



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

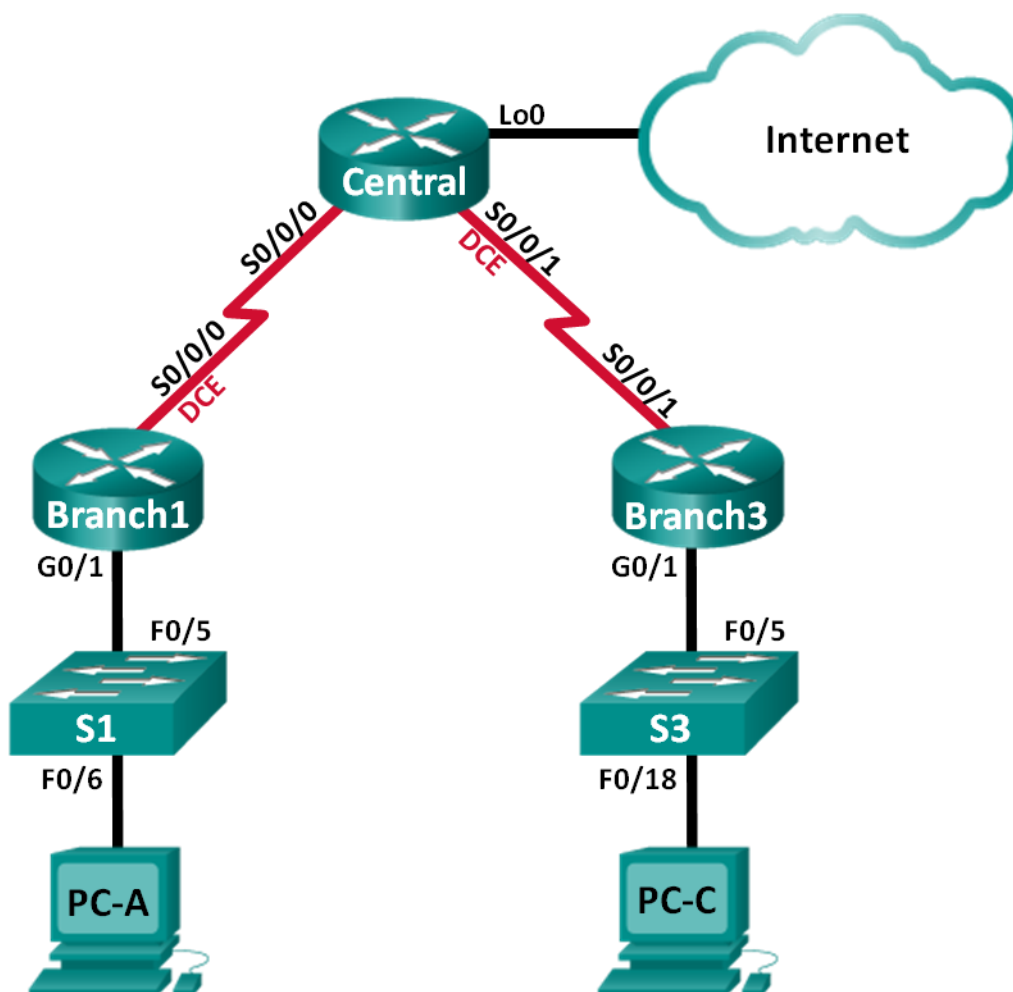
Wide Area Networks
Lab Manual
ACCA6018

Computer Networks and Cyber Security
Applied Computing Portfolio
Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea

Module Leader
Dr Kapilan Radhakrishnan

Lab 1 – Configuring Basic PPP with Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Branch1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
Central	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
Branch3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure PPP Encapsulation

Part 3: Configure PPP CHAP Authentication

Background / Scenario

The Point-to-Point Protocol (PPP) is a very common Layer 2 WAN protocol. PPP can be used to connect from LANs to service provider WANs and for connection of LAN segments within an enterprise network.

In this lab, you will configure PPP encapsulation on dedicated serial links between the branch routers and a central router. You will configure PPP Challenge Handshake Authentication Protocol (CHAP) on the PPP serial links. You will also examine the effects of the encapsulation and authentication changes on the status of the serial link.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

-
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
 - 2 PCs (Windows with terminal emulation program, such as Tera Term)
 - Console cables to configure the Cisco IOS devices via the console ports
 - Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses, routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the Topology, and cable as necessary.

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure the device name.
- Encrypt plaintext passwords.
- Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Set console logging to synchronous mode.
- Apply the IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces.
- Set the clock rate to **128000** for DCE serial interfaces.
- Create **Loopback0** on the Central router to simulate access to the Internet and assign an IP address according to the Addressing Table.

Step 4: Configure routing.

- Enable single-area OSPF on the routers and use a process ID of 1. Add all the networks, except 209.165.200.224/27 into the OSPF process.
- Configure a default route to the simulated Internet on the Central router using Lo0 as the exit interface and redistribute this route into the OSPF process.
- Issue the **show ip route ospf**, **show ip ospf interface brief**, and **show ip ospf neighbor** commands on all routers to verify that OSPF is configured correctly. Take note of the router ID for each router.

Step 5: Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 6: Verify end-to-end connectivity.

All devices should be able to ping other devices in the Topology. If not, troubleshoot until you can establish end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Step 7: Save your configurations.**Part 2: Configure PPP Encapsulation****Step 1: Display the default serial encapsulation.**

On the routers, issue **show interfaces serial *interface-id*** to display the current serial encapsulation.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1003 packets input, 78348 bytes, 0 no buffer
    Received 527 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1090 packets output, 80262 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    2 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
```

What is the default serial encapsulation for a Cisco router? _____

Step 2: Change the serial encapsulation to PPP.

- a. Issue the **encapsulation ppp** command on the S0/0/0 interface for the Branch1 router to change the encapsulation from HDLC to PPP.

```
Branch1(config)# interface s0/0/0
```

```
Branch1(config-if)# encapsulation ppp
```

```
Branch1(config-if)#
```

```
Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
Branch1(config-if)#
```

```
Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
```

- b. Issue the command to display the line status and line protocol for interface S0/0/0 on the Branch1 router. Document the command issued. What is current interface status for S0/0/0?

-
- c. Issue the **encapsulation ppp** command on interface S0/0/0 for the Central router to correct the serial encapsulation mismatch.

```
Central(config)# interface s0/0/0
```

```
Central(config-if)# encapsulation ppp
```

```
Central(config-if)#
```

```
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

```
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

- d. Verify that interface S0/0/0 on both Branch1 and Central routers is up/up and is configured with PPP encapsulation.

What is the status of the PPP Link Control Protocol (LCP)? _____

Which Network Control Protocol (NCP) protocols have been negotiated?

```
Branch1# show interfaces s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
```

```
Hardware is WIC MBRD Serial
```

```
Internet address is 10.1.1.1/30
```

```
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation PPP, LCP Open
```

```
Open: IPCP, CDPCP, loopback not set
```

```
Keepalive set (10 sec)
```

```
Last input 00:00:00, output 00:00:00, output hang never
```

```
Last clearing of "show interface" counters 00:03:58
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  77 packets input, 4636 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
117 packets output, 5800 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets
22 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
18 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Central# **show interfaces s0/0/0**

Serial0/0/0 is up, line protocol is up

```
Hardware is WIC MBRD Serial
Internet address is 10.1.1.2/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
Last clearing of "show interface" counters 00:01:20
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  41 packets input, 2811 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
40 packets output, 2739 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Step 3: Intentionally break the serial connection.

- a. Issue the **debug ppp** commands to observe the effects of changing the PPP configuration on the Branch1 router and the Central router.

```
Branch1# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch1# debug ppp packet
PPP packet display debugging is on
```

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central# debug ppp packet
PPP packet display debugging is on
```

- b. Observe the debug PPP messages when traffic is flowing on the serial link between the Branch1 and Central routers.

```
Branch1#
Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
```

```
Central#
Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic 0x8CE1F65F
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic 0x73885AF2
Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
```

- c. Break the serial connection by returning the serial encapsulation to HDLC for interface S0/0/0 on the Branch1 router. Record the command used to change the encapsulation to HDLC.

-
- d. Observe the debug PPP messages on the Branch1 router. The serial connection has terminated, and the line protocol is down. The route to 10.1.1.2 (Central) has been removed from the routing table.

```
Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.295: PPP: NET STOP send to AAA.
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
```

```

Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.29
Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN
Branch1(config-if)#
Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

```

- e. Observe the debug PPP messages on the Central router. The Central router continues to attempt to establish a connection with Branch1 as indicated by the debug messages. When the interfaces are unable to establish a connection, the interfaces go back down again. Furthermore, OSPF cannot establish an adjacency with its neighbor due to the mismatched serial encapsulation.

```

Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address 10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN
Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message
Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]

```

```
.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING
.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:29:52.296: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
.Jun 20 02:29:54.308: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<output omitted>
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:10.436: Se0/0/0 LCP: MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<output omitted>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP: MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not running
```

```
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING
.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]
.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
```

What happens when one end of the serial link is encapsulated with PPP and the other end of the link is encapsulated with HDLC?

- f. Issue the **encapsulation ppp** command on the S0/0/0 interface for the Branch1 router to correct mismatched encapsulation.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
```

- g. Observe the debug PPP messages from the Branch1 router as the Branch1 and Central routers establish a connection.

```
Branch1(config-if)#
Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message
Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]
Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line
Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.399: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
```

```
Jun 20 03:01:59.407: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP: Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
<output omitted>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on Serial0/0/0 from
LOADING to FULL, Loading Done
Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]
```

- h. Observe the debug PPP messages from the Central router as the Branch1 and Central routers establish a connection.

```
Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10
Jun 20 03:01:59.393: Se0/0/0 LCP: MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating
Jun 20 03:01:59.393: PPP: NET STOP send to AAA.
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
```

```
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negotiated
Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0, address
10.1.1.1
Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<output omitted>
Jun 20 03:01:59.401: Se0/0/0 LCP: MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]
Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]
Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol not up
Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.433: Se0/0/0 IPCP: Address 10.1.1.2 (0x03060A010102)
Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP. state[Initial]
Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4
Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]
<output omitted>
Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open
Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
10.1.1.1
Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1
Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
```

```
.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
```

From the debug message, what phases does PPP go through when the other end of the serial link on the Central router is configured with PPP encapsulation?

What happens when PPP encapsulation is configured on each end of the serial link?

- i. Issue the **undebg all** (or **u all**) command on the Branch1 and Central routers to turn off all debugging on both routers.
- j. Issue the **show ip interface brief** command on the Branch1 and Central routers after the network converges. What is the status for interface S0/0/0 on both routers?
- k. Verify that the interface S0/0/0 on both Branch1 and Central routers are configured for PPP encapsulation.

Record the command to verify the PPP encapsulation in the space provided below.

-
- l. Change the serial encapsulation for the link between the Central and Branch3 routers to PPP encapsulation.

```
Central(config)# interface s0/0/1
```

```
Central(config-if)# encapsulation ppp
```

```
Central(config-if)#
```

```
Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
```

```
Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

```
Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
Branch3(config)# interface s0/0/1
```

```
Branch3(config-if)# encapsulation ppp
```

```
Branch3(config-if)#
```

```
Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
```

```
.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

```
.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1 from LOADING to FULL, Loading Done
```

- m. Verify that end-to-end connectivity is restored before continuing to Part 3.

Part 3: Configure PPP CHAP Authentication

Step 1: Verify that PPP encapsulation is configured on all serial interfaces.

Record the command used to verify that PPP encapsulation is configured.

Step 2: Configure PPP CHAP authentication for the link between the Central router and the Branch3 router.

- a. Configure a username for CHAP authentication.

```
Central(config)# username Branch3 password cisco
```

```
Branch3(config)# username Central password cisco
```

- b. Issue the **debug ppp** commands on the Branch3 router to observe the process, which is associated with authentication.

```
Branch3# debug ppp negotiation
```

```
PPP protocol negotiation debugging is on
```

```
Branch3# debug ppp packet
```

```
PPP packet display debugging is on
```

- c. Configure the interface S0/0/1 on Branch3 for CHAP authentication.

```
Branch3(config)# interface s0/0/1
```

```
Branch3(config-if)# ppp authentication chap
```

- d. Examine the debug PPP messages on the Branch3 router during the negotiation with the Central router.

```
Branch3(config-if)#
```

```
Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed
```

```
Jun 20 04:25:02.079: PPP: NET STOP send to AAA.
```

```
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]
```

```
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]
```

```
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]
```

```
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]
```

```
Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]
```

```
Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,  
changed state to down
```

```
Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not negotiated
```

```
.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN
```

```
.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0, address  
10.2.2.2
```

```
.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2
```

```
.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1  
from FULL to DOWN, Neighbor Down: Interface down or detached
```

```
.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]
```

```
.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING
```

```
.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction
```

```
.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line
```

```
.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]
```

```
<output omitted>
```

```
.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]
```

```
.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15
```

```
.Jun 20 04:25:02.091: Se0/0/1 LCP: AuthProto CHAP (0x0305C22305)
```

```
.Jun 20 04:25:02.091: Se0/0/1 LCP: MagicNumber 0xF7B20F10 (0x0506F7B20F10)
```

```
.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to Open]
```

```
.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end
```

```
.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"
```

```
.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open
```

```
.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]
```

```
.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"
```

```
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
```

```
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated User
```

```
.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User
.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol not up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP. state[Initial]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10
<output omitted>
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0, address
10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/0/1
from LOADING to FULL, Loading Done
.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333 link[cdp]
.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
```

From the PPP debug messages, what phases did the Branch3 router go through before the link is up with the Central router?

-
- e. Issue the **debug ppp authentication** command to observe the CHAP authentication messages on the Central router.

```
Central# debug ppp authentication
```

```
PPP authentication debugging is on
```

- f. Configure CHAP authentication on S0/0/1 on the Central router.

```
Central(config)# interface s0/0/1
```

```
Central(config-if)# ppp authentication chap
```

- g. Observe the debug PPP messages relating to CHAP authentication on the Central router.

```
Central(config-if)#
```

```
.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,  
changed state to down
```

```
.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from  
FULL to DOWN, Neighbor Down: Interface down or detached
```

```
.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction
```

```
.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line
```

```
.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]
```

```
.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"
```

```
.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"
```

```
.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
```

```
.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS
```

```
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname
```

```
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA
```

```
.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"
```

```
.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"
```

```
.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request
```

```
.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS
```

```
.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4
```

```
.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4
```

```
.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,  
changed state to up
```

```
.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from  
LOADING to FULL, Loading Done
```

- h. Issue the **undebg all** (or **u all**) command on the Central and Branch3 routers to turn off all debugging.

```
Central# undebg all
```

```
All possible debugging has been turned off
```

Step 3: Intentionally break the serial link configured with authentication.

- a. On the Central router, configure a username for use with Branch1. Assign **cisco** as the password.

```
Central(config)# username Branch1 password cisco
```

- b. On the Central and Branch1 routers, configure CHAP authentication on interface S0/0/0. What is happening with the interface?
-

Note: To speed up the process, shut down the interface and enable it again.

- c. Use a **debug ppp negotiation** command to examine what is happening.

```
Central# debug ppp negotiation
```

```
PPP protocol negotiation debugging is on
```

```
Central(config-if)#
```

```
.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP
.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message
.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]
.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING
.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction
.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15
.Jun 20 05:25:26.229: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP: MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 05:25:26.233: Se0/0/0 LCP: AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.233: Se0/0/0 LCP: MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to Stopping]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN
```

Explain what is causing the link to terminate. Correct the issue and document the command issued to correct the issue in the space provided below.

-
-
- d. Issue the **undebug all** command on all routers to turn off debugging.
 - e. Verify end-to-end connectivity.

Reflection

1. What are the indicators that you may have a serial encapsulation mismatch on a serial link?

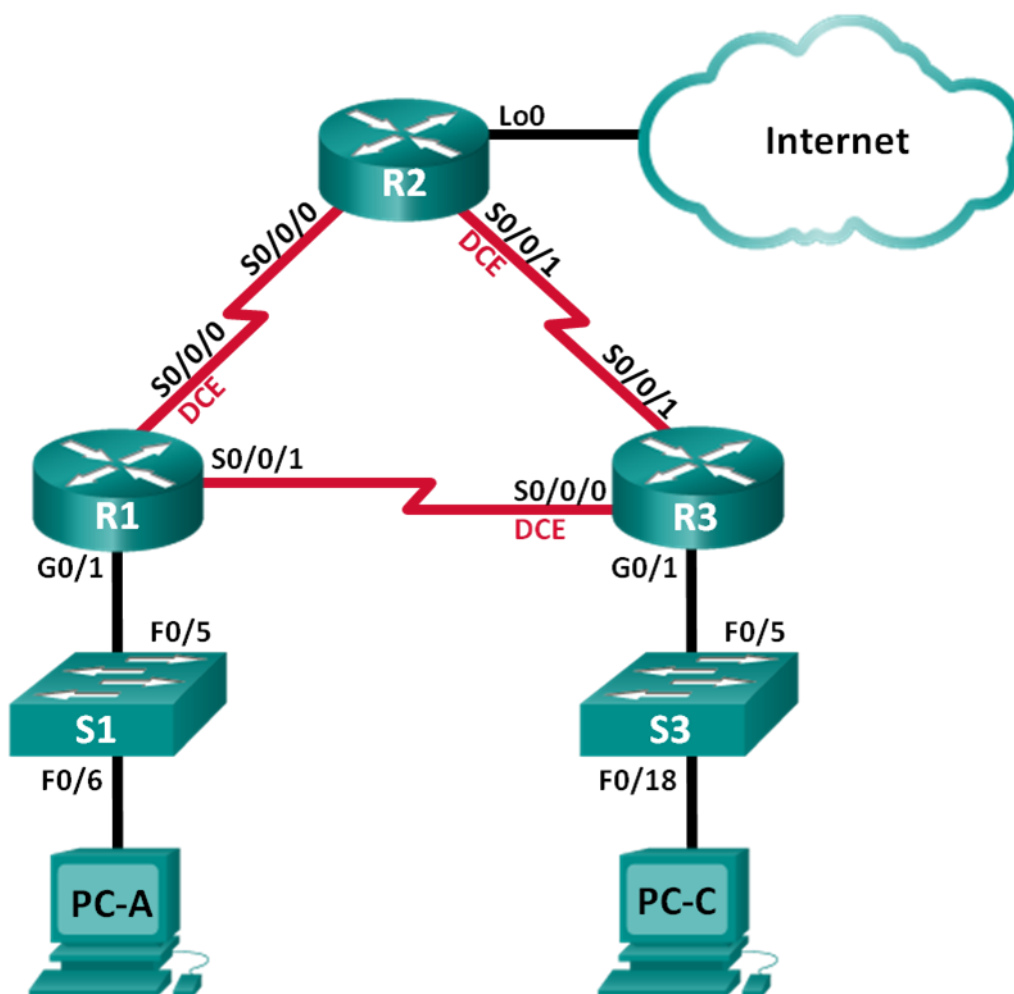
2. What are the indicators that you may have an authentication mismatch on a serial link?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 2 – Troubleshooting Basic PPP with Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot the Data Link Layer

Part 3: Troubleshoot the Network Layer

Background / Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your manager has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Ensure that all of the serial links use PPP CHAP authentication, and that all of the networks are reachable.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

In Part 1, you will set up the network topology, configure basic settings on the PC hosts, and load configurations on the routers.

Step 1: Cable the network as shown in the topology.

Step 2: Configure the PC hosts.

Step 3: Load router configurations.

Load the following configurations into the appropriate router. All routers have the same passwords. The privileged EXEC mode password is **class**. The password for console and vty access is **cisco**. All serial interfaces should be configured with PPP encapsulation and authenticated with CHAP using the password of **chap123**.

Router R1 Configuration:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
interface s0/0/1
 ip address 192.168.31.1 255.255.255.252
 encapsulation ppp
```

```
    ppp authentication pap
exit
router ospf 1
    router-id 1.1.1.1
    network 192.168.1.0 0.0.0.255 area 0
    network 192.168.12.0 0.0.0.3 area 0
    network 192.168.13.0 0.0.0.3 area 0
    passive-interface g0/1
exit
line con 0
    password cisco
    logging synchronous
    login
line vty 0 4
    password cisco
    login
```

