    - Go to Sw2 and find that same MAC address in its MAC Address-Table. It should have been learned via Port-Channel 1.

```
Sw1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Sw1#sho interface vlan 2
Vlan2 is up, line protocol is up
  Hardware is Ethernet SVI, address is 00af.ff11.8002 (bia 00af.ff11.8002)
  Internet address is 2.2.2.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
Sw1#
```

```
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#
Sw2#show mac address-table address 00af.ff11.8002
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
-----
2       00af.ff11.8002   DYNAMIC   Po1
Total Mac Addresses for this criterion: 1
Sw2#
```

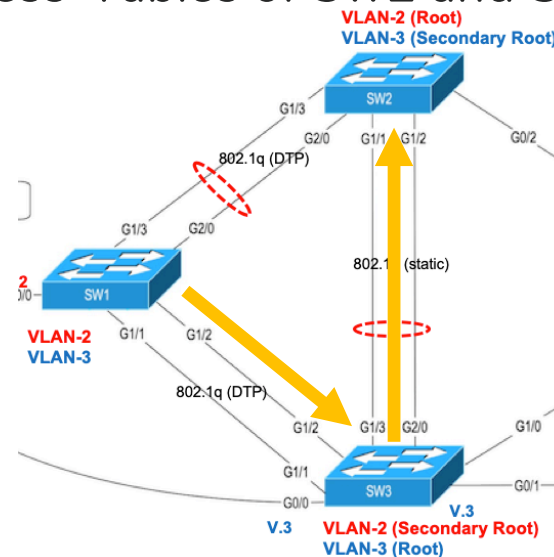


## Lab Tasks (RSTP & Etherchannels)

10. By modifying RSTP interface “cost” values, change the blocking-and-forwarding states of various interfaces such that when you repeat Step-9, those same pings must now go through Sw3 (across interface Gig1/2) to reach Sw2.
  - a. Verify this by viewing the MAC Address-Tables of Sw2 and Sw3

```
Sw1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/32/40 ms
Sw1#

Sw2#
Sw2#show mac address-table address 00af.ff11.8002
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
-----
2       00af.ff11.8002   DYNAMIC Po2
Total Mac Addresses for this criterion: 1
Sw2#
```





**Thanks For  
Participating!**



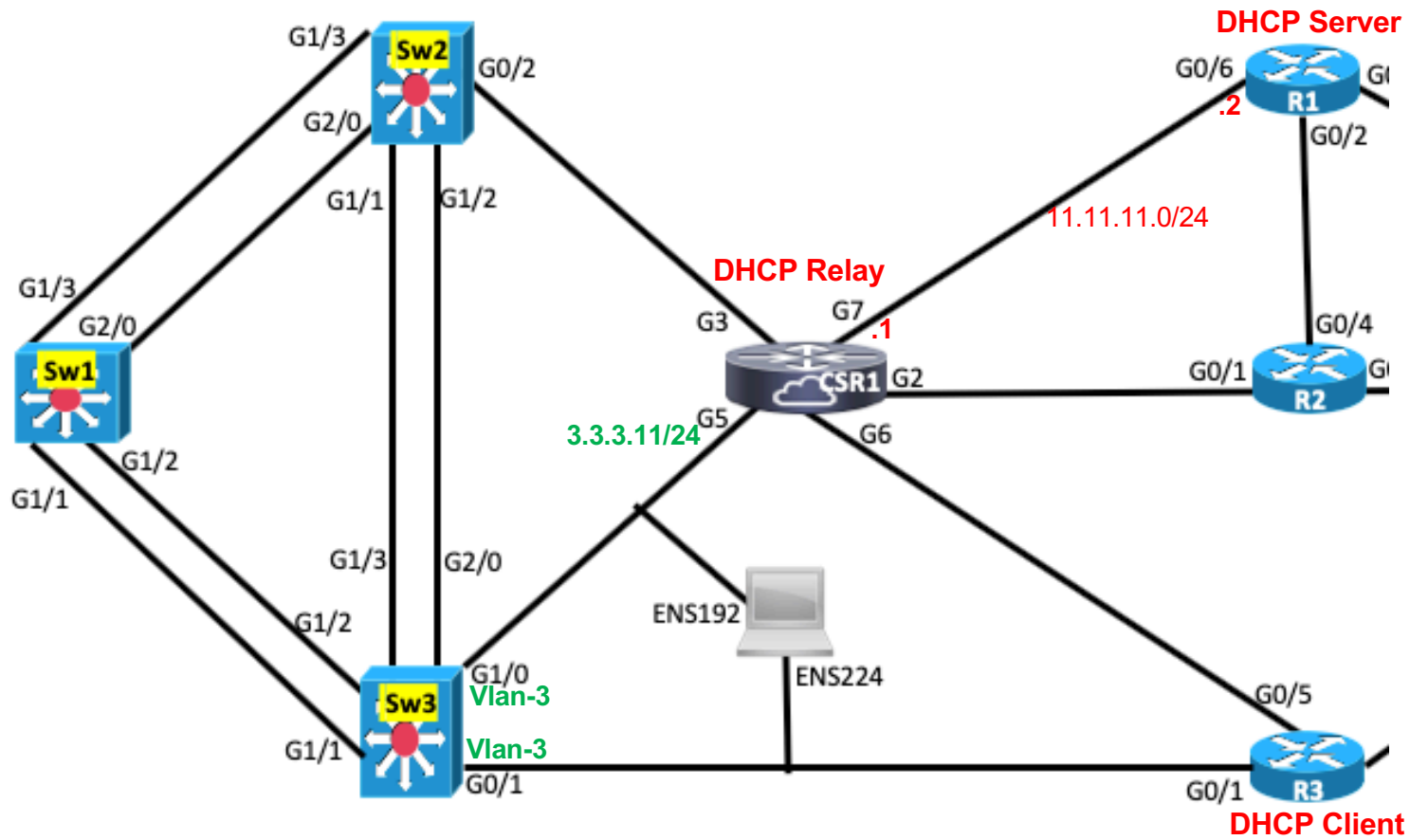
# Lab Task

Implementing & Viewing DHCP

[ine.com](http://ine.com)



# Topology Diagram



## Lab Tasks (Implementing & Viewing DHCP)

---

1. Use the “config replace” command to load the configuration “**DHCP-Basics**” from Flash memory on R1, CSR1, Sw3 and R3
2. Configure an IPv4 DHCP Pool on device R1 using the following criteria:
  - a. The name of your DHCP Pool should be INE
  - b. The pool should allocate IPv4 addresses from the network 3.3.3.0/24
  - c. The pool should provide a default-gateway IPv4 address of 3.3.3.11
  - d. The pool should allocate an IPv4 address that has a lifetime of 2-days
3. While still on R1, ensure it does not allocate (via DHCP) any static IP addresses you’ve already configured in this subnet, namely 3.3.3.1, 3.3.3.2 or 3.3.3.3
4. Configure CSR1 as a DHCP relay agent, pointing it to the address of 11.11.11.2 for relaying of DHCP broadcast messages.



## Lab Tasks (Implementing & Viewing DHCP)

---

5. On your Ubuntu host, start the Wireshark application, capturing all frames on the ENS-192 connection (which connects Ubuntu to Sw3)
6. Move to R3 and:
  - a. Shutdown interface Gigabit0/1
  - b. Configure its Gigabit0/1 interface as a DHCP client
  - c. Enable interface Gigabit0/1
7. All of the DHCP transactions between the DHCP Client (R3) and the DHCP Server (R1) should have been captured and viewable via Wireshark on the Ubuntu host. View those packets now.
8. After a DHCP address has been allocated to R3, go back to R1 (the IOS DHCP Server) and familiarize yourself with the output of “[show ip dhcp binding](#)”



## Lab Tasks (Implementing & Viewing DHCP)

---

9. On router R3, perform the following actions:
  - a. Disable/shutdown interface Gigabit0/1
  - b. From privileged EXEC mode, enable the command, “`debug dhcp detail`”
  - c. Re-enable interface Gigabit0/1 and view the DHCP debug output
  - d. Once the debug output has stopped, cease the debug operation with the command, “`undebug all`”
10. If you haven't already done so, quit the Wireshark packet capture program on your Ubuntu host