Router R2 Configuration:

```
hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
interface lo0
    ip address 209.165.200.225 255.255.255.252
interface s0/0/0
    ip address 192.168.12.2 255.255.255.252
    encapsulation ppp
    ppp authentication chap
    no shutdown
interface s0/0/1
    ip address 192.168.23.1 255.255.255.252
    clock rate 128000
no shutdown
exit
router ospf 1
    router-id 2.2.2.2
    network 192.168.12.0 0.0.0.3 area 0
    network 192.168.23.0 0.0.0.3 area 0
```

```
default-information originate
exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
```

Router R3 Configuration:

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
interface s0/0/0
ip address 192.168.13.2 255.255.255.252
clock rate 128000
encapsulation ppp
ppp authentication chap
no shutdown
interface s0/0/1
ip address 192.168.23.2 255.255.255.252
encapsulation ppp
ppp authentication chap
no shutdown
exit
router ospf 1
router-id 3.3.3.3
network 192.168.13.0 0.0.0.3 area 0
network 192.168.23.0 0.0.0.3 area 0
passive-interface g0/1
line con 0
password cisco
```

```
logging synchronous
login
line vty 0 4
password cisco
login
```

Step 4: Save your running configuration.

Part 2: Troubleshoot the Data Link Layer

In Part 2, you will use **show** commands to troubleshoot data link layer issues. Be sure to verify settings, such as clock rate, encapsulation, CHAP, and usernames/passwords.

Step 1: Examine the R1 configuration.

- a. Use the **show interfaces** command to determine whether PPP has been established on both serial links. From the **show interfaces** results for S0/0/0 and S0/0/1, what are possible issues with the PPP links?

- b. Use the **debug ppp authentication** command to view real-time PPP authentication output during troubleshooting.

```
R1# debug ppp authentication
PPP authentication debugging is on
```

- c. Use the **show run interface s0/0/0** command to examine the settings on S0/0/0. Resolve all problems found for S0/0/0. Record the commands used to correct the configuration.

After correcting the issue, what information does the debug output provide?

- d. Use the **show run interface s0/0/1** command to examine the settings on S0/0/1. Resolve all problems found for S0/0/1. Record the commands used to correct the configuration.

After correcting the issue, what information does the debug output provide?

-
- e. Use the **no debug ppp authentication** or **undebug all** command to turn off the debug PPP output.
 - f. Use the **show running-config | include username** command to verify the correct username and password configurations.

Resolve all problems found. Record the commands used to correct the configuration.

Step 2: Examine the R2 configuration.

- a. Use the **show interfaces** command to determine if PPP has been established on both serial links.
Have all links been established? _____

If the answer is no, which links need to be examined? What are the possible issues?

- b. Use the **show run interface** command to examine links that have not been established.
Resolve all problems found for the interfaces. Record the commands used to correct the configuration.
-
-
-

- c. Use the **show running-config | include username** command to verify the correct username and password configurations.
Resolve all problems found. Record the commands used to correct the configuration.
-
-
-

- d. Use the **show ppp interface serial** command for the serial interface that you are troubleshooting.
Has the link been established? _____

Step 3: Examine the R3 configuration.

- a. Use the **show interfaces** command to determine whether PPP has been established on both serial links.
Have all links been established? _____

If the answer is no, which links need to be examined? What are the possible issues?

- b. Using the **show run interface** command to examine on any serial link that has not been established.

Resolve all problems found on the interfaces. Record the commands used to correct the configuration.

- c. Use the **show running-config | include username** command to verify the correct username and password configurations.

Resolve all problems found. Record the commands used to correct the configuration.

- d. Use the **show interface** command to verify that serial links have been established.
- e. Have all PPP links been established? _____
- f. Can PC-A ping Lo0? _____
- g. Can PC-A ping PC-C? _____

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Part 3: Troubleshoot the Network Layer

In Part 3, you will verify that Layer 3 connectivity is established on all interfaces by examining IPv4 and OSPF configurations.

Step 1: Verify that the interfaces listed in the Addressing Table are active and configured with the correct IP address information.

Issue the **show ip interface brief** command on all routers to verify that the interfaces are in an up/up state. Resolve all problems found. Record the commands used to correct the configuration.

Step 2: Verify OSPF Routing

Issue the **show ip protocols** command to verify that OSPF is running and that all networks are advertised. Resolve all problems found. Record the commands used to correct the configuration.

Can PC-A ping PC-C? _____

If connectivity does not exist between all hosts, then continue troubleshooting to resolve any remaining issues.

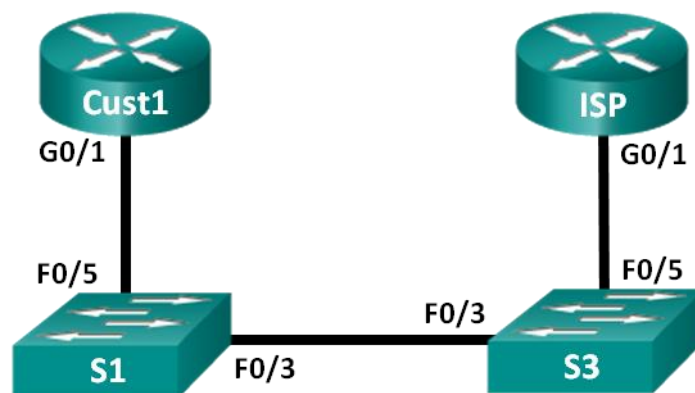
Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 3 – Configuring a Router as a PPPoE Client for DSL Connectivity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Cust1	G0/1	Learned via PPP	Learned via PPP	Learned via PPP
ISP	G0/1	N/A	N/A	N/A

Objectives

Part 1: Build the Network

Part 2: Configure the ISP Router

Part 3: Configure the Cust1 Router

Background / Scenario

ISPs often use Point-to-Point Protocol over Ethernet (PPPoE) on DSL links to their customers. PPP supports the assignment of IP address information to a device at the remote end of a PPP link. More importantly, PPP supports CHAP authentication. ISPs can check accounting records to see if a customer's bill has been paid, before letting them connect to the Internet.

In this lab, you will configure both the client and ISP side of the connection to set up PPPoE. Typically, you would only configure the client end.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco

IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Encrypt plaintext passwords.
- Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Set console logging to synchronous mode.
- Save your configuration.

Part 2: Configure the ISP Router

In Part 2, you configure the ISP router with PPPoE parameters for connection from the Cust1 router.

Note: Many of the ISP router PPPoE configuration commands are beyond the scope of the course; however, they are necessary for completion of the lab. They can be copied and pasted into the ISP router at the global configuration mode prompt.

- Create a local database username **Cust1** with a password of **ciscoppoe**.

```
ISP(config)# username Cust1 password ciscoppoe
```

- Create a pool of addresses that will be assigned to customers.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

- c. Create the Virtual Template and associate the IP address of G0/1 with it. Associate the Virtual Template with the pool of addresses. Configure CHAP to authenticate customers.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

- d. Assign the template to the PPPoE group.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

- e. Associate the bba-group with the G0/1 physical interface.

```
ISP(config)# interface g0/1
ISP(config-if)# pppoe enable group global
ISP(config-if)# no shutdown
```

Part 3: Configure the Cust1 Router

In Part 3, you will configure the Cust1 router with PPPoE parameters.

- a. Configure G0/1 interface for PPPoE connectivity.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

- b. Associate the G0/1 interface with a dialer interface. Use the username **Cust1** and password **ciscopppoe** configured in Part 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

- c. Set up a static default route pointing to the Dialer interface.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

- d. Set up debugging on the Cust1 router to display PPP and PPPoE negotiation.

```
Cust1# debug ppp authentication
```

```
Cust1# debug pppoe events
```

- e. Enable the G0/1 interface on the Cust1 router and observe the debug output as the PPPoE dialer session is established and CHAP authentication takes place.

```
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Jul 30 19:29:03.839: padi timer expired
*Jul 30 19:29:03.839: Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887: PPPOE: we've got our pado and the pado timer went off
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr prepared
```

- f. Issue a **show ip interface brief** command on the Cust1 router to display the IP address assigned by the ISP router. Sample output is shown below. By what method was the IP address obtained? _____

```
Cust1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down
Dialer1	10.0.0.1	YES	IPCP	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	unset	up	up

- g. Issue a **show ip route** command on the Cust1 router. Sample output is shown below.

Cust1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Dialer1
 10.0.0.0/32 is subnetted, 2 subnets
 C 10.0.0.1 is directly connected, Dialer1
 C 10.0.0.254 is directly connected, Dialer1

- h. Issue a **show pppoe session** on Cust1 router. Sample output is shown below.

Cust1# **show pppoe session**

1 client session

Uniq ID	PPPoE	RemMAC	Port	VT	VA	State
	SID	LocMAC			VA-st	Type
N/A	1	30f7.0da3.0b01	Gi0/1	Di1	Vi2	UP
		30f7.0da3.0bc1			UP	

- i. Issue a ping to 10.0.0.254 from the Cust1 router. The ping should be successful. If not, troubleshoot until you have connectivity.

Cust1# **ping 10.0.0.254**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Reflection

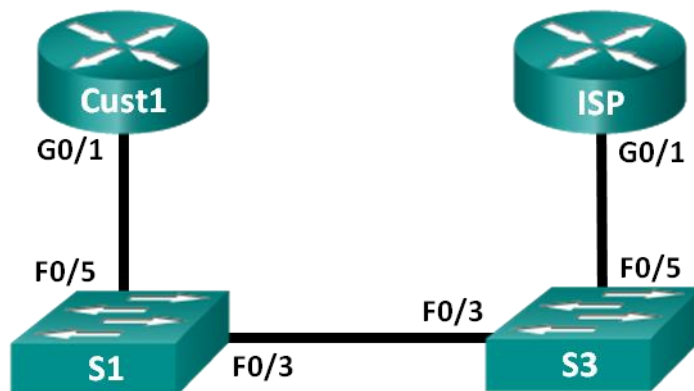
Why do ISPs who use DSL, primarily use PPPoE with their customers?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 4 – Troubleshoot PPPoE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Cust1	G0/1	Learned via PPP	Learned via PPP	Learned via PPP
ISP	G0/1	N/A	N/A	N/A

Objectives

Part 1: Build the Network

Part 2: Troubleshoot PPPoE on Cust1

Background / Scenario

ISPs sometimes use Point-to-Point Protocol over Ethernet (PPPoE) on DSL links to their customers. PPP supports the assignment of IP address information to a device at the remote end of a PPP link. More importantly, PPP supports CHAP authentication. ISPs can check accounting records to see if a customer's bill has been paid, before letting them connect to the Internet.

In this lab, you will troubleshoot the Cust1 router for PPPoE configuration problems.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Step 3: Copy the configurations on to routers.

- a. Copy and paste the Cust1 configuration to the Cust1 router.

```
hostname Cust1
enable secret class
no aaa new-model
no ip domain lookup
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
    pppoe enable group global
    pppoe-client dial-pool-number 1
    no shut
interface Dialer1
    mtu 1492
    ip address negotiated
    encapsulation ppp
    dialer pool 1
    ppp authentication chap callin
    ppp chap hostname Cust1
    ppp chap password 0 ciscopp
ip route 0.0.0.0 0.0.0.0 Dialer1
banner motd ^C
Unauthorized Access Prohibited.
^C
line con 0
```

```
password cisco
logging synchronous
login
line aux 0
line vty 0 4
password cisco
login
end
```

- b. Copy and paste the ISP configuration to the ISP router.

```
hostname ISP
enable secret class
username Cust1 password 0 ciscoppoe
bba-group pppoe global
virtual-template 1
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
pppoe enable group global
no shut
interface Virtual-Template1
ip address 10.0.0.254 255.255.255.0
mtu 1492
peer default ip address pool PPPoEPOOL
ppp authentication chap callin
ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
ip forward-protocol nd
banner motd ^C
Unauthorized Access Prohibited.
^C
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
end
```

Note: Many of the ISP router PPPoE configuration commands are beyond the scope of the course.

-
- c. Save the router configurations.

Part 2: Troubleshoot PPPoE on Cust1

In Part 2, you will troubleshoot PPPoE on the Cust 1 router. The privileged EXEC mode password is **class**, and console and vty passwords are **cisco**. The ISP has provided a username of **Cust1** and a password of **ciscoppoe** for PPPoE CHAP authentication.

The following log messages should be appearing on your console session to Cust1:

```
Cust1#
*Nov  5 22:53:46.999: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 22:53:47.003: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Nov  5 22:53:47.035: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Nov  5 22:53:47.039: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
Cust1#
```

Step 1: Verify that IPv4 Address is assigned to the Cust1 Dialer interface.

The Dialer virtual interface did not receive an IP address.

```
Cust1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down
Dialer1	unassigned	YES	manual	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	unset	down	down

Step 2: Debug PPP to determine if the problem is with authentication.

- a. Turn on debug for PPP authentication.

```
Cust1# debug ppp authentication
PPP authentication debugging is on
Cust1#
*Nov  5 23:09:00.283: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 23:09:00.287: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Nov  5 23:09:00.287: Vi2 PPP: Using dialer call direction
*Nov  5 23:09:00.287: Vi2 PPP: Treating connection as a callout
*Nov  5 23:09:00.287: Vi2 PPP: Session handle[8A000036] Session id[54]
*Nov  5 23:09:00.315: Vi2 PPP: No authorization without authentication
*Nov  5 23:09:00.315: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Nov  5 23:0
Cust1#9:00.315: Vi2 PPP: Sent CHAP SENDAUTH Request
```

```
*Nov  5 23:09:00.315: Vi2 PPP: Received SENDAUTH Response FAIL
*Nov  5 23:09:00.315: Vi2 CHAP: Using hostname from interface CHAP
*Nov  5 23:09:00.315: Vi2 CHAP: Using password from interface CHAP
*Nov  5 23:09:00.315: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Nov  5 23:09:00.315: Vi2 CHAP: I FAILURE id 1 len 25 msg is "Authentication failed"
*Nov  5 23:09:00.315: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Nov  5 23:09:00.319: %LINK-3
Cust1#-UPDOWN: Interface Virtual-Access2, changed state to down
Cust1#
```

- b. End debug mode.

```
Cust1# u all
All possible debugging has been turned off
Cust1#
```

Step 3: Verify that the PPPoE username and password matches what was given by the ISP.

- a. Display the running configuration; apply a filter to display only the Dialer section. Verify that the username and password matches what was provided by the ISP.

```
Cust1# show run | section Dialer
interface Dialer1
  mtu 1492
  ip address negotiated
  encapsulation ppp
  dialer pool 1
  ppp authentication chap callin
  ppp chap hostname Cust1
  ppp chap password 0 ciscoppo
ip route 0.0.0.0 0.0.0.0 Dialer1
```

- b. The problem appears to be with the password. Enter Global configuration mode and fix the ppp password.

```
Cust1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cust1(config)# interface Dialer1
Cust1(config-if)# ppp chap password ciscoppoe
Cust1(config-if)# end
Cust1#
*Nov  5 23:42:07.343: %SYS-5-CONFIG_I: Configured from console by console
Cust1#
*Nov  5 23:42:25.039: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 23:42:25.043: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
Cust1#
```

```
*Nov  5 23:42:25.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
```

Step 4: Verify PPPoE connectivity.

- a. Verify that this change resolved the problem and that an IP address has been assigned to the Dialer1 interface.

```
Cust1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down
Dialer1	10.0.0.1	YES	IPCP	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	unset	up	up

- b. Display the routing table to verify a route to the ISP router.

```
Cust1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C      10.0.0.1 is directly connected, Dialer1
C      10.0.0.254 is directly connected, Dialer1
```

- c. Display information about the active PPPoE sessions.

```
Cust1# show pppoe session
```

```
1 client session
```

Uniq ID	PPPoE	RemMAC	Port	VT	VA	State
	SID	LocMAC			VA-st	Type
N/A	1	30f7.0da3.1641	Gi0/1	Di1	Vi2	UP

30f7.0da3.0da1

UP

Step 5: Adjust the maximum segment size on the physical interface.

The PPPoE header adds an additional 8 bytes to each segment. To prevent TCP sessions from being dropped, the maximum segment size (MSS) needs to be adjusted to its optimum value on the physical interface.