**Thanks For  
Participating!**



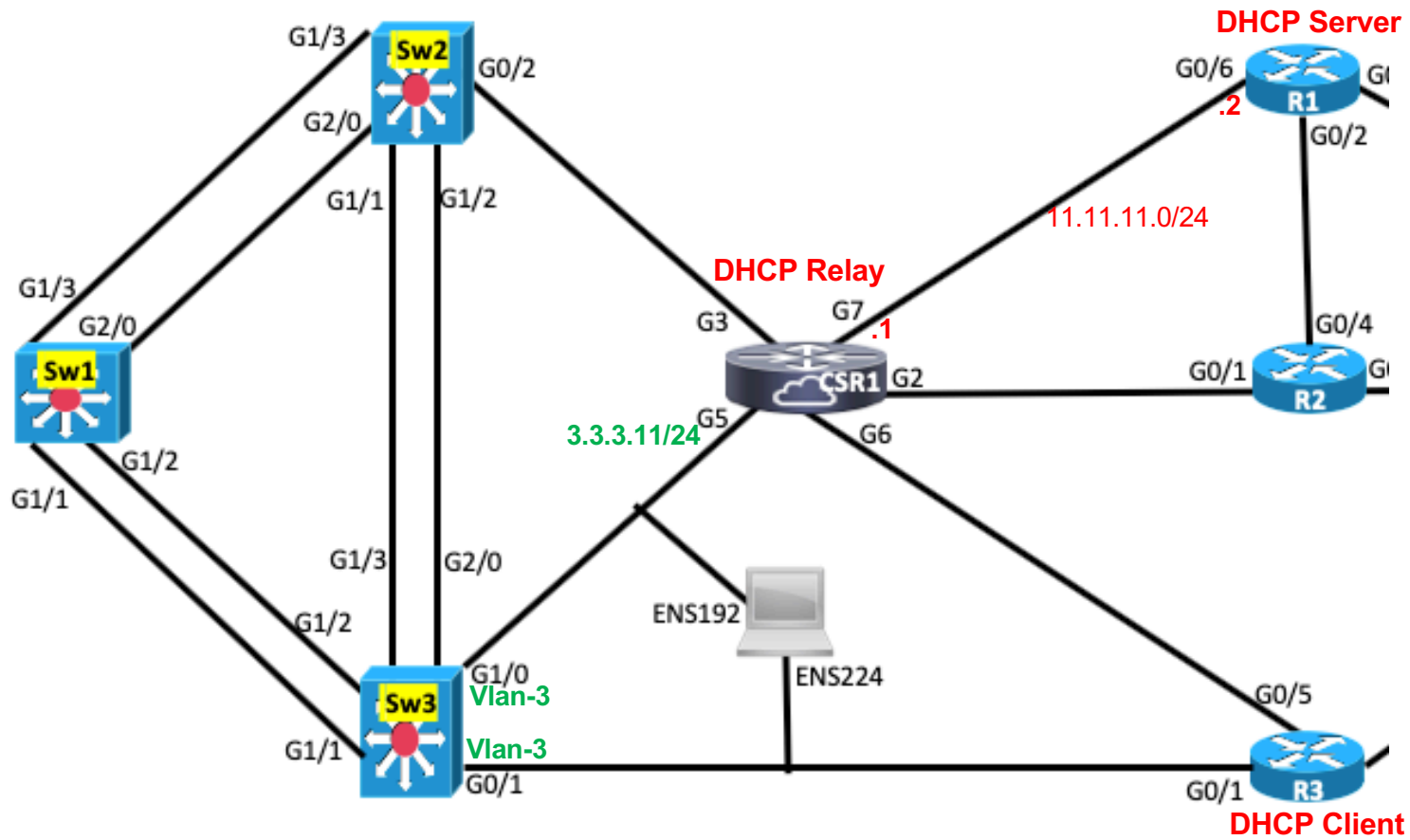
# Lab Task

Securing Switches With Port-Security

[ine.com](http://ine.com)



# Topology Diagram



## Lab Tasks (Port Security)

---

1. On devices R3 and Sw3, use the “config replace” command to load the configuration titled, “**Port-Security**” from flash memory.
2. Enable Port-Security on interface Gigabit0/1 of Sw3 with only a single command.
  - a. Familiarize yourself with the output of the command, “show port-security”
  - b. Familiarize yourself with the output of the command, “show port-security interface Gigabit0/1”
3. Open a second Telnet window (so you can watch R3 and Sw3 simultaneously) and move to R3 and change the mac address of interface Gigabit0/1 on this device to 00bb.bbbb.bbbb
  - a. Did you see any SYSLOG messages in Sw3 as a result of the action you just took on R3?
  - b. View the output again of the commands in step-2a and 2b above and notice the “Port Status” and “Last Source Address” fields.

## Lab Tasks (Port Security)

---

4. On R3, disable interface Gigabit0/1
5. Move back to Sw3 and notice the status of interface Gigabit0/1 in the output of the “[show interface Gigabit0/1](#)” command.
  - a. “Bounce” interface Gigabit0/1 with the “[shutdown](#)” and “[no shutdown](#)” commands.
6. On Sw3 modify Port-Security using the following guidelines:
  - a. Port-Security should be pre-configured to recognize the MAC address of 00bb.bbbb.bbbb as a secure, authorized MAC
  - b. Port-Security should be allowed to learn a maximum of two(2) MAC addresses
  - c. If a security violation occurs, the offending frame should be discarded silently, without any SYSLOGS or violation counters displaying the violation ever happened.
7. Move back to R3 and re-enable its interface.
  - a. Did it receive an IPv4 address via DHCP (it should have)?
  - b. View the output of “[show port-security address](#)”. Does 00bb.bbbb.bbbb now display as an authorized address (it should)?

## Lab Tasks (Port Security)

8. On R3, remove the “mac” command you previously configured on interface Gigabit0/1 and allow it to revert to using its default MAC address.
  - a. From R3 ping the default-gateway address of 3.3.3.11 (the ping should be successful).
9. Move back to Sw3 and issue the command, “show port-security address”. You should now see two MAC addresses having been learned via Port-Security on interface Gigabit0/1.

```
Sw3#sho port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address          Type                Ports    Remaining Age
(mins)
-----
3       0050.56a5.0c3b      SecureDynamic       Gi0/1    -
3       00bb.bbbb.bbbb      SecureConfigured    Gi0/1    -
```

## Lab Tasks (Port Security)

10. Move back to R3 and change its MAC address again, this time to **00dd.dddd.dddd**
  - a. From R3 ping the default-gateway address of 3.3.3.11 again. This time (because Sw3 is seeing a third incoming MAC address) this should cause a violation and the ping should fail.
  - b. View the output of “show port-security interface gigabit0/1” and notice the “Port Status” is “Secure-up” but you DO see the third MAC address that was dropped.

```
R3#ping 3.3.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.11, timeout is 2 seconds:
*****
Success rate is 0 percent (0/5)
```

```
Sw3#show port-security int gig 0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Protect
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
Total MAC Addresses     : 2
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 00dd.dddd.dddd 3
Security Violation Count : 0
```