- a. Display G0/1s configuration setting to see if the MSS has been adjusted.

```
Cust1# show run interface g0/1
Building configuration...

Current configuration : 136 bytes
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
end
```

- b. Adjust the MSS to its optimum value of 1452 bytes.

```
Cust1(config)# interface g0/1
Cust1(config-if)# ip tcp adjust-mss 1452
Cust1(config-if)# end
```

Reflection

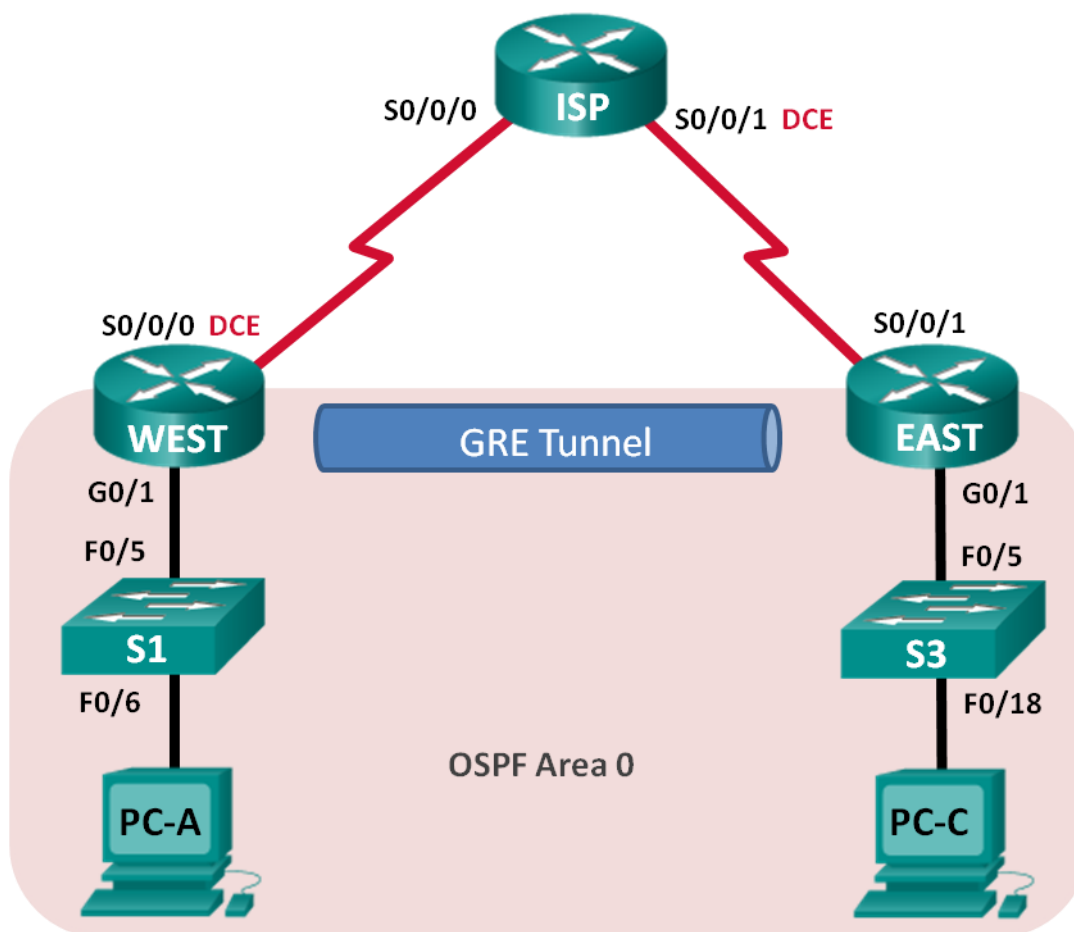
Explain why the TCP segment size needs to be adjusted for PPPoE.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 5 – Configuring a Point-to-Point GRE VPN Tunnel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	172.16.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
EAST	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure a GRE Tunnel

Part 3: Enable Routing over the GRE Tunnel

Background / Scenario

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of network layer protocols between two locations over a public network, such as the Internet.

GRE can be used with:

- Connecting IPv6 networks over IPv4 networks
- Multicast packets, such as OSPF, EIGRP, and streaming applications

In this lab, you will configure an unencrypted point-to-point GRE VPN tunnel and verify that network traffic is using the tunnel. You will also configure the OSPF routing protocol inside the GRE VPN tunnel. The GRE tunnel is between the WEST and EAST routers in OSPF area 0. The ISP has no knowledge of the GRE tunnel. Communication between the WEST and EAST routers and the ISP is accomplished using default static routes.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses, routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- Disable DNS lookup.
- Configure the device names.
- Encrypt plain text passwords.
- Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Set console logging to synchronous mode.
- Apply IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Do NOT configure the Tunnel0 interfaces at this time.
- Set the clock rate to **128000** for DCE serial interfaces.

Step 4: Configure default routes to the ISP router.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

```
EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Step 5: Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 6: Verify connectivity.

At this point, the PCs are unable to ping each other. Each PC should be able to ping its default gateway. The routers are able to ping the serial interfaces of the other routers in the topology. If not, troubleshoot until you can verify connectivity.

Step 7: Save your running configuration.**Part 2: Configure a GRE Tunnel**

In Part 2, you will configure a GRE tunnel between the WEST and EAST routers.

Step 1: Configure the GRE tunnel interface.

- a. Configure the tunnel interface on the WEST router. Use S0/0/0 on WEST as the tunnel source interface and 10.2.2.1 as the tunnel destination on the EAST router.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

- b. Configure the tunnel interface on the EAST router. Use S0/0/1 on EAST as the tunnel source interface and 10.1.1.1 as the tunnel destination on the WEST router.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source 10.2.2.1
EAST(config-if)# tunnel destination 10.1.1.1
```

Note: For the **tunnel source** command, either the interface name or the IP address can be used as the source.

Step 2: Verify that the GRE tunnel is functional.

- a. Verify the status of the tunnel interface on the WEST and EAST routers.

```
WEST# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	172.16.1.1	YES	manual	up	up
Serial0/0/0	10.1.1.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Tunnel0	172.16.12.1	YES	manual	up	up

```
EAST# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
-----------	------------	-----	--------	--------	----------

Embedded-Service-Engine0/0	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/1	172.16.2.1	YES	manual	up		up
Serial0/0/0	unassigned	YES	unset	administratively	down	down
Serial0/0/1	10.2.2.1	YES	manual	up		up
Tunnel0	172.16.12.2	YES	manual	up		up

- b. Issue the **show interfaces tunnel 0** command to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel.

What is the tunneling protocol used? What are the tunnel source and destination IP addresses associated with GRE tunnel on each router?

- c. Ping across the tunnel from the WEST router to the EAST router using the IP address of the tunnel interface.

WEST# **ping 172.16.12.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

- d. Use the **traceroute** command on the WEST to determine the path to the tunnel interface on the EAST router. What is the path to the EAST router?
-

- e. Ping and trace the route across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface.

What is the path to the WEST router from the EAST router? _____

With which interfaces are these IP addresses associated? Explain.

- f. The **ping** and **traceroute** commands should be successful. If not, troubleshoot before continuing to the next part.

Part 3: Enable Routing over the GRE Tunnel

In Part 3, you will configure OSPF routing so that the LANs on the WEST and EAST routers can communicate using the GRE tunnel.

After the GRE tunnel is set up, the routing protocol can be implemented. For GRE tunneling, a network statement will include the IP network of the tunnel, instead of the network associated with the serial interface. just like you would with other interfaces, such as Serial and Ethernet. Remember that the ISP router is not participating in this routing process.

Step 1: Configure OSPF routing for area 0 over the tunnel.

- a. Configure OSPF process ID 1 using area 0 on the WEST router for the 172.16.1.0/24 and 172.16.12.0/24 networks.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

- b. Configure OSPF process ID 1 using area 0 on the EAST router for the 172.16.2.0/24 and 172.16.12.0/24 networks.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Step 2: Verify OSPF routing.

- a. From the WEST router, issue the **show ip route** command to verify the route to 172.16.2.0/24 LAN on the EAST router.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

```
S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C      172.16.1.0/24 is directly connected, GigabitEthernet0/1
L      172.16.1.1/32 is directly connected, GigabitEthernet0/1
O      172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C      172.16.12.0/30 is directly connected, Tunnel0
L      172.16.12.1/32 is directly connected, Tunnel0
```

What is the exit interface and IP address to reach the 172.16.2.0/24 network?

-
- b. From the EAST router issue the command to verify the route to 172.16.1.0/24 LAN on the WEST router.

What is the exit interface and IP address to reach the 172.16.1.0/24 network?

Step 3: Verify end-to-end connectivity.

- a. Ping from PC-A to PC-C. It should be successful. If not, troubleshoot until you have end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

- b. Traceroute from PC-A to PC-C. What is the path from PC-A to PC-C?
-

Reflection

1. What other configurations are needed to create a secured GRE tunnel?

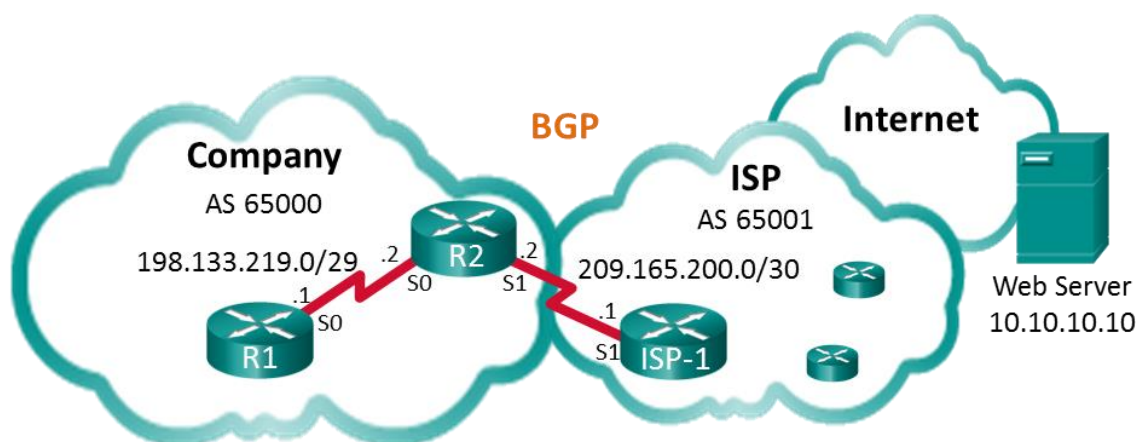
2. If you added more LANs to the WEST or EAST router, what would you need to do so that the network will use the GRE tunnel for traffic?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 6 - Configure and Verify eBGP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0 (DCE)	198.133.219.1	255.255.255.248
R2	S0/0/0	198.133.219.2	255.255.255.248
	S0/0/1 (DCE)	209.165.200.2	255.255.255.252
ISP-1	S0/0/1	209.165.200.1	255.255.255.252
Web Server		10.10.10.10	255.255.255.255

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure eBGP on R1

Part 3: Verify eBGP Configuration

Background / Scenario

In this lab you will configure eBGP for the Company. The ISP will provide the default route to the Internet. Once configuration is complete you will use various **show** commands to verify that the eBGP configuration is working as expected.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on R1 and R2 routers. You will also copy the provided configuration for ISP-1 on to that router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the network devices as necessary.

Step 3: Configure basic settings on R1 and R2.

- Disable DNS lookup to prevent the routers from attempting to translate incorrectly entered commands as though they were host names.
- Configure the hostnames according to the topology.
- Configure interfaces according to the Addressing Table.
- Save the running configuration to the startup configuration file.

Step 4: Copy configuration to ISP-1.

Copy and paste the following configuration to ISP-1.

```
hostname ISP-1
no ip domain-lookup
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
interface Serial0/0/1
 ip address 209.165.200.1 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 lo0
router bgp 65001
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 209.165.200.2 remote-as 65000
```

```
end
```

Part 2: Configure eBGP on R2

Configure R2 to become an eBGP peer with ISP-1. Refer to the Topology for BGP AS number information.

Step 1: Enable BGP and identify the AS number for the Company.

```
R2(config)# router bgp 65000
```

Step 2: Use the neighbor command to identify ISP-1 as the BGP peer.

```
R2(config-router)# neighbor 209.165.200.1 remote-as 65001
```

Step 3: Add the Company's network to the BGP table so it is advertised to ISP-1.

```
R2(config-router)# network 198.133.219.0 mask 255.255.255.248
```

Part 3: Verify eBGP Configuration

In Part 3, use the BGP verifications commands to verify that the BGP configuration is working as expected.

Step 1: Display the IPv4 routing table on R2.

```
R2# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

```
Gateway of last resort is 209.165.200.1 to network 0.0.0.0
```

```
B*    0.0.0.0/0 [20/0] via 209.165.200.1, 00:00:07
      198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C      198.133.219.0/29 is directly connected, Serial0/0/0
L      198.133.219.2/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.0/30 is directly connected, Serial0/0/1
L      209.165.200.2/32 is directly connected, Serial0/0/1
```

Step 2: Display the BGP table on R2.

```
R2# show ip bgp
BGP table version is 4, local router ID is 209.165.200.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 0.0.0.0	209.165.200.1	0		0	65001 i
*> 198.133.219.0/29	0.0.0.0	0		32768	i

Step 3: Display the BGP connection status on R2.

```
R2# show ip bgp summary
BGP router identifier 209.165.200.2, local AS number 65000
BGP table version is 4, main routing table version 4
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs
```

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
209.165.200.1	4	65001	12	11	4	0	0	00:06:56

Step 4: Display the IPv4 routing table on ISP-1.

Verify that the 198.133.218.0/29 network is being advertised to the ISP-1 router.

```
ISP-1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
```

+ - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Loopback0

10.0.0.0/32 is subnetted, 1 subnets

C 10.10.10.10 is directly connected, Loopback0

198.133.219.0/29 is subnetted, 1 subnets

B 198.133.219.0 [20/0] via 209.165.200.2, 00:00:25

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.0/30 is directly connected, Serial0/0/1

L 209.165.200.1/32 is directly connected, Serial0/0/1

Ping the Web Server from R1. Were the pings successful?

Reflection

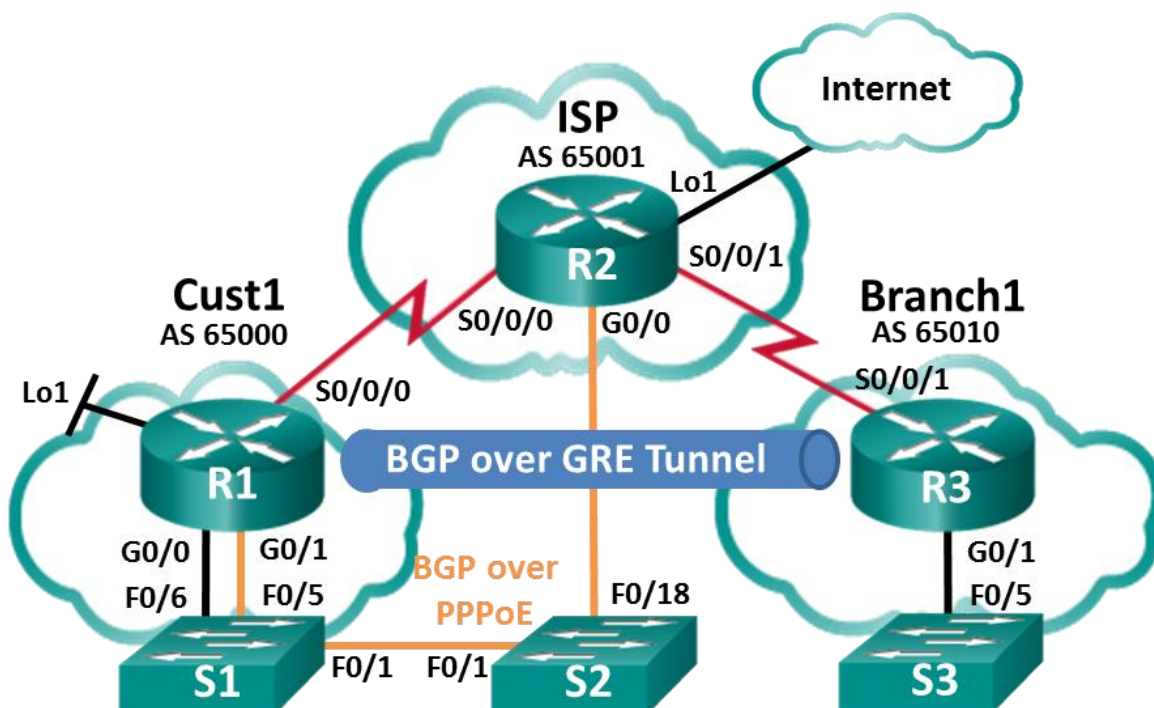
The topology used in this lab was created to demonstrate how to configure the BGP routing protocol. However, the BGP protocol would not normally be configured for a topology like this in the real world. Explain.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 7 – Configure a Branch Connection

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0	192.168.1.1	255.255.255.0
	G0/1	PPPoE Client	
	Lo1	209.165.200.49	255.255.255.240
	S0/0/0 (DCE)	209.165.200.81	255.255.255.252
R2	G0/0	PPPoE Provider	
	Lo1	209.165.200.65	255.255.255.240
	S0/0/0	209.165.200.82	255.255.255.252
	S0/0/1 (DCE)	209.165.200.85	255.255.255.252
R3	G0/1	192.168.3.1	255.255.255.0
	S0/0/1 (DCE)	209.165.200.86	255.255.255.252

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Configure a PPPoE Client Connection

Part 3: Configure a GRE Tunnel

Part 4: Configure BGP over PPPoE and BGP over a GRE Tunnel

Background / Scenario

In this lab, you will configure two separate WAN connections, a BGP route over a PPPoE connection, and a BGP route over a GRE tunnel. This lab is a test case scenario and does not represent a realistic BGP implementation.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS, Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

-
- Console cables to configure the Cisco IOS devices via the console ports
 - Ethernet cables and Serial cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

Step 1: Cable the network as shown in the topology.

Step 2: Load router configurations.

Copy and paste the following configurations into the appropriate routers and switch.

Cust 1 (R1) Configuration:

```
conf t
hostname Cust1
no cdp run
interface Loopback1
 ip address 209.165.200.49 255.255.255.240
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shut
interface Serial0/0/0
 ip address 209.165.200.81 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 s0/0/0 25
end
```

Note: In the Cust1 configuration above, CDP is disabled with the **no cdp run** command. The static default route with an administrative distance is manually configured to 25 instead of the default 1. The significance of these configurations will be explained later in the lab.

ISP (R2) Configuration:

```
conf t
hostname ISP
username Cust1 password 0 ciscoppoe
bba-group pppoe global
 virtual-template 1
interface Loopback 1
 ip address 209.165.200.65 255.255.255.240
interface GigabitEthernet0/0
 ip tcp adjust-mss 1452
 pppoe enable group global
 no shut
```

```
interface Serial0/0/0
  ip address 209.165.200.82 255.255.255.252
  no shut
interface Serial0/0/1
  ip address 209.165.200.85 255.255.255.252
  no shut
interface Virtual-Template1
  mtu 1492
  ip address 209.165.200.30 255.255.255.224
  peer default ip address pool PPPoEPOOL
  ppp authentication chap callin
router bgp 65001
  network 0.0.0.0
  neighbor 209.165.200.1 remote-as 65000
ip local pool PPPoEPOOL 209.165.200.1 209.165.200.20
ip route 0.0.0.0 0.0.0.0 Loopback1
end
```

Branch1 (R3) Configuration:

```
conf t
hostname Branch1
interface GigabitEthernet0/1
  ip address 192.168.3.1 255.255.255.0
  no shut
interface Serial0/0/1
  ip address 209.165.200.86 255.255.255.252
  no shut
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
end
```

S1 Configuration:

```
conf t
hostname S1
vlan 111
interface f0/6
  switchport mode access
  switchport access vlan 111
end
```

Note: Because S1 connects to two separate networks, G0/0 and G0/1 on Cust1, it is necessary to segment the switch into two separate VLANs, in this case VLAN111, and VLAN1.

Step 3: Save the configuration on all configured routers and switches.

Part 2: Configure a PPPoE Client Connection

In Part 2, following the PPPoE requirements listed below, you will configure Cust1 as the PPPoE client. The ISP router configuration is already complete.

PPPoE requirements for the Cust1 router:

- Configure an **interface Dialer1** with the following settings:
 - **a negotiated ip address**
 - **mtu 1492**
 - **ppp encapsulation**
 - **dialer pool 1**
 - **ppp chap callin authentication**
 - **ppp chap hostname Cust1**
 - **ppp chap password ciscoppoe (unencrypted)**
- Configure **G0/1** with the following settings:
 - **enable global pppoe**
 - **adjust the TCP maximum segment size to 1452**
 - **set the pppoe-client to dialer pool 1**

List the commands used to configure Cust1 as the PPPoE Client:

If the Cust1 router is configured correctly, it should receive an IP address from the ISP router. What IP address did Cust1 receive and on what interface? What command did you use to check for the IP address and interface?

Note: If Cust1 had CDP running on interface dialer1, it could produce the following repeating log message: *PPP: Outbound cdp packet dropped, NCP not negotiated.* To prevent this, CDP was globally turned off.

Part 3: Configure a GRE Tunnel

In Part 3, following the GRE requirements listed below, you will configure a GRE tunnel between Cust1 and Branch1.

GRE tunnel requirements:

- On Cust1 and Branch1, configure **interface Tunnel 0** with the following settings:
 - **IP address 192.168.2.1/24 and 192.168.2.2/24 respectively**
 - **Tunnel mode GRE over IP**
 - **Tunnel source interface and destination address using serial interfaces**

List the commands used to configure a GRE tunnel between Cust1 and Branch1:

How can you tell if the tunnel was created successfully? What command could you use to test the tunnel?

What would happen if Cust1 did not have a static default route? Test it by removing the static default route. What was the result? Make sure to replace the static default route, as shown in the Cust1 configuration in Part 1 Step2, before moving on.

Part 4: Configure BGP over PPPoE and BGP over a GRE Tunnel

In Part 4, following the BGP requirements listed below, you will configure BGP on Cust1 and Branch1. The ISP router configuration is already complete.

BGP requirements:

- On Cust1:
 - **Create a BGP routing process AS 65000**
 - **Advertise networks attached to Loopback 1 and G0/0**
 - **Configure BGP neighbors to the ISP and Branch1 routers**
- On Branch1:
 - **Create a BGP routing process AS 65010**
 - **Advertise the network attached to G0/1**
 - **Configure BGP neighbor to Cust1 only**

List the commands used to configure BGP on Cust1 and Branch1:

On Cust1, did you receive console messages regarding BGP neighbor relationships to ISP and Branch1?

On Cust1, can you ping the ISP at 209.165.200.30 over PPPoE? Can you ping the Branch1 local network at 192.168.3.1?

Check the routing table of Cust1. What routes were learned by BGP? There should be a route learned from both ISP and Branch1.

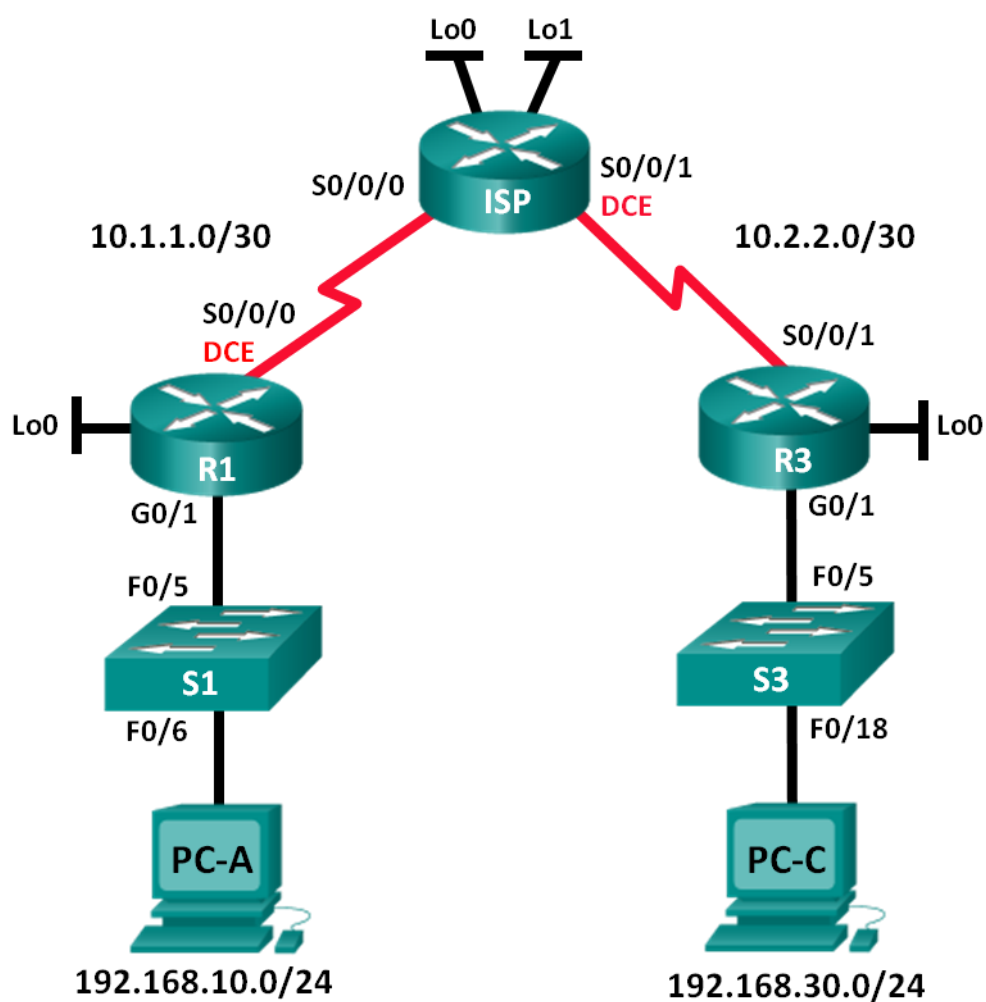
Examine the two routes learned by BGP in the Cust1 routing table. What do they show about routes in the network now?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 8 – Configuring and Verifying Extended ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

- Configure basic settings on PCs, routers, and switches.
- Configure OSPF routing on R1, ISP, and R3.

Part 3: Configure and Verify Extended Numbered and Named ACLs

- Configure, apply, and verify a numbered extended ACL.
- Configure, apply, and verify a named extended ACL.

Part 4: Modify and Verify Extended ACLs

Background / Scenario

Extended access control lists (ACLs) are extremely powerful. They offer a much greater degree of control than standard ACLs as to the types of traffic that can be filtered, as well as where the traffic originated and where it is going.

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router between R1 and R3 does not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router as you can only control and manage your own equipment.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure IP addresses on PC-A and PC-C.

Step 2: Configure basic settings on R1.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Create a loopback interface on R1.
- Configure interface IP addresses as shown in the Topology and Addressing Table.
- Configure a privileged EXEC mode password of **class**.

-
- f. Assign a clock rate of **128000** to the S0/0/0 interface.
 - g. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both the console and vty lines.
 - h. Enable web access on R1 to simulate a web server with local authentication for user **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Step 3: Configure basic settings on ISP.

- a. Configure the device name as shown in the topology.
- b. Create the loopback interfaces on ISP.
- c. Configure interface IP addresses as shown in the Topology and Addressing Table.
- d. Disable DNS lookup.
- e. Assign **class** as the privileged EXEC mode password.
- f. Assign a clock rate of **128000** to the S0/0/1 interface.
- g. Assign **cisco** as the console and vty password and enable Telnet access. Configure **logging synchronous** for both console and vty lines.
- h. Enable web access on the ISP. Use the same parameters as in Step 2h.

Step 4: Configure basic settings on R3.

- a. Configure the device name as shown in the topology.
- b. Create a loopback interface on R3.
- c. Configure interface IP addresses as shown in the Topology and Addressing Table.
- d. Disable DNS lookup.
- e. Assign **class** as the privileged EXEC mode password.
- f. Assign **cisco** as the console password and configure **logging synchronous** on the console line.
- g. Enable SSH on R3.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

- h. Enable web access on R3. Use the same parameters as in Step 2h.

Step 5: (Optional) Configure basic settings on S1 and S3.

- a. Configure the hostnames as shown in the topology.

-
- b. Configure the management interface IP addresses as shown in the Topology and Addressing Table.
 - c. Disable DNS lookup.
 - d. Configure a privileged EXEC mode password of **class**.
 - e. Configure a default gateway address.

Step 6: Configure OSPF routing on R1, ISP, and R3.

- a. Assign 1 as the OSPF process ID and advertise all networks on R1, ISP, and R3. The OSPF configuration for R1 is included for reference.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.20.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

- b. After configuring OSPF on R1, ISP, and R3, verify that all routers have complete routing tables listing all networks. Troubleshoot if this is not the case.

Step 7: Verify connectivity between devices.

Note: It is very important to verify connectivity **before** you configure and apply ACLs! Ensure that your network is properly functioning before you start to filter out traffic.

- a. From PC-A, ping PC-C and the loopback and serial interfaces on R3.
Were your pings successful? _____
- b. From R1, ping PC-C and the loopback and serial interface on R3.
Were your pings successful? _____
- c. From PC-C, ping PC-A and the loopback and serial interface on R1.
Were your pings successful? _____
- d. From R3, ping PC-A and the loopback and serial interface on R1.
Were your pings successful? _____
- e. From PC-A, ping the loopback interfaces on the ISP router.
Were your pings successful? _____
- f. From PC-C, ping the loopback interfaces on the ISP router.
Were your pings successful? _____
- g. Open a web browser on PC-A and go to <http://209.165.200.225> on ISP. You will be prompted for a username and password. Use **admin** for the username and **class** for the password. If you are prompted to accept a signature, accept it. The router will load the Cisco Configuration Professional (CCP) Express in a separate window. You may be prompted for a username and password. Use **admin** for the username and **class** for the password.
- h. Open a web browser on PC-C and go to <http://10.1.1.1> on R1. You will be prompted for a username and password. Use **admin** for username and **class** for the password. If you are prompted to accept a

signature, accept it. The router will load CCP Express in a separate window. You may be prompted for a username and password. Use **admin** for the username and **class** for the password.

Part 3: Configure and Verify Extended Numbered and Named ACLs

Extended ACLs can filter traffic in many different ways. Extended ACLs can filter on source IP addresses, source ports, destination IP addresses, destination ports, as well as various protocols and services.

Security policies are as follows:

1. Allow web traffic originating from the 192.168.10.0/24 network to go to any network.
2. Allow an SSH connection to the R3 serial interface from PC-A.
3. Allow users on 192.168.10.0/24 network access to 192.168.20.0/24 network.
4. Allow web traffic originating from the 192.168.30.0/24 network to access R1 via the web interface and the 209.165.200.224/27 network on ISP. The 192.168.30.0/24 network should NOT be allowed to access any other network via the web.

In looking at the security policies listed above, you will need at least two ACLs to fulfill the security policies. A best practice is to place extended ACLs as close to the source as possible. We will follow this practice for these policies.

Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.

You will use a numbered extended ACL on R1. What are the ranges for extended ACLs?

-
- a. Configure the ACL on R1. Use 100 for the ACL number.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

What does the 80 signify in the command output listed above?

To what interface should ACL 100 be applied?

In what direction should ACL 100 be applied?

-
- b. Apply ACL 100 to the S0/0/0 interface.

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 out
```

- c. Verify ACL 100.

-
- 1) Open up a web browser on PC-A, and access <http://209.165.200.225> (the ISP router). It should be successful; troubleshoot, if not.
 - 2) Establish an SSH connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in with **admin** and **class** for your credentials. It should be successful; troubleshoot, if not.
 - 3) From privileged EXEC mode prompt on R1, issue the **show access-lists** command.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)

20 permit tcp any any eq www (111 matches)

- 4) From the PC-A command prompt, issue a ping to 10.2.2.1. Explain your results.

Step 2: Configure a named extended ACL on R3 for security policy number 3.

- a. Configure the policy on R3. Name the ACL WEB-POLICY.

R3(config)# **ip access-list extended WEB-POLICY**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80**

R3(config-ext-nacl)# **permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80**

- b. Apply ACL WEB-POLICY to the S0/0/1 interface.

R3(config-ext-nacl)# **interface S0/0/1**

R3(config-if)# **ip access-group WEB-POLICY out**

- c. Verify the ACL WEB-POLICY.

- 1) From R3 privileged EXEC mode command prompt, issue the **show ip interface s0/0/1** command.

What, if any, is the name of the ACL? _____

In what direction is the ACL applied? _____

- 2) Open up a web browser on PC-C and access <http://209.165.200.225> (the ISP router). It should be successful; troubleshoot, if not.
- 3) From PC-C, open a web session to <http://10.1.1.1> (R1). It should be successful; troubleshoot, if not.
- 4) From PC-C, open a web session to <http://209.165.201.1> (ISP router). It should fail; troubleshoot, if not.
- 5) From a PC-C command prompt, ping PC-A. What was your result and why?

Part 4: Modify and Verify Extended ACLs

Because of the ACLs applied on R1 and R3, no pings or any other kind of traffic is allowed between the LAN networks on R1 and R3. Management has decided that all traffic between the 192.168.10.0/24 and 192.168.30.0/24 networks should be allowed. You must modify both ACLs on R1 and R3.

Step 1: Modify ACL 100 on R1.

- a. From R1 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list? _____

- b. Enter global configuration mode and modify the ACL on R1.

```
R1(config)# ip access-list extended 100
```

```
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0  
0.0.0.255
```

```
R1(config-ext-nacl)# end
```

- c. Issue the **show access-lists** command.

Where did the new line that you just added appear in ACL 100?

Step 2: Modify ACL WEB-POLICY on R3.

- a. From R3 privileged EXEC mode, issue the **show access-lists** command.

How many lines are there in this access list? _____

- b. Enter global configuration mode and modify the ACL on R3.