**Thanks For  
Participating!**

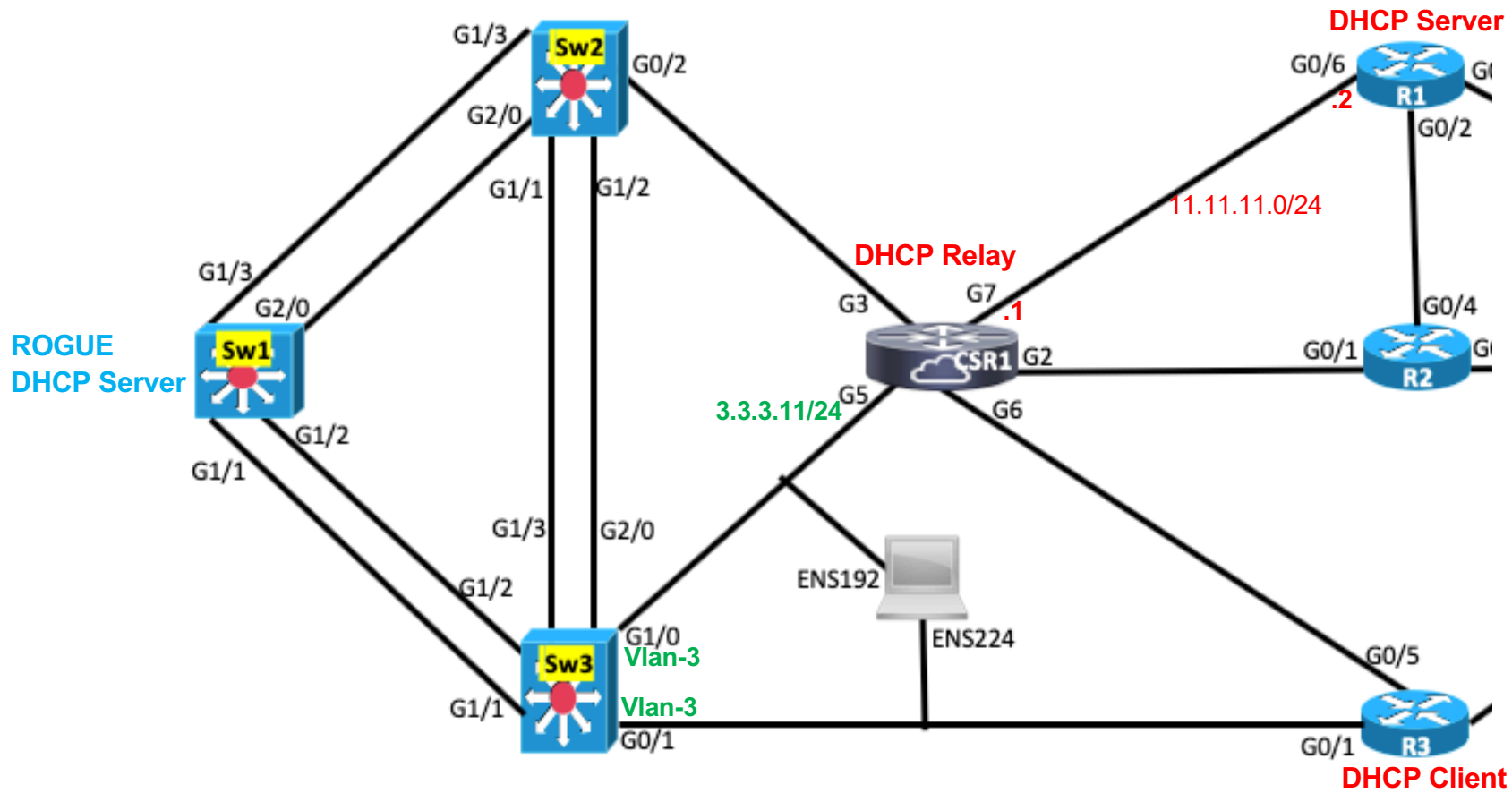


# Lab Task

DHCP Snooping & Dynamic ARP Inspection

[ine.com](http://ine.com)

# Topology Diagram



## Lab Tasks (DHCP Snooping)

---

1. On the following devices, use the “config replace” command to load the configuration titled, “**Snoop-Inspect**” from flash memory:
  - a. Sw1
  - b. Sw3
  - c. R1
  - d. R3
  - e. CSR1

## Lab Tasks (DHCP Snooping)

2. Verify that R1 is still configured as a DHCP Server by viewing the output of “show running-config”
3. Verify that R3 has received an IPv4 address on its Gigabit 0/1 interface via DHCP by viewing the output of “show ip interface brief”. If it has not, troubleshoot and fix this issue.

```
R1#show run | begin ip dhcp
ip dhcp excluded-address 3.3.3.1 3.3.3.3
!
ip dhcp pool INE
network 3.3.3.0 255.255.255.0
default-router 3.3.3.11
lease 2
```

```
R3#show ip interface brief
Interface IP-Address OK? Method Status Prot
ocol
GigabitEthernet0/0 unassigned YES NVRAM up
GigabitEthernet0/1 3.3.3.8 YES DHCP up
```



## Lab Tasks (DHCP Snooping)

---

4. Configure Sw1 as a Rogue (unauthorized) DHCP Server by performing the following actions:
  - a. Configure a DHCP Pool named, "Rogue"
  - b. Within that pool provide a network of 99.99.99.0 /24
  - c. Within that pool provide a default gateway address of 99.99.99.1
  - d. Within that pool provide a lease of 12-days and 6-hours
  - e. Change the IPv4 address of interface VLAN 3 to be 99.99.99.1 /24

## Lab Tasks (DHCP Snooping)

5. Move over to device R3 and configure the following statements:
  - a. R3(config)#**logging console 6** ← 

This command prevents debug output from being displayed on the console connection.
  - b. R3(config)#**logging buffer debug** ← 

This command stores debug output in the memory buffer for viewing later.
  - c. R3(config)#end
  - d. R3#**clear log** ← 

This command clears out the contents of the logging buffer.
  - e. R3#**debug dhcp detail**
6. On R3, disable (shutdown) interface Gigabit0/1, wait about 10-15 seconds and then re-enable this interface.
  - a. View the output of your debug by typing, “show log”
  - b. Do you see incoming DHCP offers from the legitimate DHCP Server (R1) as well as the Rogue DHCP Server (Sw1)? You should.
  - c. Which IPv4 address was accepted by R3?
7. If you perform the step above another two or three times, at some point R3 should accept the IPv4 address from the Rogue DHCP Server.

## Lab Tasks (DHCP Snooping)

---

8. Configure DHCP Snooping on Sw3 in such a way that the the Rogue DHCP Server is rendered powerless but DHCP transactions can still occur to/from the legitimate DHCP Server.

\*\*\***NOTE:** Remember to disable Sw1 from adding Option-82 (the “Information Option”) to DHCP messages.

9. On R3, clear your logging buffer, and disable/re-enable interface Gigabit0/1.
  - a. View your DHCP debugging output in the log. Now you should ONLY see DHCP Offers from the legitimate DHCP Server.
  - b. **Turn off all debugs on R3 by typing, “`undebug all`”**
10. On Sw3, familiarize yourself with the output of the following commands:
  - a. `Show ip dhcp snooping`
  - b. `Show ip dhcp snooping binding`





## Lab Tasks (Dynamic ARP Inspection)

---

11. From R3, ensure it can still ping the IPv4 address it received via DHCP as its Default-Gateway (3.3.3.11)
12. Move over to device Sw1 and do the following:
  - a. Remove the Rogue DHCP Pool
  - b. Reconfigure interface VLAN 3 with the correct IPv4 address (3.3.3.1 /24)
  - c. Ensure that from Sw1 you can ping CSR1 at 3.3.3.11
13. Ensure you have at least two Telnet windows open so you can view the output of Sw1 and Sw3 simultaneously.

## Lab Tasks (Dynamic ARP Inspection)

---

14. On Sw3, configure Dynamic ARP Inspection for VLAN-3
15. Move back to Sw1 and clear its ARP cache with the command, “clear ip arp 3.3.3.11”
  - a. Can you still ping CSR1 at 3.3.3.11 from Sw1? You should NOT be able to do so.
  - b. If you ARE able to ping 3.3.3.11 from Sw1, clear your ARP cache again with the command, “clear arp”
  - c. Dynamic ARP Inspection (on Sw3) should be blocking the ARP requests from Sw1 going to CSR1...and that’s why your Pings should fail. Sw3 should also be reporting this via SYSLOG messages.

```
*Jan 13 15:01:02.343: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/1, vlan 3. ([00af.ff11.8003/3.3.3.1/0000.0000.0000/3.3.3.11/15:01:01 UTC Mon Jan 13 2020])
```

## Lab Tasks (Dynamic ARP Inspection)

---

16. Notice that even with Dynamic ARP Inspection enabled on Sw3, pings from R3 to 3.3.3.11 should still be successful:
  14. This is because DAI can validate the legitimacy of R3 via the DHCP Snooping Binding Table. No such validation is possible for Sw1 which has a static IPv4 address.
17. Using an interface-level command (related to Dynamic ARP Inspection) on Sw3, make it possible for Sw1 to ping CSR1 (at 3.3.3.11)

## Lab Tasks (Dynamic ARP Inspection)

---

18. Provide a static IPv4 address of 3.3.3.33 to interface Gigabit0/1 on R3
19. Attempt to ping 3.3.3.11 from R3 now. The ping should fail due to Dynamic ARP Inspection on Sw3.
20. Configure an ARP Access-List on Sw3 and associate it to Dynamic ARP Inspection to make it possible for R3 to ping CSR1 (at 3.3.3.11)