```
R3(config)# ip access-list extended WEB-POLICY
```

```
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0  
0.0.0.255
```

```
R3(config-ext-nacl)# end
```

- c. Issue the **show access-lists** command to verify that the new line was added at the end of the ACL.

Step 3: Verify modified ACLs.

- a. From PC-A, ping the IP address of PC-C. Were the pings successful? _____

- b. From PC-C, ping the IP address of PC-A. Were the pings successful? _____

Why did the ACLs work immediately for the pings after you changed them?

Reflection

1. Why is careful planning and testing of ACLs required?
- _____

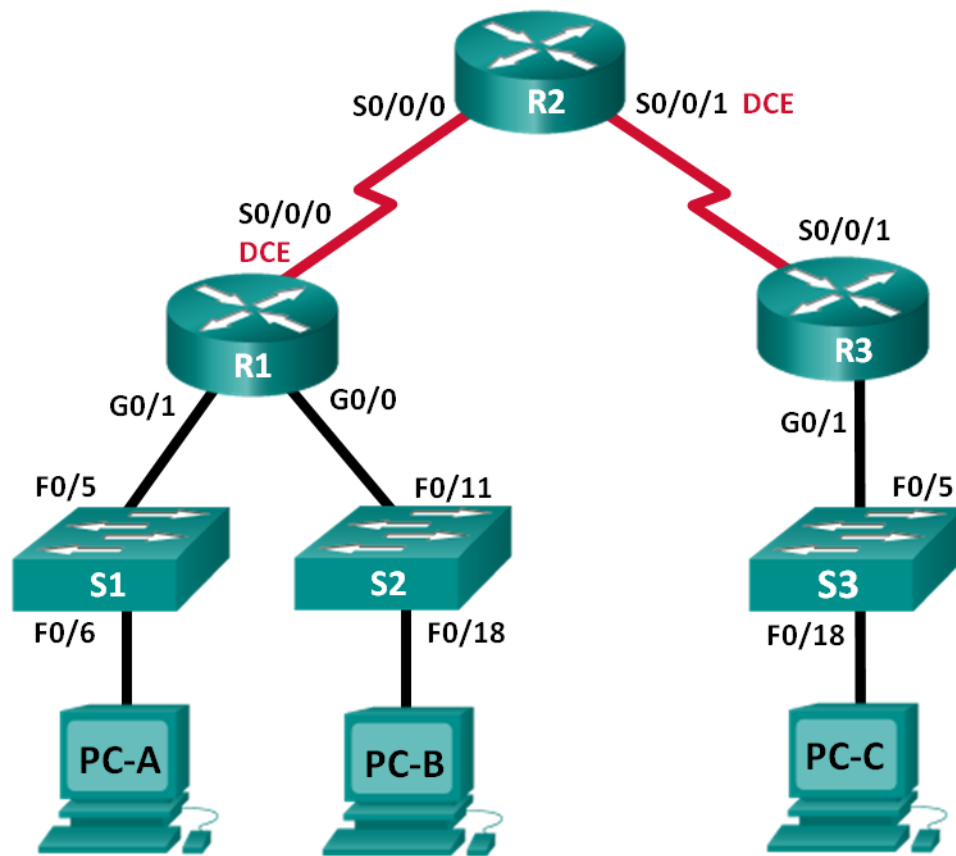
2. Which type of ACL is better: standard or extended?

3. Why are OSPF hello packets and routing updates not blocked by the implicit **deny any** access control entry (ACE) or ACL statement of the ACLs applied to R1 and R3?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 9 – Configuring and Verifying IPv6 ACLs

Topology

Addressing Table

Device	Interface	IP Address	Default Gateway
R1	G0/0	2001:DB8:ACAD:B::1/64	N/A
	G0/1	2001:DB8:ACAD:A::1/64	N/A
	S0/0/0 (DCE)	2001:DB8:AAAA:1::1/64	N/A
R2	S0/0/0	2001:DB8:AAAA:1::2/64	N/A
	S0/0/1 (DCE)	2001:DB8:AAAA:2::2/64	N/A
R3	G0/1	2001:DB8:CAFE:C::1/64	N/A
	S0/0/1	2001:DB8:AAAA:2::1/64	N/A
S1	VLAN1	2001:DB8:ACAD:A::A/64	N/A
S2	VLAN1	2001:DB8:ACAD:B::A/64	N/A
S3	VLAN1	2001:DB8:CAFE:C::A/64	N/A
PC-A	NIC	2001:DB8:ACAD:A::3/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::3/64	FE80::1
PC-C	NIC	2001:DB8:CAFE:C::3/64	FE80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Configure and Verify IPv6 ACLs

Part 4: Edit IPv6 ACLs

Background / Scenario

You can filter IPv6 traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create IPv4 named ACLs. IPv6 ACL types are extended and named. Standard and numbered ACLs are no longer used with IPv6. To apply an IPv6 ACL to a vty interface, you use the new **ipv6 access-class** command. The **ipv6 traffic-filter** command is still used to apply an IPv6 ACL to interfaces.

In this lab, you will apply IPv6 filtering rules and then verify that they are restricting access as expected. You will also edit an IPv6 ACL and clear the match counters.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary

from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you set up the network topology and clear any configurations if necessary.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you configure basic settings on the routers, switches and PCs. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure IPv6 addresses on all PCs.

Configure IPv6 global unicast addresses according to the Addressing Table. Use the link-local address of **FE80::1** for the default-gateway on all PCs.

Step 2: Configure the switches.

- Disable DNS lookup.
- Assign the hostname.
- Assign a domain-name of **ccna-lab.com**.
- Encrypt plain text passwords.
- Create a MOTD banner warning users that unauthorized access is prohibited.
- Create a local user database with a username of **admin** and password as **classadm**.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Enable login on the VTY lines using the local database.

-
- j. Generate a crypto rsa key for ssh using a modulus size of 1024 bits.
 - k. Change the transport input VTY lines to all for SSH and Telnet only.
 - l. Assign an IPv6 address to VLAN 1 according to the Addressing Table.
 - m. Administratively disable all inactive interfaces.

Step 3: Configure basic settings on all routers.

- a. Disable DNS lookup.
- b. Assign the hostname.
- c. Assign a domain-name of **ccna-lab.com**.
- d. Encrypt plain text passwords.
- e. Create a MOTD banner warning users that unauthorized access is prohibited.
- f. Create a local user database with a username of **admin** and password as **classadm**.
- g. Assign **class** as the privileged EXEC encrypted password.
- h. Assign **cisco** as the console password and enable login.
- i. Enable login on the VTY lines using the local database.
- j. Generate a crypto rsa key for ssh using a modulus size of 1024 bits.
- k. Change the transport input VTY lines to all for SSH and Telnet only.

Step 4: Configure IPv6 settings on R1.

- a. Configure the IPv6 unicast address on interface G0/0, G0/1, and S0/0/0.
- b. Configure the IPv6 link-local address on interface G0/0, G0/1, and S0/0/0. Use **FE80::1** for the link-local address on all three interfaces.
- c. Set the clock rate on S0/0/0 to 128000.
- d. Enable the interfaces.
- e. Enable IPv6 unicast routing.
- f. Configure an IPv6 default route to use interface S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

Step 5: Configure IPv6 settings on R2.

- a. Configure the IPv6 unicast address on interface S0/0/0 and S0/0/1.
- b. Configure the IPv6 link-local address on interface S0/0/0 and S0/0/1. Use **FE80::2** for the link-local address on both interfaces.
- c. Set the clock rate on S0/0/1 to 128000.
- d. Enable the interfaces.
- e. Enable IPv6 unicast routing.

-
- f. Configure static IPv6 routes for traffic handling of R1 and R3 LAN subnets.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
```

```
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

Step 6: Configure IPv6 settings on R3.

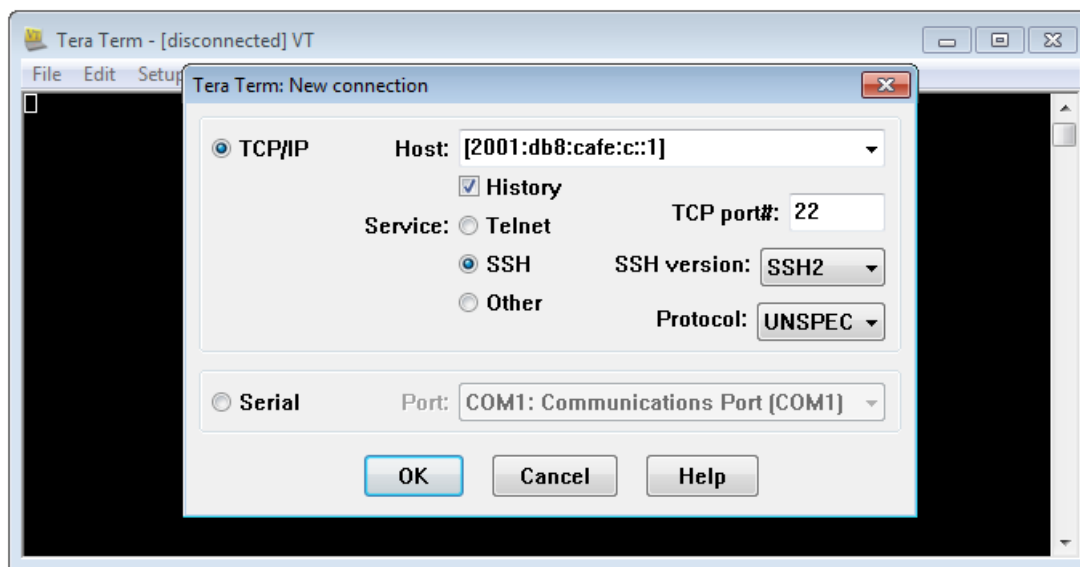
- Configure the IPv6 unicast address on interface G0/1 and S0/0/1.
- Configure the IPv6 link-local address on interface G0/1 and S0/0/1. Use **FE80::1** for the link-local address on both interfaces.
- Enable the interfaces.
- Enable IPv6 unicast routing.
- Configure an IPv6 default route to use interface S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

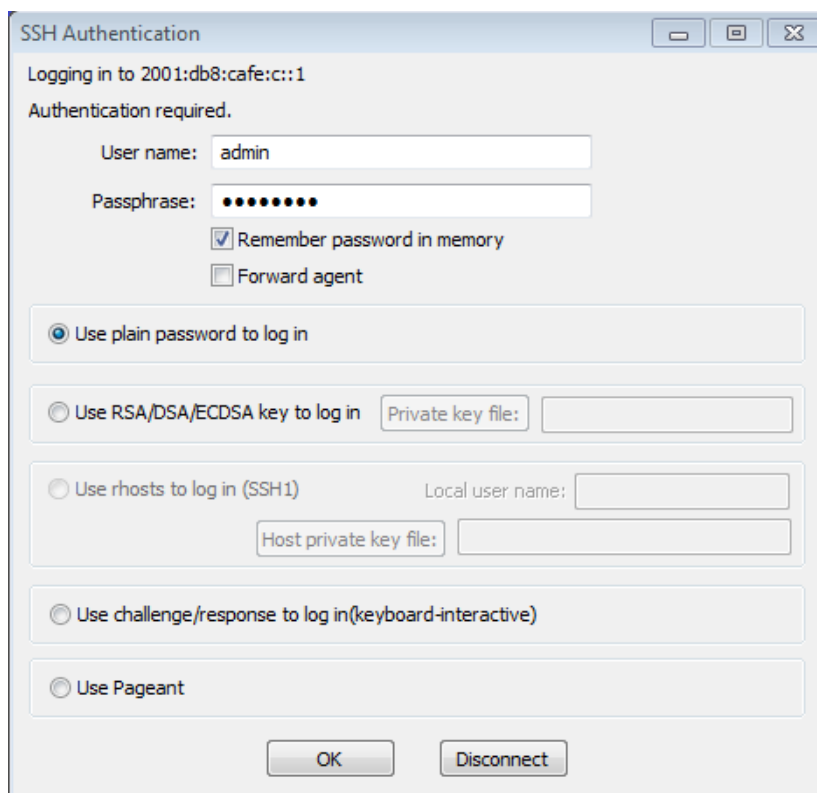
Step 7: Verify connectivity.

- Each PC should be able to ping the other PCs in the topology.
- Telnet to R1 from all PCs in the Topology.
- SSH to R1 from all PCs in the Topology.
- Telnet to S1 from all PCs in the Topology.
- SSH to S1 from all PCs in the Topology.
- Troubleshoot connectivity issues now because the ACLs that you create in Part 3 of this lab will restrict access to some areas of the network.

Note: Tera Term requires the target IPv6 address to be enclosed in brackets. Enter the IPv6 address as shown, click **OK** and then click **Continue** to accept the security warning and connect to the router.



Input the user credentials configured (username **admin** and password **classadm**) and select the **Use plain password to log in** in the SSH Authentication dialogue box. Click **OK** to continue.



Part 3: Configure and Verify IPv6 ACLs

Step 1: Configure and verify VTY restrictions on R1.

- Create an ACL to only allow hosts from the 2001:db8:acad:a::/64 network to telnet to R1. All hosts should only be able to ssh to R1.

```
R1(config)# ipv6 access-list RESTRICT-VTY
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any eq 23
R1(config-ipv6-acl)# permit tcp any any eq 22
```

- Apply the RESTRICT-VTY ACL to R1's VTY lines.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

- Show the new ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
    permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
    permit tcp any any eq 22 sequence 20
```

- d. Verify that the RESTRICT-VTY ACL is only allowing Telnet traffic from the 2001:db8:acad:a::/64 network. How does the RESTRICT-VTY ACL only allow hosts from the 2001:db8:acad:a::/64 network to telnet to R1?

What does the second permit statement in the RESTRICT-VTY ACL do?

Step 2: Restrict Telnet access to the 2001:db8:acad:a::/64 network.

- a. Create an ACL called RESTRICTED-LAN that will block Telnet access to the 2001:db8:acad:a::/64 network.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

- b. Apply the RESTRICTED-LAN ACL to interface G0/1 for all outbound traffic.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

- c. Telnet to S1 from PC-B and PC-C to verify that Telnet has been restricted. SSH to S1 from PC-B to verify that it can still be reached using SSH. Troubleshoot if necessary.
- d. Use the **show ipv6 access-list** command to view the RESTRICTED-LAN ACL.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
    deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches) sequence 20
    permit ipv6 any any (45 matches) sequence 30
```

Notice that each statement identifies the number of hits or matches that have occurred since the ACL was applied to the interface.

- e. Use the **clear ipv6 access-list** to reset the match counters for the RESTRICTED-LAN ACL.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

- f. Redisplay the ACL with the **show access-lists** command to confirm that the counters were cleared.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any sequence 30
```

Part 4: Edit IPv6 ACLs

In Part 4, you will edit the RESTRICTED-LAN ACL that you created in Part 3. It is always a good idea to remove the ACL from the interface to which it is applied before editing it. After you complete your edits, then reapply the ACL to the interface.

Note: Many network administrators will make a copy of the ACL and edit the copy. When editing is complete, the administrator will remove the old ACL and apply the newly edited ACL to the interface. This method keeps the ACL in place until you are ready to apply the edited copy of the ACL.

Step 1: Remove the ACL from the interface.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Step 2: Use the show access-lists command to view the ACL.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
  permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
  permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (36 matches) sequence 30
```

Step 3: Insert a new ACL statement using sequence numbering.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host 2001:db8:acad:a::a
eq 23 sequence 15
```

What does this new permit statement do?

Step 4: Insert a new ACL statement at the end of the ACL.

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3 eq www
```

Note: This permit statement is only used to show how to add a statement to the end of an ACL. This ACL line would never be matched because the previous permit statement is matching on everything.

Step 5: Use the do show access-lists command to view the ACL change.

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
  permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
  permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (124 matches) sequence 30
  permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

Note: The **do** command can be used to execute any privileged EXEC command while in global configuration mode or a submode.

Step 6: Delete an ACL statement.

Use the **no** command to delete the permit statement that you just added.

```
R1(config-ipv6-acl)# no permit tcp any host 2001:DB8:ACAD:A::3 eq www
```

Step 7: Use the do show access-list RESTRICTED-LAN command to view the ACL.

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
  permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq telnet sequence 15
  deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
  permit ipv6 any any (214 matches) sequence 30
```

Step 8: Re-apply the RESTRICTED-LAN ACL to the interface G0/1.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

Step 9: Test ACL changes.

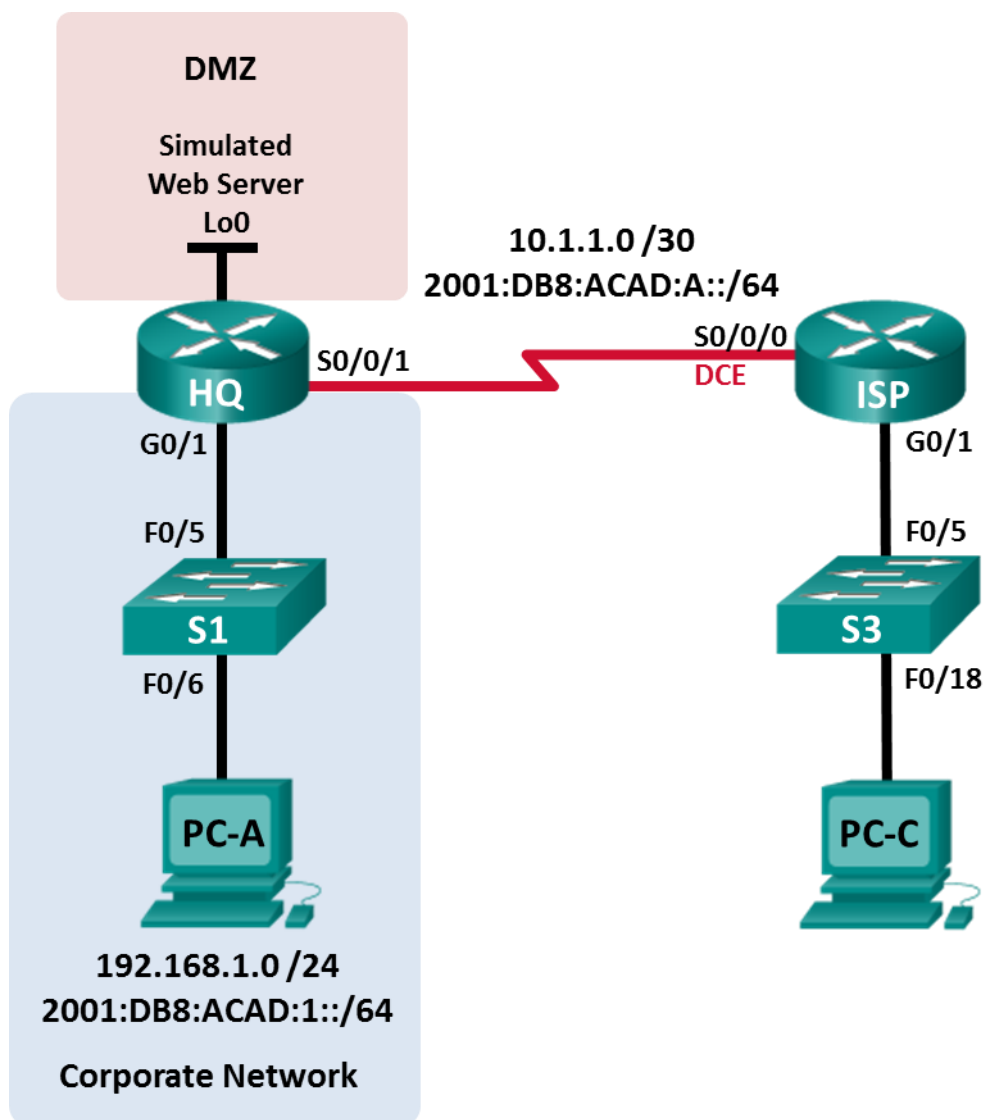
Telnet to S1 from PC-B. Troubleshoot if necessary.

Reflection

1. What is causing the match count on the RESTRICTED-LAN **permit ipv6 any any** statement to continue to increase?

-
2. What command would you use to reset the counters for the ACL on the VTY lines?
-

Lab 11 - Troubleshooting ACL Configuration and Placement

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
		IPv6 Address / Prefix		
		Link Local Address		
HQ	G0/1	192.168.1.1	255.255.255.0	N/A
		2001:DB8:ACAD:1::1/64		
		FE80::1		
	S0/0/1	10.1.1.2	255.255.255.252	N/A
		2001:DB8:ACAD:A::2/64		
		FE80::2		
	Lo0	192.168.4.1	255.255.255.0	N/A
		2001:DB8:ACAD:4::1/64		
		FE80::1		
ISP	G0/1	192.168.3.1	255.255.255.0	N/A
		2001:DB8:ACAD:3::1/64		
		FE80::1		
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
		2001:DB8:ACAD:A::1/64		
		FE80::1		
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
		2001:DB8:ACAD:1::3/64		FE80::1
		FE80::3		
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1
		2001:DB8:ACAD:3::3/64		FE80::1
		FE80::3		

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Internal Access

Part 3: Troubleshoot Remote Access

Background / Scenario

An access control list (ACL) is a series of IOS commands that provide basic traffic filtering on a Cisco router. ACLs are used to select the types of traffic to be processed.

A single ACL statement is called an access control entry (ACE). The ACEs in the ACL are evaluated from top to bottom with an implicit deny all ACE at the end of the list. ACLs can also control the types of traffic into or out of a network by the source and destination hosts or network. To process the desired traffic correctly, the placement of the ACLs is critical.

In this lab, a small company has just added a web server to the network to allow customers to access confidential information. The company IPv4 and IPv6 network is divided into two zones: Corporate network zone and Demilitarized Zone (DMZ). The corporate network zone houses private servers and internal clients. The DMZ houses the externally accessible web server (simulated by Lo0 on HQ).

To secure access to the corporate and DMZ networks, several ACLs were configured on the HQ router. However, there are problems with the configured ACLs. In this lab, you will examine what the ACLs are doing and take corrective actions to implement them properly.

When troubleshooting ACLs, it is important that its purpose and desired outcome is well understood. For this reason, the following describes the ACLs configured on HQ:

- **ACL 101** is implemented to limit the traffic leaving the corporate network zone. This zone is often referred to as the private or internal network because it houses the private servers and internal clients. In this topology, this zone is assigned network address 192.168.1.0/24. Therefore, only traffic from that network should be permitted to leave the internal network.
- **ACL 102** is used to limit the traffic into the corporate network. Only responses to requests that originated from within the corporate network are allowed back into that network. This includes TCP-based requests from internal hosts such as Web and FTP. ICMP is allowed into the network for troubleshooting purposes so that incoming ICMP messages generated in response to pings can be received by internal hosts. No other network should be able to access the corporate zone.
- **ACL 121** controls outside traffic to the DMZ and corporate network. Only HTTP traffic is allowed to the DMZ web server (simulated by Lo0 on HQ). Other network related traffic, such as EIGRP, is allowed from outside networks. Furthermore, valid internal private addresses, such as 192.168.1.0, loopback address such as 127.0.0.1 and multicast addresses are denied entrance to the corporate network to prevent malicious network attacks from outside users.
- **IPv6 ACL** named NO-ICMP denies ICMP traffic to the DMZ and corporate network originated from the outside. ICMP response is allowed into the network that is responding to the requests from the internet hosts. Other network related traffic, such as EIGRP, is allowed from outside networks. Furthermore, the outside network is allowed to access the DMZ web server (simulated by Lo0 on HQ).

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings such as passwords and IP addresses. Preset configurations are also provided for you for the initial router configurations. You will also configure the IP settings for the PCs in the topology.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts according to the Addressing Table

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: (Optional) Configure basic settings for each switch.

- Disable DNS lookup.
- Configure host names as shown in the Topology.
- Configure IP addresses and default gateways as shown in the Addressing Table.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the privileged EXEC password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Configure basic settings for each router.