**Thanks For  
Participating!**

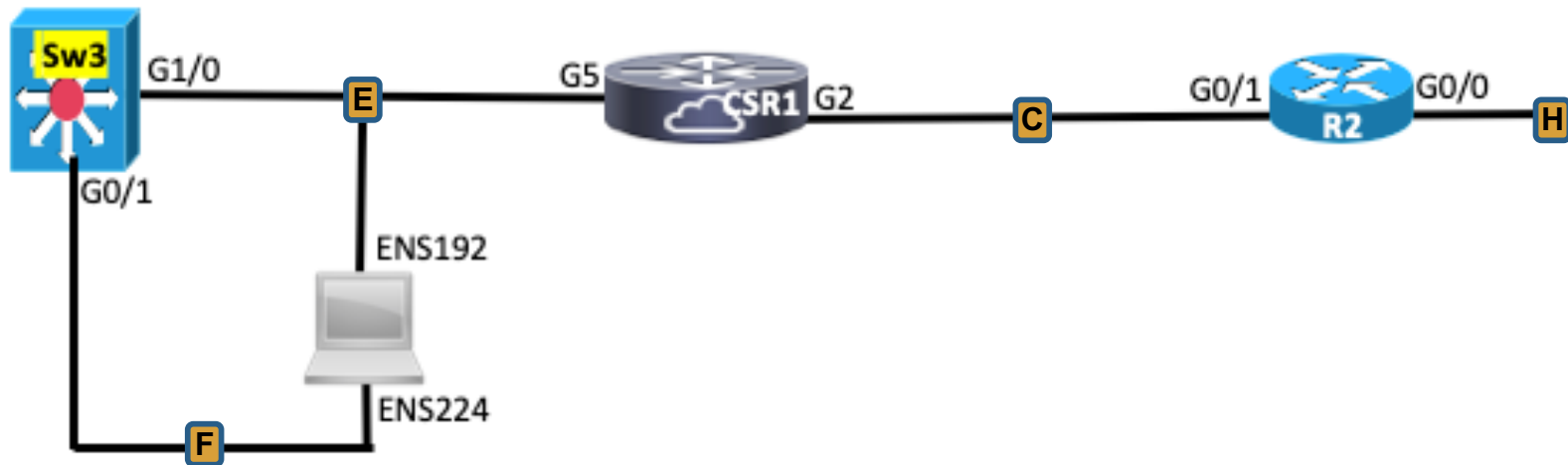


# CCNA 200-301 Bootcamp

IPv4 Routing Basics

[ine.com](http://ine.com)

## Topology Diagram



Network Segment	Prefix	First Host	Second Host
C	21.21.21.0/24	CSR1(Gig2)= .1	R2(Gig0/1)= .2
E	3.3.3.0/24	Sw3(VLAN-3) = .3	CSR1(Gig5)= .11
F	192.168.1.0/24	Ubuntu(ENS224)= .10	Sw3(VLAN-192) = .254
H	22.22.22.0/24	N/A for this lab	R2(Gig0/0)= .2

## Lab Tasks (IPv4 Routing Basics)

---

1. On the following devices, use the “config replace” command to load the configuration titled, “**Routing-Basics**” from flash memory:
  - + Sw3
  - + CSR1
  - + R2



## Lab Tasks (Routing Basics)

---

2. On Sw3 configure VLAN-192
  - a. Apply this VLAN to interface Gigabit0/1 (connected to ENS-224 on the Ubuntu host)
  - b. Use the “show vlan” command to confirm the VLAN addition and port assignment on Sw3
3. On Sw3, configure a Switched Virtual Interface (SVI) for VLAN-192. Assign it the IPv4 address provided in the addressing chart at the beginning of this lab.
4. From the Ubuntu host, ensure you can ping the SVI you just created on Sw3
  - a. From the Terminal app in Ubuntu, issue the command, “`sudo arp`” to view the ARP cache of this device.
  - b. Compare the MAC address that was learned from your Ping with the MAC address of interface VLAN-192 on Sw3 and confirm they are the same.

## Lab Tasks (Routing Basics)

5. From the IOS CLI of Sw3 attempt the following:
  - a. Ping the IPv4 address assigned to interface Gigabit5 on CSR1. This ping should be successful.
  - b. Ping the IPv4 address assigned to interface Gigabit2 on CSR1. This ping should fail because Sw3 has no IP reachability to that subnet/network.
6. From the Terminal app of the Ubuntu host, attempt the following:
  - a. Ping the IPv4 address of 3.3.3.3 assigned to interface VLAN-3 on Sw3. This ping should fail because Ubuntu is not connected to it and has no route to it.
  - b. You can confirm this by issuing the command “`route`” within the Terminal app

```
user@user-virtual-machine:/$ route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
default          _gateway        0.0.0.0         UG    100   0      0 ens160
default          one.one.one.one 0.0.0.0         UG    102   0      0 ens192
1.1.1.0          0.0.0.0         255.255.255.0   U     102   0      0 ens192
link-local      0.0.0.0         255.255.0.0     U     1000  0      0 ens160
192.168.1.0     0.0.0.0         255.255.255.0   U     101   0      0 ens224
192.168.200.0   0.0.0.0         255.255.252.0   U     100   0      0 ens160
```

You output may not match 100% to this example.



## Lab Tasks (Routing Basics)

---

7. Provide the Ubuntu host IPv4 static routes it will need to accomplish the rest of this lab using the following commands within the Terminal app:
  - a. `sudo route add -net 3.3.3.0/24 gw 192.168.1.254 ens224`
  - b. `sudo route add -net 21.21.21.0/24 gw 192.168.1.254 ens224`
  - c. `sudo route add -net 22.22.22.0/24 gw 192.168.1.254 ens224`
8. Confirm that your routes are now in the routing table of the Ubuntu host by viewing the output of the “`route`” command like you did previously.
9. From the Terminal app of the Ubuntu host, attempt the following:
  - a. Ping the IPv4 address of 3.3.3.3 assigned to interface VLAN-3 on Sw3. This ping should now succeed because Ubuntu has a route to it.

## Lab Tasks (Routing Basics)

---

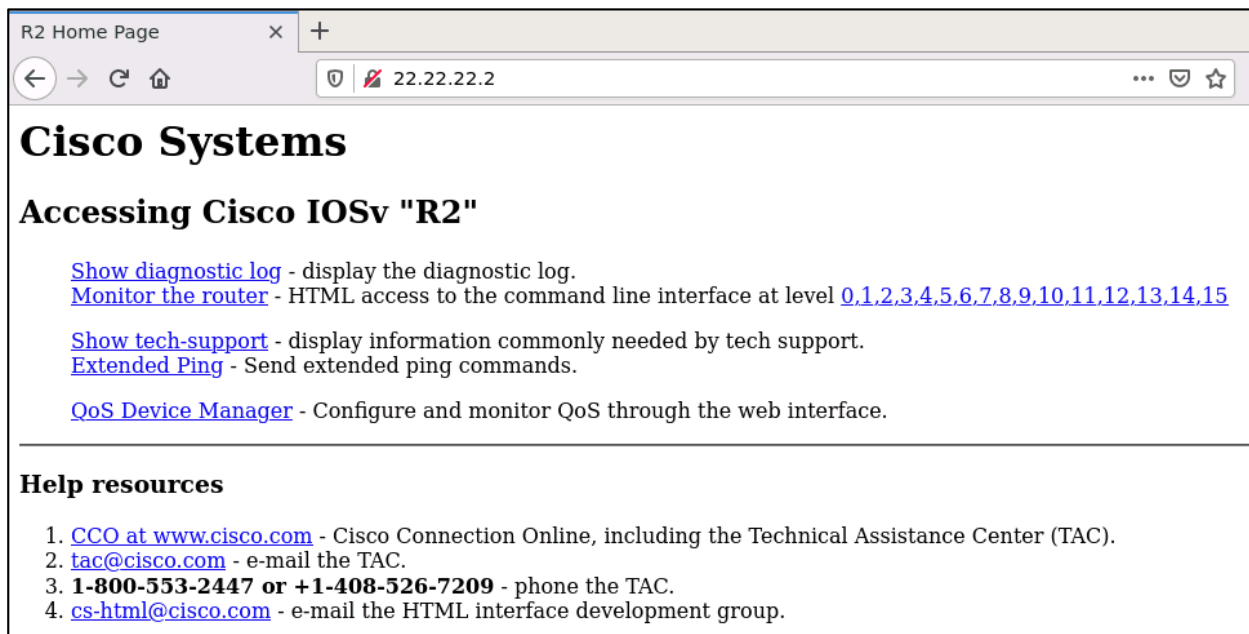
10. Your objective is to be able to ping from the Ubuntu host to the IPv4 address configured on interface Gigabit0/0 of R2. In order to accomplish this, configure IPv4 static routes in devices Sw3, CSR1 and R2 using the following guidelines:
  - a. Sw3 and CSR1 should contain one-or-more routes to specific destination prefixes with a mask of /24 and an IPv4 address as the next-hop for those routes.
  - b. R2 should contain a single static, default route so that it can reply to traffic sourced from the Ubuntu host.
11. Configure device R2 as an HTTP server with the following commands:

```
R2(config)#username Test privilege 15 password Test  
R2(config)#ip http server  
R2(config)#ip http authentication local
```

## Lab Tasks (Routing Basics)

---

12. Open a web browser in the Ubuntu box and browse to the web interface of R2 at <http://22.22.22.2>
13. Familiarize yourself with the basic Web GUI that IOS provides.