- Disable DNS lookup.
- Configure host names as shown in the topology.

-
- c. Assign **class** as the privileged EXEC password.
 - d. Assign **cisco** as the console and vty passwords.
 - e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 6: Configure HTTP access and user credentials on HQ router.

Local user credentials are configured to access the simulated web server (192.168.4.1).

```
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Step 7: Load router configurations.

The configurations for the routers ISP and HQ are provided for you. There are errors within these configurations, and it is your task to correct them.

Router ISP

```
hostname ISP
ipv6 unicast-routing
ipv6 router eigrp 1
  eigrp router-id 10.1.1.1
  no shutdown
interface GigabitEthernet0/1
  ip address 192.168.3.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:3::1/64
  ipv6 eigrp 1
  no shutdown
interface Serial0/0/0
  ip address 10.1.1.1 255.255.255.252
  clock rate 128000
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:A::1/64
  ipv6 eigrp 1
  no shutdown
router eigrp 1
  network 10.1.1.0 0.0.0.3
  network 192.168.3.0
  no auto-summary
end
```

Router HQ

```
hostname HQ
ipv6 unicast-routing
```

```
ipv6 router eigrp 1
  eigrp router-id 10.1.1.2
  no shutdown
interface Loopback0
  ip address 192.168.4.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:4::1/64
  ipv6 eigrp 1
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:1::1/64
  ip access-group 101 out
ip access-group 102 in
ipv6 eigrp 1
  no shutdown
interface Serial0/0/1
  ip address 10.1.1.2 255.255.255.252
  ip access-group 121 in
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD:A::2/64
  ipv6 eigrp 1
ipv6 traffic-filter NO-ICMP out
  no shutdown
router eigrp 1
  network 10.1.1.0 0.0.0.3
  network 192.168.1.0
  network 192.168.4.0
  no auto-summary
ip http server
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
access-list 121 deny icmp any host 192.168.4.11
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny ip 127.0.0.0 0.255.255.255 any
access-list 121 deny ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
```

```
ipv6 access-list NO-ICMP
deny icmp any any echo-request
permit ipv6 any any
end
```

Part 2: Troubleshoot Internal Access

In Part 2, the ACLs on router HQ are examined to determine if they are configured correctly.

Step 1: Troubleshoot ACL 101

ACL 101 is implemented to limit the traffic leaving the corporate network zone. This zone houses only internal clients and private servers. Only 192.168.1.0/24 network can exit this corporate network zone.

- Can PC-A ping its default gateway? _____
- After verifying that PC-A was configured correctly, examine the HQ router to find possible configuration errors by viewing the summary of ACL 101. Enter the command **show access-lists 101**.

```
HQ# show access-lists 101
Extended IP access list 101
 10 permit ip 192.168.11.0 0.0.0.255 any
 20 deny ip any any
```

- Are there any problems with ACL 101?

- Correct ACL 101. Record the commands used to correct the errors.

- Can PC-A ping its default gateway? _____
- PC-A still cannot ping its default gateway, therefore verify that ACL 101 is applied in the correct direction on the G0/1 interface. Enter the **show ip interface g0/1** command.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.1.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is 101
 Inbound access list is 102
```

Is the direction for interface G0/1 configured correctly for ACL 101?

- g. Correct the direction of ACL 101 on the G0/1 interface. Record the commands used to correct the errors.

- h. Verify the traffic from network 192.168.1.0 /24 can exit the corporate network. PC-A should now be able to ping its default gateway interface.

Step 2: Troubleshoot ACL 102

ACL 102 is implemented to limit traffic going into the corporate network. Traffic originating from the outside network is not allowed onto the corporate network. Remote traffic is allowed into the corporate network if the established traffic originated from the internal network. ICMP reply messages are allowed for troubleshooting purposes.

- a. Can PC-A ping PC-C? _____
- b. Examine the HQ router to find possible configuration errors by viewing the summary of ACL 102. Enter the command **show access-lists 102**.

```
HQ# show access-lists 102
Extended IP access list 102
 10 permit tcp any any established
 20 permit icmp any any echo-reply
 30 permit icmp any any unreachable
 40 deny ip any any (57 matches)
```

- c. Are there any problems with ACL 102? _____
- d. Verify that the ACL 102 is applied in the correct direction on G0/1 interface. Enter the **show ip interface g0/1** command.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.1.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is 101
 Inbound access list is 101
```

-
- e. Are there any problems with the application of ACL 102 to interface G0/1?
- _____
- f. Correct any errors found regarding ACL 102. Record the commands used to correct the errors.
- _____
- _____
- g. Can PC-A ping PC-C now? _____

Part 3: Troubleshoot Remote Access

In Part 3, ACL 121 is configured to prevent spoofing attacks from the outside networks and allow only remote HTTP access to the web server (192.168.4.1) in the DMZ.

- a. Verify ACL 121 has been configured correctly. Enter the **show ip access-list 121** command.

```
HQ# show ip access-lists 121
Extended IP access list 121
 10 permit tcp any host 192.168.4.1 eq 89
 20 deny icmp any host 192.168.4.11
 30 deny ip 192.168.1.0 0.0.0.255 any
 40 deny ip 127.0.0.0 0.255.255.255 any
 50 deny ip 224.0.0.0 31.255.255.255 any
 60 permit ip any any (354 matches)
 70 deny ip any any
```

Are there any problems with this ACL?

- b. Make and record the necessary configuration changes to ACL 121.

- c. Verify that the ACL 121 is applied in the correct direction on the HQ S0/0/1 interface. Enter the **show ip interface s0/0/1** command.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
 Internet address is 10.1.1.2/30
 Broadcast address is 255.255.255.255
```

```
<output omitted>
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is not set
Inbound access list is 121
```

Are there any problems with the application of this ACL?

- d. Verify that PC-C can only access the simulated web server on HQ by using the web browser. Provide the username **admin** and password **adminpass** to access the web server (192.168.4.1).

Part 4: Troubleshoot IPv6 ACL

In Part 4, an IPv6 ACL named NO-ICMP denies ICMP traffic to the DMZ and corporate network originating from the outside. ICMP response to the internal hosts, EIGRP packets, and network related traffic are allowed from outside networks. Furthermore, the outside network is allowed to access the DMZ web server (simulated by Lo0 on HQ).

- a. Verify ACL **NO-ICMP** has been configured correctly. Enter the **show ipv6 access-list NO-ICMP** command.

```
HQ# show ipv6 access-list NO-ICMP
IPv6 access list NO-ICMP
    deny icmp any any echo-request sequence 10
    permit ipv6 any any sequence 20
```

Are there any problems with this ACL?

- b. Verify that the ACL NO-ICMP is applied in the correct direction on the HQ S0/0/1 interface. Enter the **show ipv6 interface s0/0/1** command.

```
HQ# show ipv6 interface s0/0/1
Serial0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::2
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::A
    FF02::1:FF00:1
    FF02::1:FF00:2
  MTU is 1500 bytes
```

```
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
Output features: Access List
Outgoing access list NO-ICMP
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND RAs are suppressed (periodic)
Hosts use stateless autoconfig for addresses.
```

Are there any problems with the application of this ACL?

- c. Make and record the necessary configuration changes to ACL NO-ICMP.

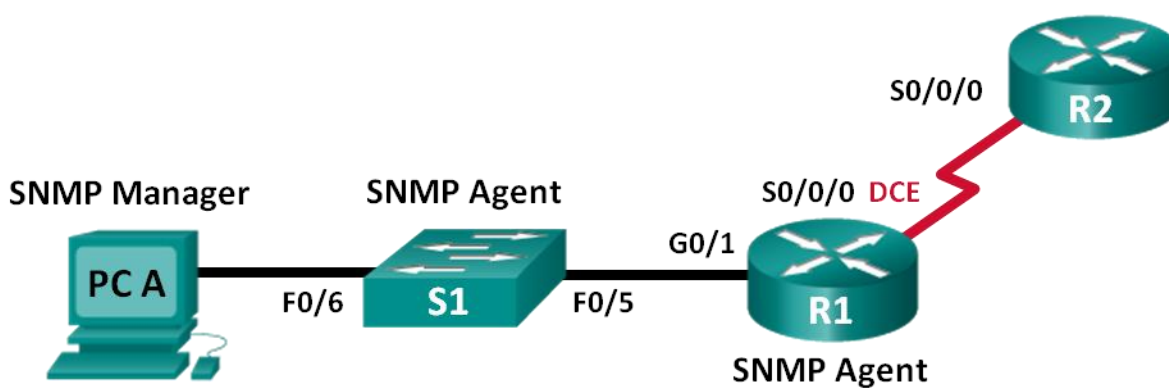
Reflection

1. How should the ACL statement be ordered? From general to specific or vice versa?

2. If you delete an ACL by using the **no access-list** command and the ACL is still applied to the interface, what happens?

Lab 12 – Configuring SNMP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure an SNMPv2 Manager and Agent

Part 3: Configure an SNMPv3 Manager and Agent

Background / Scenario

Simple Network Management Protocol (SNMP) is a network management protocol and an IETF standard which can be used to both monitor and control clients on the network. SNMP can be used to get and set variables related to the status and configuration of network hosts like routers and switches, as well as network client computers. The SNMP manager can poll SNMP agents for data, or data can be automatically sent to the SNMP manager by configuring traps on the SNMP agents.

In this lab, you will download, install, and configure SNMP management software on PC-A. You will also configure a Cisco router and Cisco switch as SNMP agents. After capturing SNMP notification messages from the SNMP agent, you will convert the MIB/Object ID codes to learn the details of the messages using the Cisco SNMP Object Navigator.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Note: The **snmp-server** commands in this lab will cause the Cisco 2960 switch to issue a warning message when saving the configuration file to NVRAM. To avoid this warning message verify that the switch is using the **lanbase-routing** template. The IOS template is controlled by the Switch Database Manager (SDM). When changing the preferred template, the new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **lanbase-routing** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end
S1# reload
```

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS, Release 15.4(3) universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows with terminal emulation program, such as Tera Term, SNMP manager, such as SNMP MIB Browser by ManageEngine, and Wireshark)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology
- SNMP Management Software (SNMP MIB Browser by ManageEngine)

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the devices with basic settings.

Step 1: Cable the network as shown in the topology.

Step 2: Configure the PC host.

Step 3: Initialize and reload the switch and routers as necessary.

Step 4: Configure basic settings for the routers and switch.

- a. Disable DNS lookup.
- b. Configure device names as shown in the topology.
- c. Configure IP addresses as shown in the Addressing Table. (Do not configure or enable the VLAN 1 interface on S1 at this time.)
- d. Assign **cisco** as the console and vty password and enable login.
- e. Assign **class** as the encrypted privileged EXEC mode password.
- f. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- g. Verify successful connectivity between PC-A and R1 and between the routers by issuing the **ping** command.
- h. Copy the running configuration to the startup configuration.

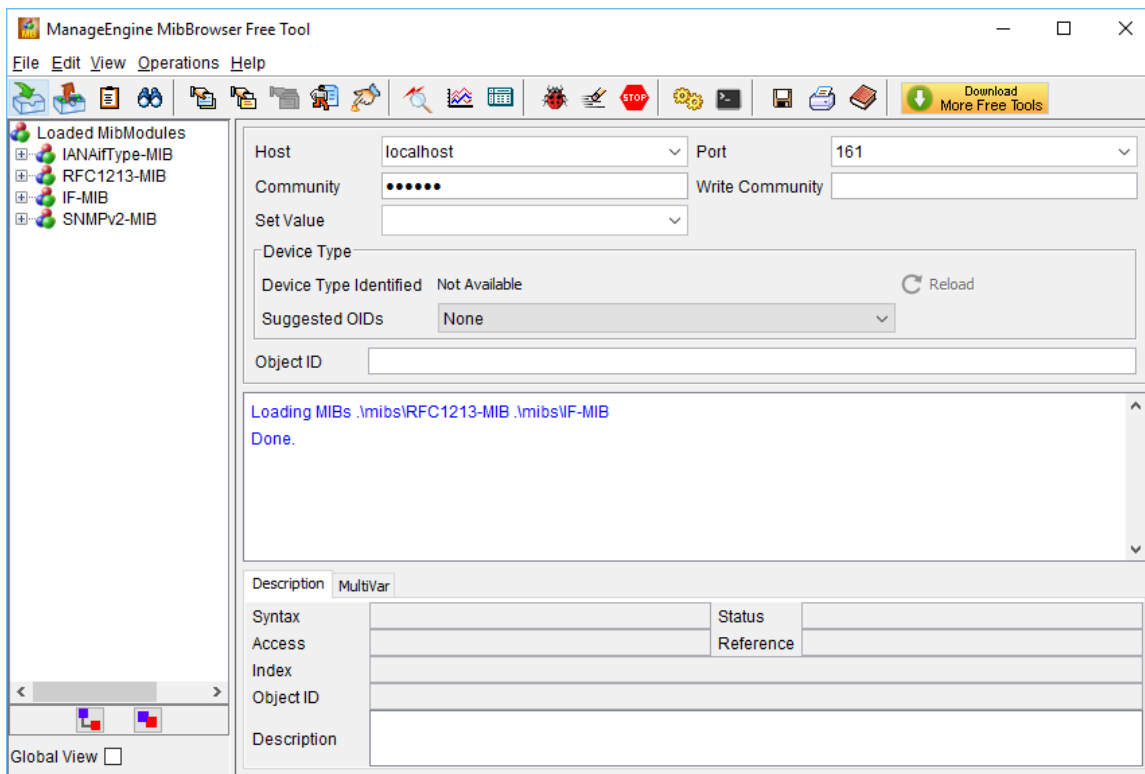
Part 2: Configure SNMPv2 Manager and Agent

In Part 2, SNMP management software will be installed and configured on PC-A, and R1 and S1 will be configured as SNMP agents.

Step 1: Install an SNMP management program.

- a. Download and install the SNMP MIB Browser by ManageEngine from the following URL: <https://www.manageengine.com/products/mibbrowser-free-tool/download.html>. You will be asked to provide an email address to download the software.
- b. Launch the ManageEngine MibBrowser program.
 - 1) If you receive an error message regarding the failure to load MIBs. Navigate to the MibBrowser Free Tool folder:
32bit: C:\Program Files (x86)\ManageEngine\MibBrowser Free Tool
64bit: C:\Program Files\ManageEngine\MibBrowser Free Tool
 - 2) Right-click the **mibs** folder and select the **Security** tab. Click **Edit**. Select **Users**. Click **Full control**. Click **OK** to change the permission.
 - 3) Repeat the previous step with the **conf** folder.

4) Launch the ManageEngine MibBrowser program again.



Step 2: Configure a SNMPv2 agent.

On S1, enter the following commands from the global configuration mode to configure the switch as an SNMP agent. In line 1 below, the SNMP community string is **ciscolab**, with read-only privileges, and the named access list **SNMP_ACL** defines which hosts are allowed to get SNMP information from S1. In lines 2 and 3, the SNMP manager location and contact commands provide descriptive contact information. Line 4 specifies the IP address of the host that will receive SNMP notifications, the SNMP version, and the community string. Line 5 enables all default SNMP traps, and lines 6 and 7 create the named access list, to control which hosts are permitted to get SNMP information from the switch.

```
S1(config)# snmp-server community ciscolab ro SNMP_ACL
S1(config)# snmp-server location Company_HQ
S1(config)# snmp-server contact admin@company.com
S1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
S1(config)# snmp-server enable traps
S1(config)# ip access-list standard SNMP_ACL
S1(config-std-nacl)# permit 192.168.1.3
```

Step 3: Verify the SNMPv2 settings.

Use the **show** commands to verify the SNMPv2 settings.

```
S1# show snmp
Chassis: FCQ1628Y5MG
Contact: admin@company.com
Location: Company_HQ
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
    Logging to 192.168.1.3.162, 0/10, 0 sent, 0 dropped.
SNMP agent enabled
```

```
S1# show snmp community
```

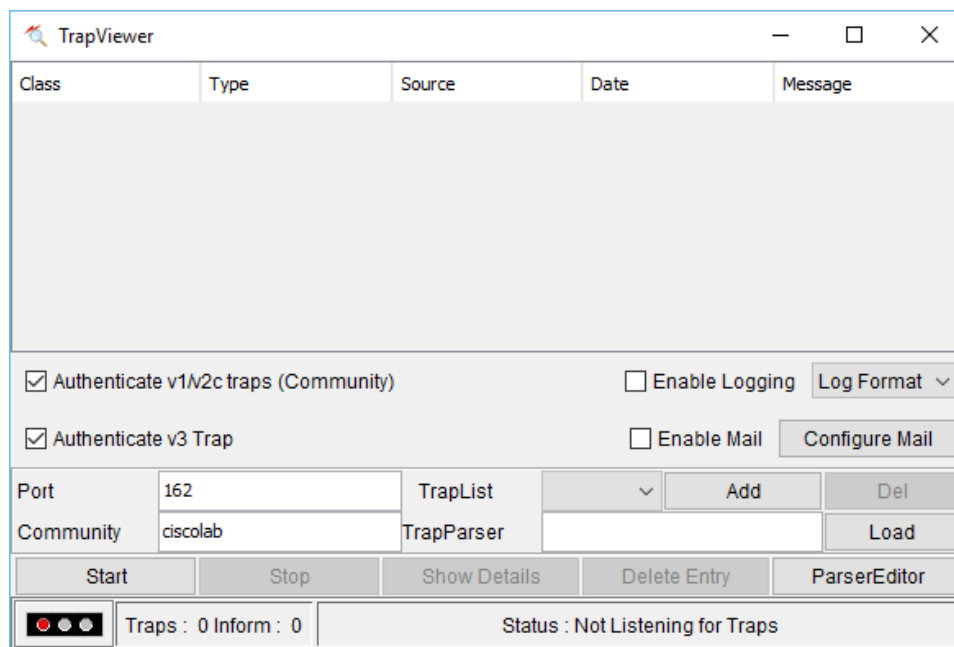
```
Community name: ciscolab
Community Index: ciscolab
Community SecurityName: ciscolab
storage-type: nonvolatile      active access-list: SNMP_ACL
<output omitted>
```

What is the configured SNMP community?

Step 4: Enable SNMP trap.

In this step, you will start the SNMP trap and observe the messages when you configure and enable SVI on VLAN 1 for S1.

- In the MibBrowser, click **Edit > Settings**. Verify that **v2c** is selected as the SNMP Version. Click **OK** to continue.
- Click **Trap Viewer UI** ().
- Verify **162** is the Port number and configure **ciscolab** as the Community.



Class	Type	Source	Date	Message

☒ Authenticate v1/v2c traps (Community)
 ☐ Enable Logging
 Log Format ▼

☒ Authenticate v3 Trap
 ☐ Enable Mail
 Configure Mail

Port: 162
 TrapList: ▼
Add Del

Community: ciscolab
 TrapParser: ▼
Load

Start Stop Show Details Delete Entry ParserEditor

Traps : 0 Inform : 0 Status : Not Listening for Traps

- Click **Start** after you have verified the settings. The TrapList field displays **162:ciscolab**.
- To generate SNMP messages, configure and enable SVI on S1. Use the IP address **192.168.1.2 /24** for VLAN 1 and disable and enable the interface.
- Enter the **show snmp** command to verify the SNMP messages were sent.