R2 Home Page

← → ↻ 🏠 22.22.22.2

# Cisco Systems

## Accessing Cisco IOSv "R2"

[Show diagnostic log](#) - display the diagnostic log.  
[Monitor the router](#) - HTML access to the command line interface at level [0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15](#)  
[Show tech-support](#) - display information commonly needed by tech support.  
[Extended Ping](#) - Send extended ping commands.  
[QoS Device Manager](#) - Configure and monitor QoS through the web interface.

---

### Help resources

1. [CCO at www.cisco.com](http://www.cisco.com) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. [tac@cisco.com](mailto:tac@cisco.com) - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. [cs-html@cisco.com](mailto:cs-html@cisco.com) - e-mail the HTML interface development group.



## Lab Tasks (Routing Basics)

---

14. Open Wireshark on the Ubuntu box and start capturing packets on the ENS-224 interface (connected to Gigabit0/1 on Sw3).
  - a. If your HTTP session to R2 is no longer running, start it up again.
  - b. Capture several packets associated with this HTTP session to R2
15. Answer the following questions about the packets you captured?
  - a. What was the initial TTL value of these packets? \_\_\_\_\_
  - b. What were the Layer-2 source and destination MAC addresses?  
L2 Src = \_\_\_\_\_ L2 Dest= \_\_\_\_\_
  - c. What were the Layer-3 source and destination IPv4 addresses?  
L3 Src = \_\_\_\_\_ L2=3 Dest= \_\_\_\_\_

## Lab Tasks (Routing Basics)

---

16. Stop your Wireshark capture of ENS-224 and turn it on again, this time capturing packets on the ENS-192 interface. You should still be capturing packets related to your web-browsing session to R2's GUI.
17. Answer the following questions about the packets you captured?
- Did the TTL value of these packets change as they were routed by Sw3?  
\_\_\_\_\_
  - Did the Layer-2 source and destination MAC addresses change as they were transmitted by Sw3?  
L2 Src = \_\_\_\_\_ L2 Dest= \_\_\_\_\_
  - Did the Layer-3 source and destination IPv4 addresses change as they were transmitted by Sw3?  
L3 Src = \_\_\_\_\_ L2=3 Dest= \_\_\_\_\_
18. Stop your wireshark capture and close your web browser on the Ubuntu box



**Thanks For  
Participating!**





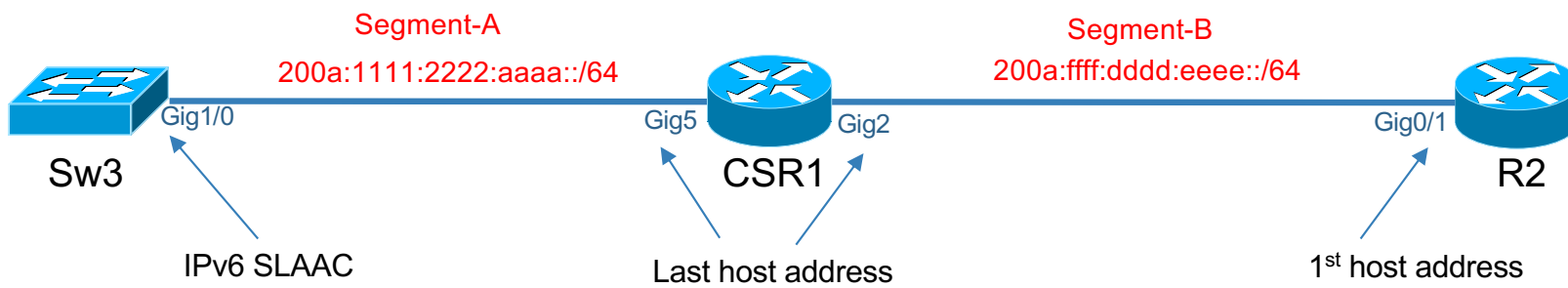
# CCNA 200-301 Bootcamp

IPv6 Basics

[ine.com](http://ine.com)

# Topology Diagram

---



## Lab Tasks (IPv6 Basics)

---

1. On the following devices, use the “config replace” command to load the configuration titled, “**IPv6-Basics**” from flash memory:
  - + Sw3
  - + CSR1
  - + R2

## Lab Tasks (IPv6 Basics)

---

2. On devices CSR1 and R2, configure IPv6 addresses as shown in the topology diagram on the relevant interfaces.
  1. Use the command, “show ipv6 interface brief” to write down the global and link-local addresses assigned to each device.
  2. From CSR1, ping the global IPv6 address you assigned to R2
  3. From CSR1, ping the Link-Local IPv6 address R2 dynamically assigned to itself.
3. Configure CSR1 to support incoming IPv6 Telnet sessions as long as they supply the username of “INE” and password of “Cisco”

## Lab Tasks (IPv6 Basics)

---

4. On R2, configure a static IPv6 route so that it has reachability to all IPv6 addresses on Segment-A.
5. Verify that your IPv6 static route is correct by:
  - a. Viewing the IPv6 Routing Table on R2
  - b. IPv6 Telnetting from R2 to CSR1's IPv6 address on Segment-A

## Lab Tasks (IPv6 Basics)

---

6. On the Ubuntu host, enable the Wireshark application and start capturing on interface ENS-192
7. Move over to Sw3 and do the following:
  - a. Disable interface Gigabit1/0
  - b. Convert interface Gigabit1/0 into a routed port
  - c. Configure interface Gigabit1/0 to obtain an IPv6 address via SLAAC
  - d. Enable interface Gigabit1/0
8. On the Ubuntu host, watch the IPv6 Neighbor Discovery (and SLAAC) process via the packets you captured on Wireshark

**NOTE:** If Sw3 doesn't receive the IPv6 packets you expected from CSR1 remember that there is an IPv6-related Global Configuration command on CSR1 to enable it to respond to the SLAAC process on Sw3

## Lab Tasks (IPv6 Basics)

---

4. On Sw3, configure an IPv6 static default route pointing to the IPv6 address of CSR1 (Gigabit5) as the next-hop.
5. If your static, default route was configured correctly, you should be able to ping the IPv6 address of R2 from Sw3



**Thanks For  
Participating!**



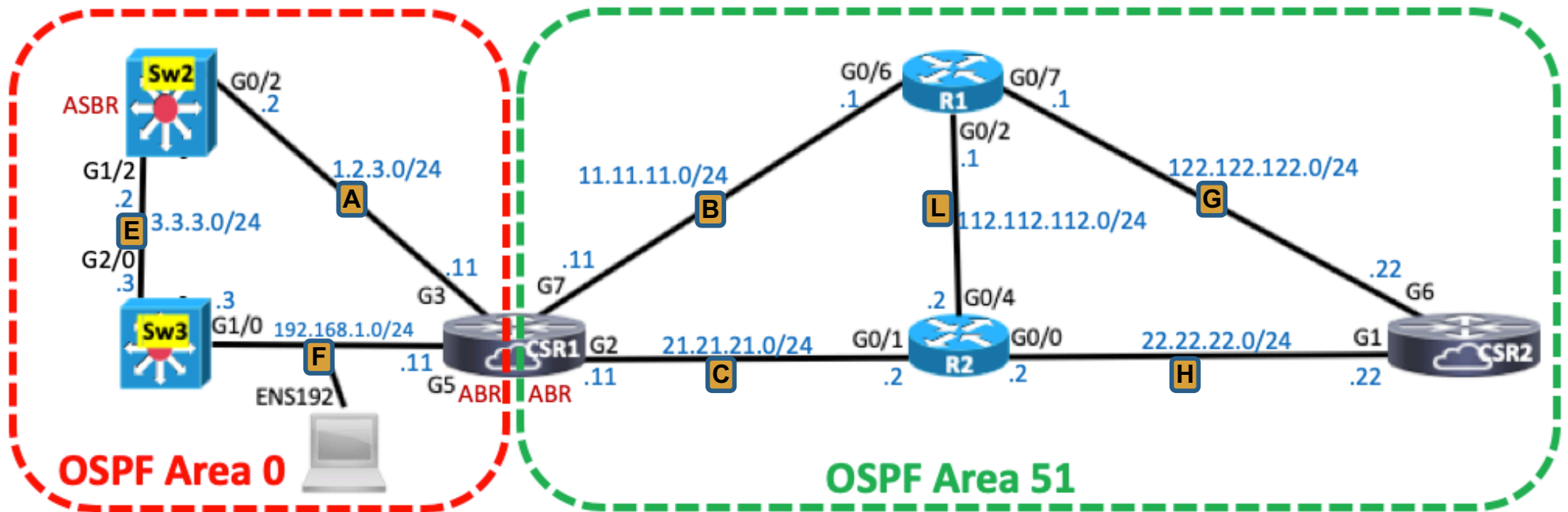


# CCNA 200-301 Bootcamp

OSPF Routing

[ine.com](http://ine.com)

# Topology Diagram



## Lab Tasks (OSPF Routing)

---

1. Use the “config replace” command to load the configuration titled, “**OSPF-Routing**” from flash memory on all devices shown in the topology diagram.
2. Configure OSPFv2 (for IPv4) on all devices with links in OSPF Area-51 using the following guidelines (**read through ALL guidelines on all slides prior to implementing any configuration**):
  - a) Devices CSR2 and R1 should have OSPF activated on their networks via interface-level commands
  - b) Devices CSR1 and R2 should have OSPF activated on their networks via OSPF “network” commands utilizing wildcard masks that match the length of their networks.

## Lab Tasks (OSPF Routing)

---

### 3. Additional OSPF Area-51 Guidelines:

- c) On Segment-G, device CSR2 should be the OSPF Designated Router. This should be controlled by configuring an OSPF Router-ID on CSR2 that is higher than the Router-ID dynamically selected by R1.
  - i. Validate that you met this objective by viewing the output of “[show ip ospf interface Gigabit6](#)” on CSR2.
- d) On Segment-G, device R2 should be the OSPF Designated Router. This should be controlled by configuring an OSPF interface priority on R2 that is higher than the interface priority used by CSR2.
  - i. Validate that you met this objective by viewing the output of “[show ip ospf neighbor](#)” on CSR2.

## Lab Tasks (OSPF Routing)

### 4. Additional OSPF guidelines:

- e) View the IP Routing Table of CSR2 and take note of the path it is currently using to reach Segment-B (if all routers have been correctly configured for OSPF your Routing Table should look like this on CSR2):

```
CSR2#sho ip route ospf
Gateway of last resort is not set

 11.0.0.0/24 is subnetted, 1 subnets
O    11.11.11.0 [110/2] via 122.122.122.2, 00:02:26, GigabitEthernet6
 21.0.0.0/24 is subnetted, 1 subnets
O    21.21.21.0 [110/2] via 22.22.22.2, 00:01:38, GigabitEthernet1
 112.0.0.0/24 is subnetted, 1 subnets
O    112.112.112.0 [110/2] via 122.122.122.2, 00:01:26, GigabitEthernet6
O    112.112.112.0 [110/2] via 22.22.22.2, 00:01:23, GigabitEthernet1
CSR2#
```

- f) Notice that all OSPF routes in the table are currently “[Intra Area](#)” routes as denoted by the “O” preceding them.
- g) Modify OSPF cost values on whichever links you think are appropriate such that CSR2 selects interface Gigabit1 to reach Segment-B (11.11.11.0/24).

## Lab Tasks (OSPF Routing)

5. If you haven't already completed your OSPF Area-51 configurations, do so now.
6. OSPF Area-0 Guidelines:
  - a) Configure OSPF on devices Sw2 and Sw3 placing their interfaces into Area-0. You may use either interface-level or OSPF process-level commands to accomplish this.
  - b) On device CSR1, **disable/shutdown interface Gigabit5 and then** configure interfaces Gigabit3 and Gigabit5 into OSPF Area-0.
7. View the IP Routing Table of Sw3 and (with Gigabit5 disabled on CSR1) it should resemble the following:

```
Sw3#sho ip route ospf
```

OSPF Intra-Area Route

OSPF Inter-Area Routes

```
1.0.0.0/24 is subnetted, 1 subnets
0       1.2.3.0 [110/2] via 3.3.3.2, 00:16:07, GigabitEthernet2/0
11.0.0.0/24 is subnetted, 1 subnets
0 IA    11.11.11.0 [110/3] via 3.3.3.2, 00:00:14, GigabitEthernet2/0
21.0.0.0/24 is subnetted, 1 subnets
0 IA    21.21.21.0 [110/3] via 3.3.3.2, 00:00:14, GigabitEthernet2/0
22.0.0.0/24 is subnetted, 1 subnets
0 IA    22.22.22.0 [110/4] via 3.3.3.2, 00:00:14, GigabitEthernet2/0
112.0.0.0/24 is subnetted, 1 subnets
0 IA    112.112.112.0 [110/4] via 3.3.3.2, 00:00:14, GigabitEthernet2/0
122.0.0.0/24 is subnetted, 1 subnets
0 IA    122.122.122.0 [110/4] via 3.3.3.2, 00:00:14, GigabitEthernet2/0
Sw3#
```

## Lab Tasks (OSPF Routing)

---

8. Enable the Wireshark application on the Ubuntu host on interface ENS-192 so that you can watch the OSPF adjacency process between CSR1 and Sw3.
  - a. Go back to CSR1 and enable interface Gigabit5. Spend some time familiarizing yourself with the OSPF packet exchange as captured in Wireshark between CSR1 and Sw3.
  - b. Stop the Wireshark capture, but do not terminate the application.
9. On CSR1 once again disable Gigabit5 and then enable the command, “`debug ip ospf adj`” from Privileged EXEC mode.
  - a. Enable interface Gigabit5 and notice the debug output displaying how an adjacency is built between CSR1 and Sw2.
  - b. Compare the level of detail you see the in the debug output, to the level of detail you saw with your Wireshark packet capture.

The Cisco CCNA 200-301 exam does not require detailed knowledge of how OSPF Adjacencies are formed...but it's still good experience to glean what you can from packet captures and debug output.



## Lab Tasks (OSPF Routing)

---

10. Lastly, imagine if router CSR2 were connected to another large network that was running a different routing protocol (such as EIGRP or RIP).
- Imagine that CSR2 has learned all those non-OSPF routes and, wants to provide IP reachability to those remote networks to the routers speaking OSPF.
  - Let's simulate this by configuring a Loopback0 interface on CSR2 and provide it the IP address of 222.222.222.2/24. **Do NOT advertise this network into OSPF**
  - Configure an OSPF-related command on CSR2 such that it advertises an IPv4 default route to all OSPF routers.
    - You can verify this was successful by viewing the output of "show ip route ospf" in any router and you should see an ospf route for 0.0.0.0/0
    - From any device, you should now be able to ping the IP address that you placed on Loopback0 of CSR2.

Default route in Sw3's IP Routing Table.

```
O*E2  0.0.0.0/0 [110/1] via 192.168.1.253, 00:00:01, GigabitEthernet1/0
```

```
Sw3#ping 222.222.222.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 222.222.222.22, timeout is 2 seconds:
!!!!
```







**Thanks For  
Participating!**

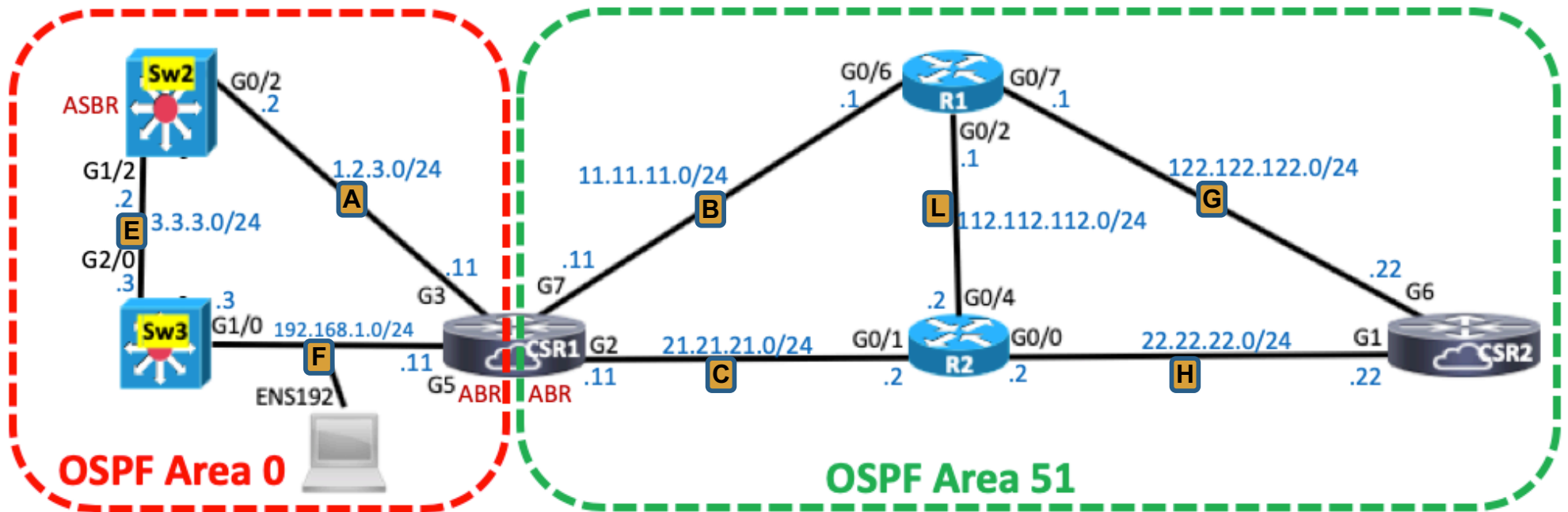


# CCNA 200-301 Bootcamp

Access-Lists

[ine.com](http://ine.com)