```

S1# show snmp
Chassis: FCQ1628Y5MG
Contact: admin@company.com
Location: Company_HQ
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  
```

```

0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 Input queue packet drops (Maximum queue size 1000)
2 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
2 Trap PDUs
SNMP global trap: enabled

```

SNMP logging: enabled

Logging to 192.168.1.3.162, 0/10, 2 sent, 0 dropped.

SNMP agent enabled

SNMP agent enabled

- g. Navigate to the TrapViewer. View the messages that have been trapped by MibBrowser. To see the details of each message, click **Show Details**.

The screenshot shows the TrapViewer application window. It contains a table with the following data:

Class	Type	Source	Date	Message
Clear	v2c Trap	192.168.1.2	Wed Oct 05 14:31:35...	.iso.org.dod.internet...
Clear	v2c Trap	192.168.1.2	Wed Oct 05 14:31:36...	.iso.org.dod.internet...

Below the table, there are several configuration options and buttons:

- ☒ Authenticate v1/v2c traps (Community)
- ☐ Enable Logging
- ☐ Enable Mail
- ☒ Authenticate v3 Trap
- Log Format (dropdown)
- Configure Mail (button)
- Port: 162
- TrapList: 162:ciscolab
- Community: ciscolab
- TrapParser: (empty)
- Buttons: Start, Stop, Show Details, Delete Entry, ParserEditor
- Status: Listening for Traps
- Traps: 2 Inform : 0

Part 3: Configure SNMPv3 Manager and Agent

Step 1: Configure a SNMPv3 agent on R1.

On R1, enter the following commands from the global configuration mode to configure the router as an SNMP agent. In lines 1 – 3 below, a standard ACL named PERMIT-ADMIN permits only the hosts of the network 192.168.1.0 /24 to access the SNMP agent running on R1. Line 4 configures an SNMP view, SNMP-RO, and it includes the iso tree from the MIB. In line 5, an SNMP group is configured with the name ADMIN, is set to SNMPv3 with authentication and encryption required, and only allows access limit to hosts permitted in the PERMIT-ADMIN ACL. Line 5 defines a user named USER1 with the group ADMIN. Authentication is set to use SHA with the password cisco12345 and encryption is set for AES 128 with cisco54321 as the configured password.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
R1(config)# snmp-server user USER1 ADMIN v3 auth sha cisco12345 pri aes 128
cisco54321
R1(config)#
*Aug  5 02:52:50.715: Configuring snmpv3 USM user, persisting
snmpEngineBoots. Please Wait...
```

Step 2: Verify a SNMPv3 configuration on R1.

Use the **show** commands to verify the SNMPv3 settings.

```
R1# show run | include snmp
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included

R1# show snmp user

User name: USER1
Engine ID: 800000090300D48CB5CEA0C0
storage-type: nonvolatile          active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN
```

Step 3: Configure SNMP manager access to the SNMPv3 agent.

- Navigate to PC-A Open **Wireshark**. Start a live capture on the appropriate interface.
- Enter **snmp** in the Filter field.

- c. In the MibBrowser, click **Edit > Settings**. Select **v3** for SNMP Version. Then click **Add**.
- d. Enter the SNMPv3 settings that were configured on R1. Click **OK** to continue.

The image shows a dialog box titled "SnmpParameterPanel" with a close button (X) in the top right corner. It contains a section for "V3 Parameters" with the following fields:

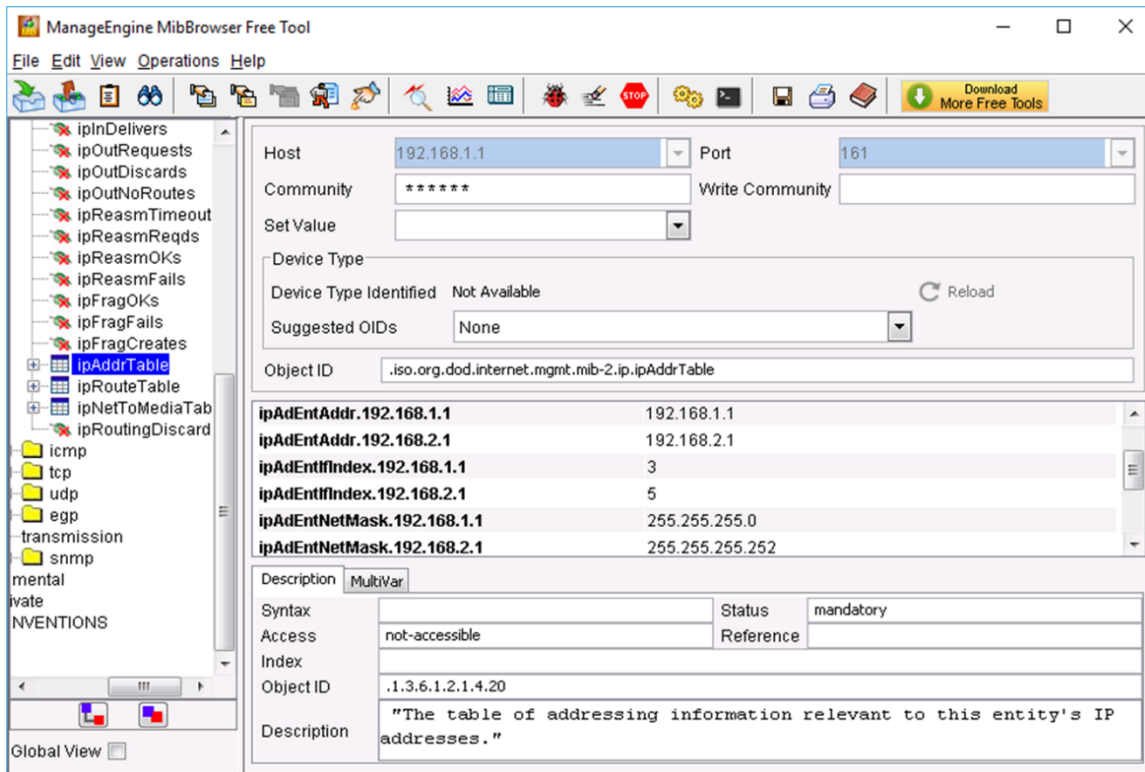
- Target Host: 192.168.1.1
- Target Port: 161
- User Name: USER1
- Security Level: Auth,Priv (dropdown menu)
- Auth Protocol: SHA (dropdown menu)
- Auth Password: cisco12345 (masked with dots)
- Priv Protocol: CFB-AES-128 (dropdown menu)
- Priv Password: cisco54321 (masked with dots)
- Context Name: (empty)
- Engine ID: (empty)

At the bottom of the dialog are three buttons: OK, Cancel, and Apply. The OK button is highlighted with a blue dashed border.

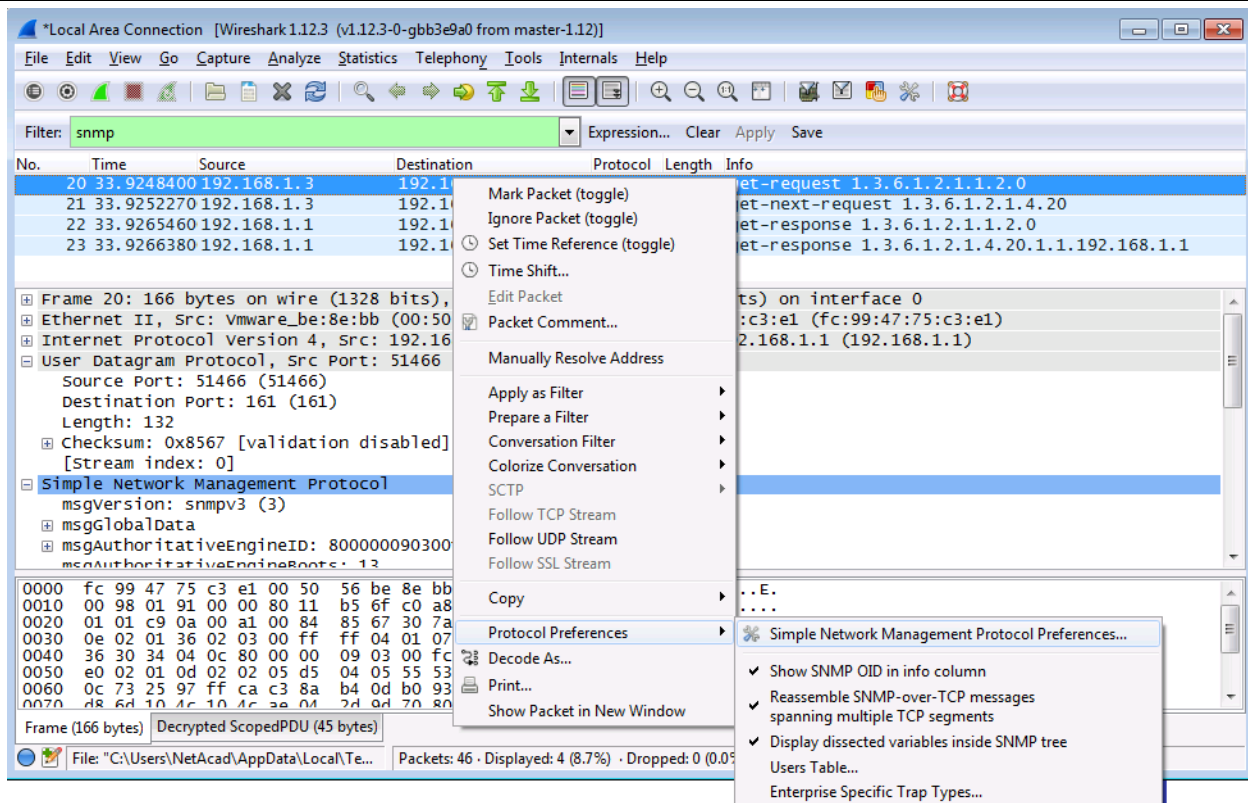
SNMPv3 Parameters	Settings
Target Host	192.168.1.1
User Name	USER1
Auth Protocol	SHA
Priv Protocol	CFB-AES-128
Target Port	161
Security Level	Auth,Priv
Auth Password	cisco12345
Priv Password	cisco54321

- e. Click **Edit > Find Node**. Enter **ipAddrTable** in the Find What field and click **Close**. Verify **ipAddrTable** is selected in the left panel and **.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable** is listed in the ObjectID field.

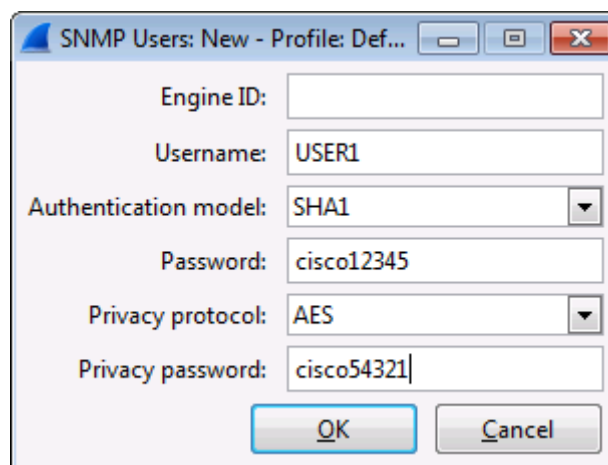
- f. Click **Operation** > **GET** to get all the objects under the select MIB object, **ipAddrTable** in this instance.



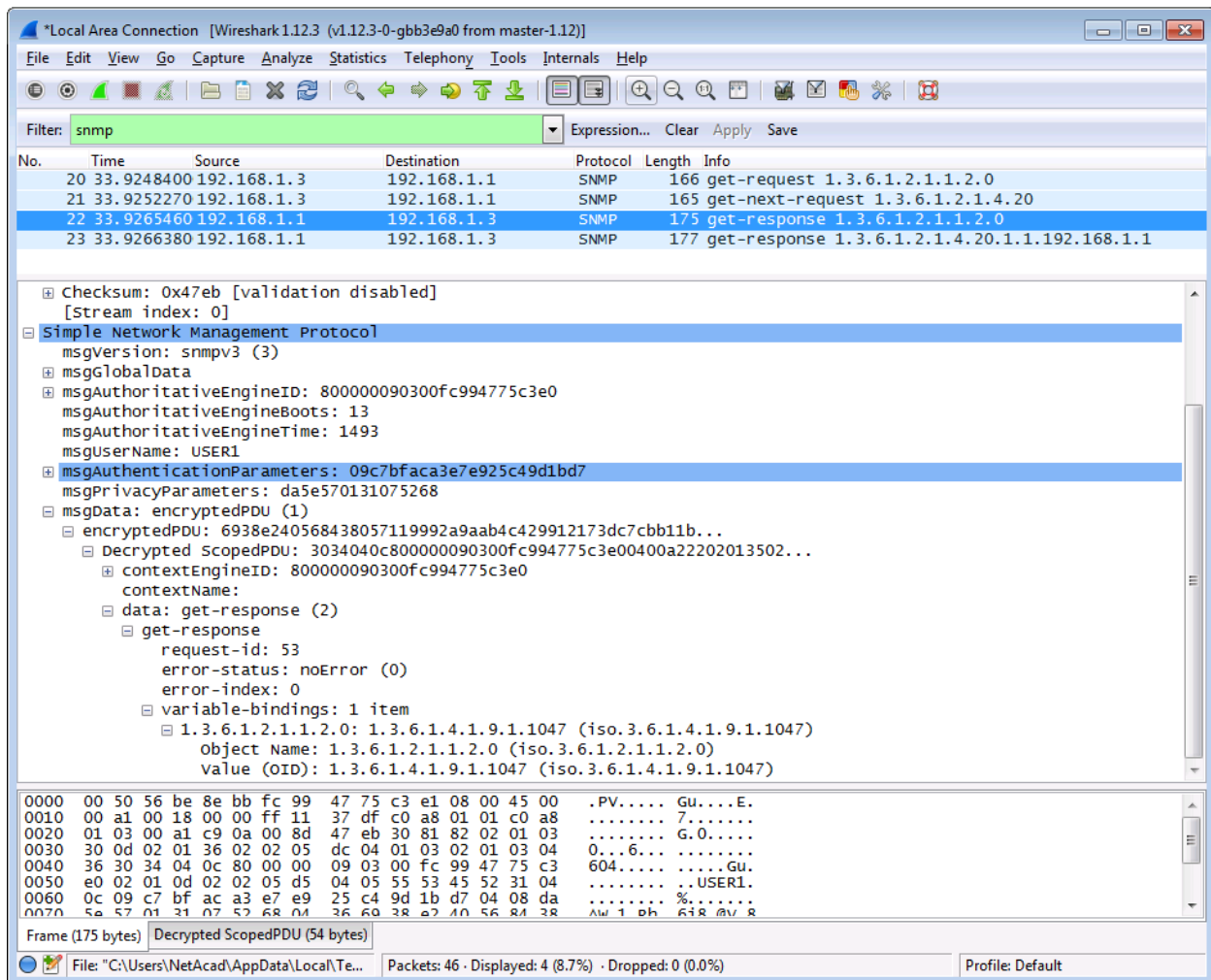
- g. Navigate back to the Wireshark screen. Stop the live capture.
- h. In the Results panel, right-click one of the results. Select **Protocol Preferences** > **Simple Network Management Preferences**.



- i. Click **Edit** for the Users Table. Click **New** and enter user information in Step 1. Click **OK**.



- j. Click **OK** to accept the user information. Click **OK** again to exit the Wireshark Preferences window.
- k. Select one of the lines. Expand the SNMP result and view the decrypted messages.



Step 4: Review your results.

What are the IP addresses configured on R1 in the SNMPv3 results?

Compare the Wireshark decrypted SNMP packets and MIB Browser results. Record your observations.

Reflection

1. What are some of the potential benefits of monitoring a network with SNMP?

2. Why is it preferable to solely use read-only access when working with SNMPv2?

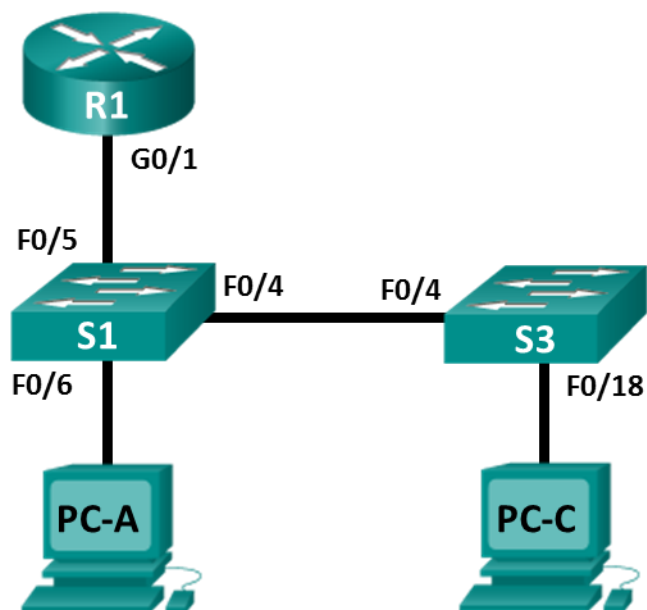
3. What are the benefits of using SNMPv3 over SNMPv2?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 13 – Implement Local SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

Background / Scenario

As the network administrator you want to analyze traffic entering and exiting the local network. To do this, you will set up port mirroring on the switch port connected to the router and mirror all traffic to another switch port. The goal is to send all mirrored traffic to an intrusion detection system (IDS) for analysis. In this initial implementation, you will send all mirrored traffic to a PC which will capture the traffic for analysis using a port sniffing program. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. SPAN is a type of port mirroring that sends copies of a frame entering a port, out another port on the same switch. It is common to find a device running a packet sniffer or Intrusion Detection System (IDS) connected to the mirrored port.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for the router.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.
- c. Configure an IP address for the router as listed in the Addressing Table.
- d. Assign **class** as the encrypted privileged EXEC mode password.
- e. Assign **cisco** for the console and vty password, enable login.
- f. Set the vty lines to **transport input telnet**.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.
- c. Assign **class** as the encrypted privileged EXEC mode password.
- d. Configure IP addresses for the switches as listed in the Addressing Table.
- e. Configure the default gateway on each switch.
- f. Assign **cisco** for the console and vty password and enable login.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- h. Copy the running configuration to the startup configuration.

Step 6: Verify connectivity.

- a. From PC-A, you should be able to ping the interface on R1, S1, S3, and PC-C. Were all pings successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

- b. From PC-C, you should be able to ping the interface on R1, S1, S3, and PC-A. Were all pings successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

To configure Local SPAN you need to configure one or more source ports called monitored ports and a single destination port also called a monitored port for copied or mirrored traffic to be sent out of. SPAN source ports can be configured to monitor traffic in either ingress or egress, or both directions (default).