# Topology Diagram



## Lab Tasks (Access-Lists)

---

1. Use the “config replace” command to load the configuration titled, “**ACL-Lab**” from flash memory on all devices shown in the topology diagram.
2. Configure a standard, numbered access-list such that any IP packets sourced from Segment-A or Segment-E are not allowed to reach any hosts (including router interfaces) on Segment-G
  - a. IP packets sourced from any other segment should be unaffected by the ACL
  - b. **This ACL must be created using only two lines of ACEs (Access-Control Entries)**
  - c. This ACL must be implemented on as few interfaces as possible.
  - d. If implemented correctly, Sw2 should not be able to ping either of the interface IP addresses connected to Segment-G.
  - e. If implemented correctly, Sw3 should not be able to ping either of the interface IP addresses on Segment-G when those pings are sourced from Gig2/0 but it SHOULD be able to ping those same addresses if the pings are sourced from Gig1/0.

## Lab Tasks (Access-Lists)

Verification:

```
Sw2#ping 122.122.122.1 source Gig0/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.122.122.1, timeout is 2 seconds:
Packet sent with a source address of 1.2.3.2
U.U.U
Success rate is 0 percent (0/5)
Sw2#ping 122.122.122.1 source gig1/2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.122.122.1, timeout is 2 seconds:
Packet sent with a source address of 3.3.3.2
U.U.U
Success rate is 0 percent (0/5)
```

```
Sw3#ping 122.122.122.22 source Gig2/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.122.122.22, timeout is 2 seconds:
Packet sent with a source address of 3.3.3.3
U.U.U
Success rate is 0 percent (0/5)
Sw3#ping 122.122.122.22 source Gig1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.122.122.22, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.254
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

## Lab Tasks (Access-Lists)

---

3. Configure an extended, numbered access-list such that CSR1 is not allowed to establish a Telnet session to the address of 22.22.22.22 from any of CSR1's interfaces, however all other IP-based protocols are allowed.
  - a. You may NOT use the "access-class" command to accomplish this.
  - b. This ACL must be created using the fewest lines of ACEs possible (Access-Control Entries)
  - c. IP packets (Telnet or Ping) sourced from any other segment should be unaffected by the ACL
  - d. This ACL must be enforced ONLY on CSR1.
  - e. If implemented correctly, CSR1 should not be able to telnet to 22.22.22.22, however it should be able to ping that same address on CSR2.
  - f. All other routers in this topology should still be able to ping and telnet to CSR2's address of 22.22.22.22

## Lab Tasks (Access-Lists)

### Verification:

```
Sw3#ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Sw3#telnet 22.22.22.22
Trying 22.22.22.22 ... Open

User Access Verification

Username: INE
Password:
CSR2>
```

A prompt from CSR2 indicates a successful Telnet connection!

```
Sw2#ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Sw2#telnet 22.22.22.22
Trying 22.22.22.22 ... Open

User Access Verification

Username: INE
Password:
CSR2>exit
```

```
CSR1#ping 22.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/173/200 ms
CSR1#telnet 22.22.22.22
Trying 22.22.22.22 ...
% Connection timed out; remote host not responding
```



**Thanks For  
Participating!**



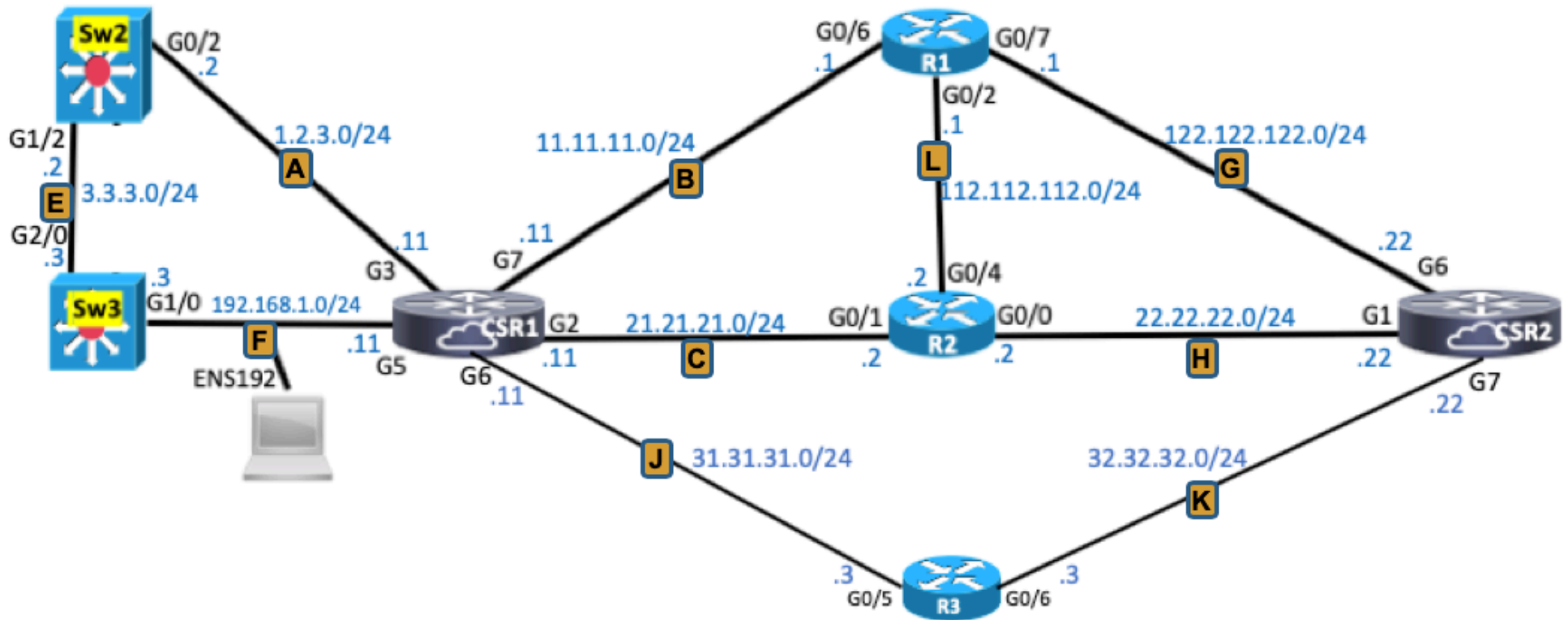


# CCNA 200-301 Bootcamp

Network Address Translation

[ine.com](https://ine.com)

# Topology Diagram



## Lab Tasks (NAT)

---

1. Use the “config replace” command to load the configuration titled, “**NAT-Lab**” from flash memory on all devices shown in the topology diagram.
2. Upon loading the configuration file, you should notice that (on CSR2) interfaces Gigabit1 and Gigabit7 are shutdown. This is intentional. Please leave them in this state.
3. CSR2 has also been configured with a Loopback interface with the address of 8.8.8.8/32. Login into either Sw2 or Sw3 and verify that they have learned of this address via OSPF.
  - a. If not, troubleshoot and resolve.

## Lab Tasks (Static NAT)

---

4. Configure Static NAT on R1 using the following guidelines:
  - a. The only packets that will be translated are those that arrive (ingress) on interface Gigabit0/6 and are routed (egress) to Gigabit0/7
  - b. Create a static NAT translation rule such that Sw3's source address of 192.168.1.3 is always translated to 122.122.122.2 as it sends any kind of IP packet through R1 (on its way to CSR2).

## Static NAT Verification

---

5. Confirm that Static NAT on R1 is working by:
  - a. Issue the command, “`show ip nat translation`” on R1. You should see a NAT translation entry even though no packets have even used it yet.
  - b. On CSR2 enable the command, “`debug ip icmp`” and then, from Sw3 ping the address of 8.8.8.8. The debug output on CSR2 should confirm that these pings have been received with a translated source address of 122.122.122.2
  - c. **From CSR2**, ping the translated address of 122.122.122.2. The pings should be successful. Since the address of 122.122.122.2 isn't configured on any interface, these successful pings prove that they are being translated to the actual destination address of 192.168.0.3 (Sw3)
  - d. On Sw3 enable the debug of “`debug ip icmp`” and from CSR2, ping 122.122.122.2 again. You should see debug output on Sw3 proving that these pings have been reverse NAT'd to 192.168.1.3
  - e. Disable all debugging with “`undebug all`”



## Lab Tasks (Dynamic NAT)

---

1. On CSR2, shutdown interface Gigabit6 and enable interface Gigabit1
2. On CSR1, confirm (by viewing the IP routing table) that it is now using interface Gigabit2 as the egress interface to reach 8.8.8.8
3. Configure Dynamic NAT on R2 using the following guidelines:
  - a. The only packets that will be translated are those that arrive (ingress) on interface Gigabit0/1 and are routed (egress) to Gigabit0/0
  - b. Configure Dynamic NAT such that packets sourced from Segment-A or Segment-F are translated as they go through R2 (on their way to CSR2's address of 8.8.8.8).
    - a. Your NAT Pool should be named "INE"
    - b. Your NAT Pool should allocate addresses from the range 22.22.22.3 through 22.22.22.10

## Dynamic NAT Verification

---

4. Confirm that Dynamic NAT on R2 is working by:
  - a. From Sw3 ping the address of 8.8.8.8 and immediately follow that by Telnetting to that same address (username = INE, password = cisco).
  - b. On R2 view the output of “`show ip nat translation`”. There should be two translation entries...one for the ICMP packets (pings) and another for the Telnet session (TCP)
  - c. On R2 view the output of “`show ip nat translation verbose`” and notice the different “timeout” and “left” values for each translation. You should see that the ICMP translation will age-out much more quickly than the TCP translation.
5. Feel free to also use other “show” and “debug” commands previously referenced in this lab.

## Lab Tasks (NAT Overloading)

---

1. On CSR2, shutdown interface Gigabit1 and enable interface Gigabit7
2. On CSR1, confirm (by viewing the IP routing table) that it is now using interface Gigabit6 as the egress interface to reach 8.8.8.8
3. Configure PAT (NAT Overloading) on R3 using the following guidelines:
  - a. The only packets that will be translated are those that arrive (ingress) on interface Gigabit0/5 and are routed (egress) to Gigabit0/6
  - b. Configure PAT such that packets sourced from Segment-A or Segment-F are translated as they go through R3 (on their way to CSR2's address of 8.8.8.8).
    - a. All packets should be translated to the same source address as that configured on Interface Gigabit0/6



## NAT Overload Verification

---

4. Confirm that PAT on R3 is working by:
  - a. From Sw3 ping the address of 8.8.8.8 and immediately follow that by Telnetting to that same address (username = INE, password = cisco).
  - b. Move to Sw2 and also Telnet to 8.8.8.8 from this device.
  - c. On R3 view the output of “`show ip nat translation`”. There should be two translation entries...one for the ICMP packets (pings) and another for the Telnet session (TCP). Both flows of traffic should have been translated to the same source IP address of 32.32.32.3
5. Feel free to also use other “show” and “debug” commands previously referenced in this lab.



**Thanks For  
Participating!**



# CCNA 200-301 Bootcamp

Essential WLAN Controller Configuration

[ine.com](http://ine.com)

## Lab Tasks (WLC Configuration)

---

1. From the Ubuntu host, open a web browser and browse to the Cisco 9800 WLAN Controller at 172.16.1.100
  - a. Username = cisco
  - b. Password = cisco

**NOTE:** If you see, “*Warning: Potential Security Risk Ahead*” click on “**Advanced**” followed by “**Accept the risk and continue**”

## Lab Tasks (WLC Configuration)

---

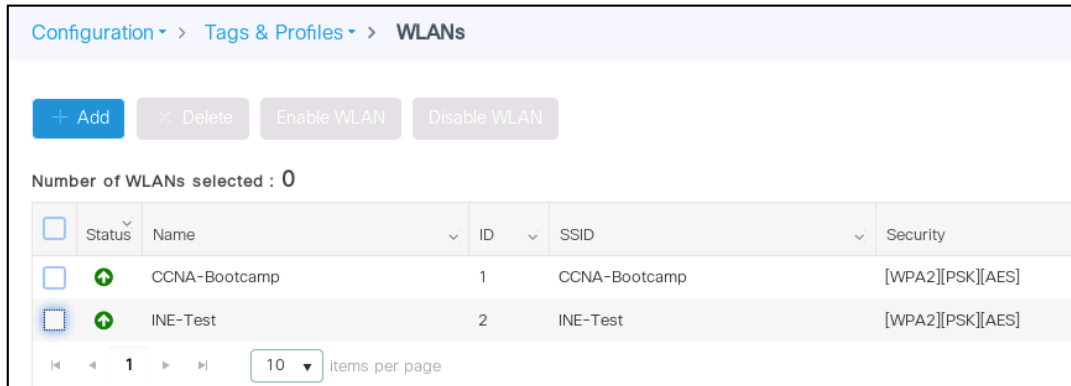
2. Go through the “Configuration Setup Wizard”.
  - a. If a value is not specified below, leave it to its default value.
3. Input the following non-default values into relevant menus or pull-down items:
  - a) **Wireless Management Settings**
    - i. VLAN = 1
    - ii. Wireless Management IP = 133.133.133.133
    - iii. Subnet Mask = 255.255.255.0
    - iv. Default Gateway = 133.133.133.1
  - b) **Wireless Network Settings**
    - i. Create a new WLAN called “CCNA-Bootcamp”
    - ii. Pre-Shared Key = INE12345
  - c) **Advanced Settings**
    - i. Password = INE98765
4. Finish/Submit your Configuration Setup Wizard



## Lab Tasks (WLC Configuration)

5. From the main Dashboard, create a new WLAN with these settings:
- WLAN name = INE-Test
  - Status = Enabled
  - Security settings:
    - WPA + WPA2
    - AES (CCMP 128) encryption (default)
    - Key management = PSK (pre-shared key)
    - Pre-Shared Key = INE-Rocks

Verification



The screenshot shows the 'WLANs' configuration page. At the top, there are navigation links for 'Configuration', 'Tags & Profiles', and 'WLANs'. Below the navigation are four buttons: '+ Add', 'Delete', 'Enable WLAN', and 'Disable WLAN'. A status indicator shows 'Number of WLANs selected : 0'. The main content is a table with columns for 'Status', 'Name', 'ID', 'SSID', and 'Security'. Two WLANs are listed: 'CCNA-Bootcamp' (ID 1) and 'INE-Test' (ID 2). Both have a status of 'Enabled' (indicated by a green plus icon) and a security profile of '[WPA2][PSK][AES]'. At the bottom, there is a pagination control showing '1' items per page.

Status	Name	ID	SSID	Security
Enabled	CCNA-Bootcamp	1	CCNA-Bootcamp	[WPA2][PSK][AES]
Enabled	INE-Test	2	INE-Test	[WPA2][PSK][AES]





**Thanks For  
Participating!**



# CCNA 200-301 Bootcamp

Applying QoS Policies To WLANs

[ine.com](http://ine.com)



## Lab Tasks (WLC Configuration)

---

1. From the Ubuntu host, open a web browser and browse to the Cisco 9800 WLAN Controller at 172.16.1.100
  - a. Username = cisco
  - b. Password = cisco

**NOTE:** If you see, “**Warning: Potential Security Risk Ahead**” click on “**Advanced**” followed by “**Accept the risk and continue**”
2. Apply the “**Platinum**” Precious Metal QoS Policy to the “CCNA Bootcamp” WLAN you created in the previous lab.
  - a. This policy should be applied against both upstream and downstream traffic in this WLAN
  - b. You may name your new Policy and Tag whatever you wish

## Lab Verification

---

WLAN-POLICY Maps: 1

+ Add    × Delete

	WLAN Profile	Policy Profile
<input type="checkbox"/>	CCNA-Bootcamp	Platinum-QoS

Your profile name will differ depending on whatever you selected.



**Thanks For  
Participating!**