The SPAN source port will need to be configured on the port that connects to the router on S1 switch port F0/5. This way all traffic entering or exiting the LAN will be monitored. The SPAN destination port will be configured on S1 switch port F0/6 which is connected to PC-A running Wireshark.

Step 1: Configure SPAN on S1.

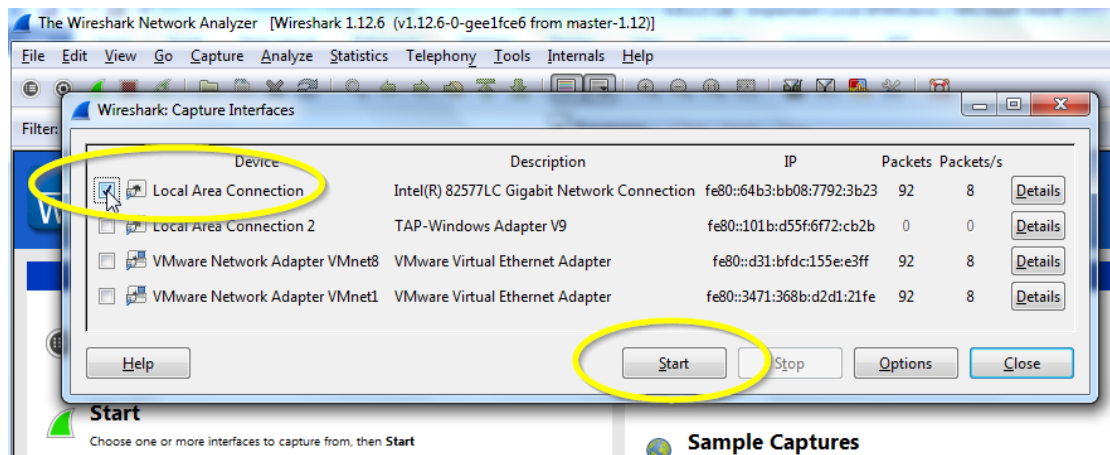
- a. Console into S1 and configure the source and destination monitor ports on S1. Now all traffic entering or leaving F0/5 will be copied and forwarded out of F0/6

```
S1(config)# monitor session 1 source interface f0/5
```

```
S1(config)# monitor session 1 destination interface f0/6
```

Step 2: Start a Wireshark Capture on PC-A.

- a. Open Wireshark on PC-A, set the capture interface to the Local Area Connection and click **Start**.



Step 3: Telnet into R1 and create ICMP traffic on the LAN.

- a. Telnet from S1 to R1.

```
S1# Telnet 192.168.1.1
```

```
Trying 192.168.1.1 . . . Open
```

User Access Verification

Password:

R1>

- b. From privileged mode, ping PC-C, S1 and S3.

R1> **enable**

Password:

R1# **ping 192.168.1.10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1# **ping 192.168.1.2**

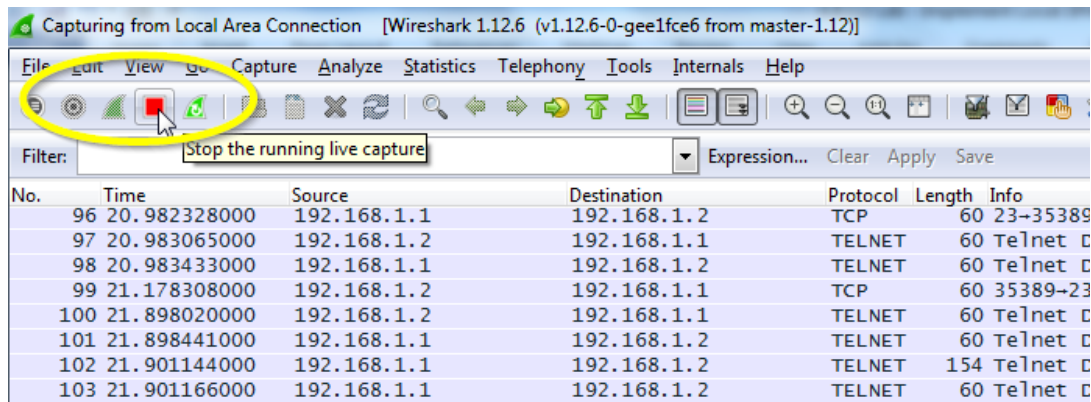
<Output omitted>

R1# **ping 192.168.1.3**

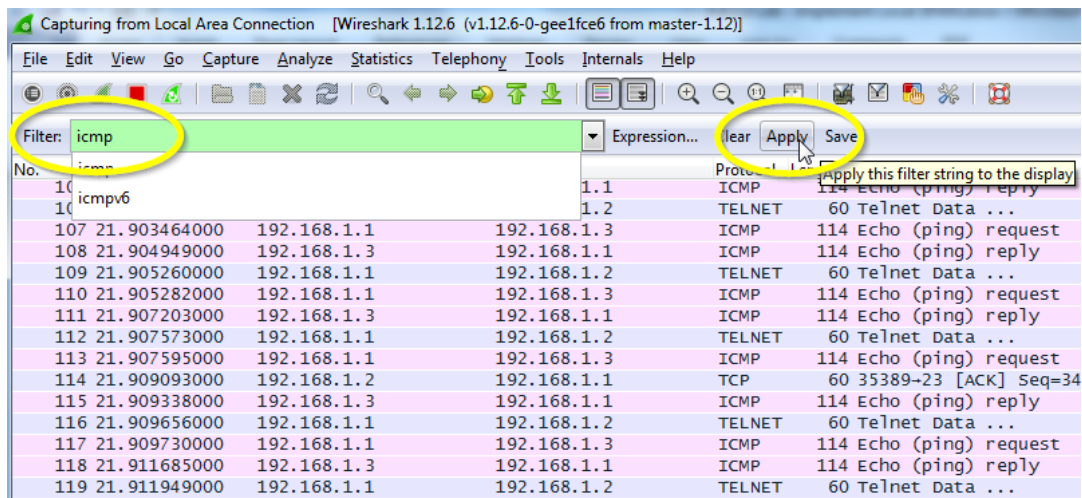
<Output omitted>

Step 4: Stop the Wireshark Capture on PC-A and Filter for ICMP.

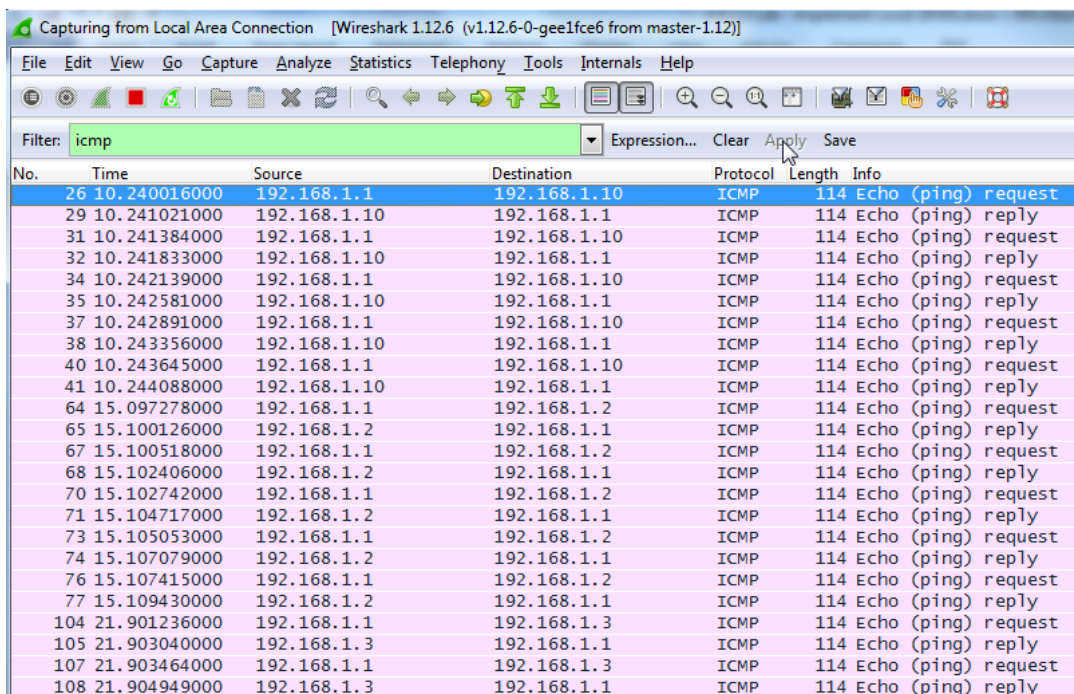
- a. Return to PC-A and stop the running Wireshark capture on PC-A.



- b. Filter the Wireshark capture for ICMP packets.



- c. Examine the Wireshark capture filtered for ICMP packets.



- d. Were the pings from R1 to PC-C, S1 and S3 successfully copied and forwarded out f0/6 to PC-A?

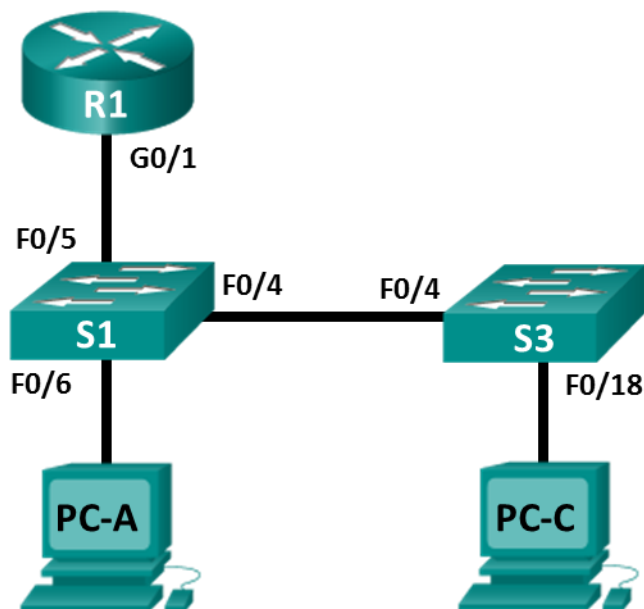
- e. Was the traffic monitored and copied in both directions? _____

Reflection

In this scenario, instead of using PC-A, and a packet sniffer, would an IDS or an IPS be more appropriate?

Lab 14 – Troubleshoot LAN Traffic Using SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

Background / Scenario

As the network administrator you decide to analyze the internal local area network for suspicious network traffic and possible DoS or reconnaissance attacks. To do this, you will set up port mirroring on all active switchports and mirror/copy all traffic to a designated switch port where a PC running Wireshark can analyze the captured traffic. The goal is to identify the source of suspicious traffic. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. It is common to find a device running a packet sniffer or Intrusion Detection System (IDS) connected to the mirrored port.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term or PuTTY, Wireshark, and Zenmap)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for the router.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.

-
- c. Configure an IP address for the router as listed in the Addressing Table.
 - d. Assign **class** as the encrypted privileged EXEC mode password.
 - e. Assign **cisco** for the console and vty password, enable login.
 - f. Set the vty lines to **transport input telnet**
 - g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
 - h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure the device name as shown in the topology.
- c. Assign **class** as the encrypted privileged EXEC mode password.
- d. Configure IP addresses for the switches as listed in the Addressing Table.
- e. Configure the default gateway on each switch.
- f. Assign **cisco** for the console and vty password and enable login.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- h. Copy the running configuration to the startup configuration.

Step 6: Verify connectivity.

- a. From PC-A, you should be able to ping the interface on R1, S1, S3, and PC-C. Were all pings successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.
- b. From PC-C, you should be able to ping the interface on R1, S1, S3, and PC-A. Were all pings successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure Local SPAN and Capture Copied Traffic with Wireshark

To configure Local SPAN, you need to configure one or more source ports called monitored ports, and a single destination port, also called a monitored port, for copied or mirrored traffic to be sent out of. SPAN source ports can be configured to monitor traffic in either ingress, or egress, or both directions (default).

Step 1: Configure SPAN on S1.

- a. Locate the switchports that are up on S1

S1# **show ip interface brief**

Which switchports are physically up and logically up? _____

On S1, F0/6 connects to PC-A which will be used for analyzing traffic with Wireshark. F0/6 will be the SPAN destination monitor port for duplicated packets. F0/4 and F0/5 will be the source monitor ports for

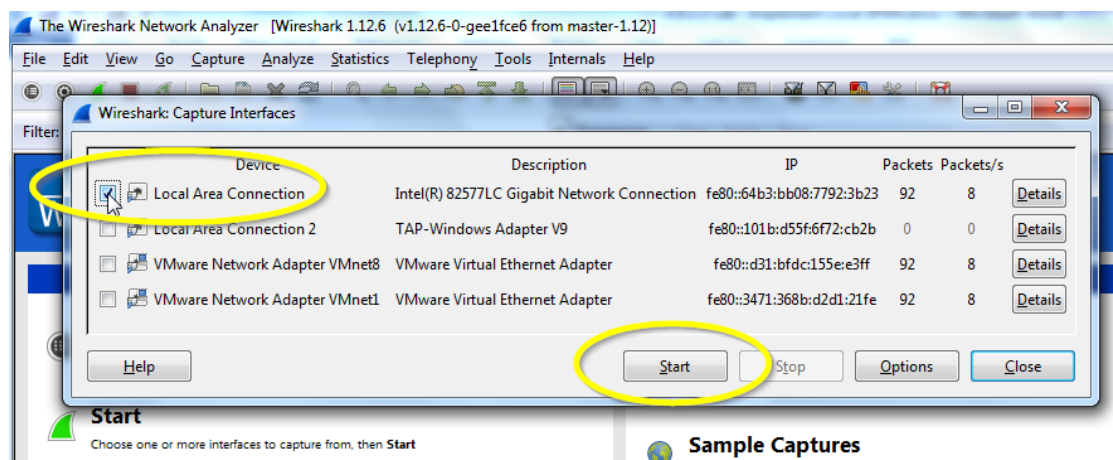
intercepted packets. You can configure multiple source monitor ports but only one destination monitor port.

```
S1(config)# monitor session 1 source interface f0/4 - 5
```

```
S1(config)# monitor session 1 destination interface f0/6
```

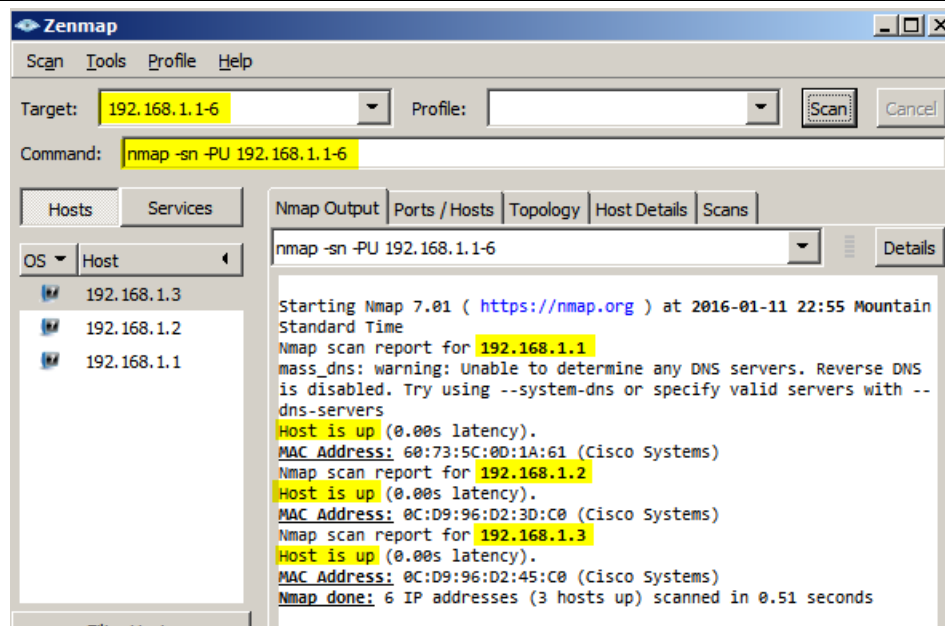
Step 2: Start a Wireshark Capture on PC-A.

- Open Wireshark on PC-A, set the capture interface to the Local Area Connection and click Start.

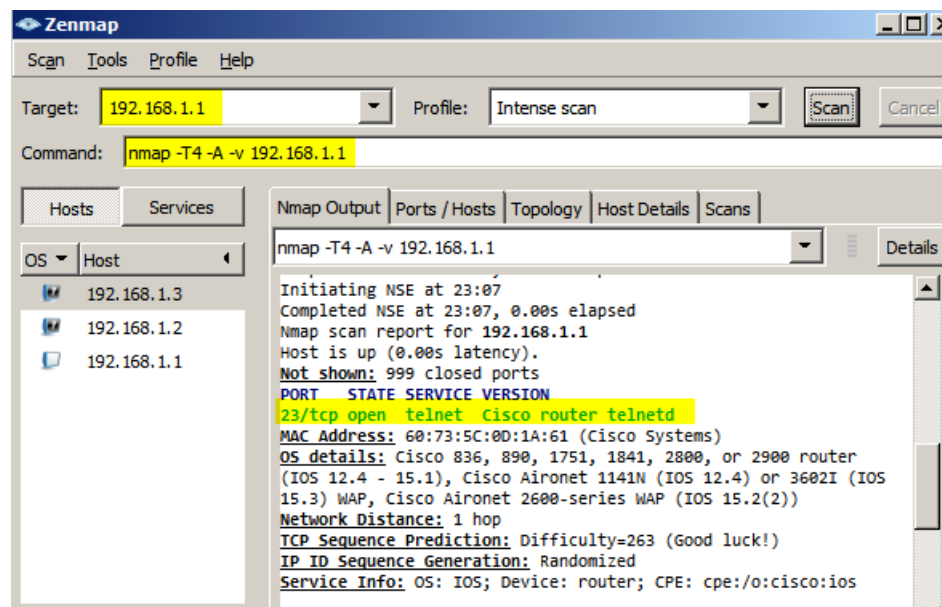


Step 3: From PC-C, Use NMAP to Generate Suspicious Traffic.

- If necessary, navigate to NMAP.org to download Zenmap. Scroll down the page to find the latest stable release for PC-C. Then following the on-screen instructions to install Zenmap with default settings.
- Open Zenmap on PC-C and run a UDP ping scan to scan for available hosts (`nmap -sn -PU 192.168.1-6`). The scan result identifies 3 hosts on the network R1, S1, and S2 at 192.168.1.1, 192.168.1.2 and 192.168.1.3. Notice that Zenmap has also identified the MAC addresses of the three hosts as Cisco Systems interfaces. If this were a real network reconnaissance attack the scan might involve the entire range of network hosts as well as ports and OS fingerprinting.

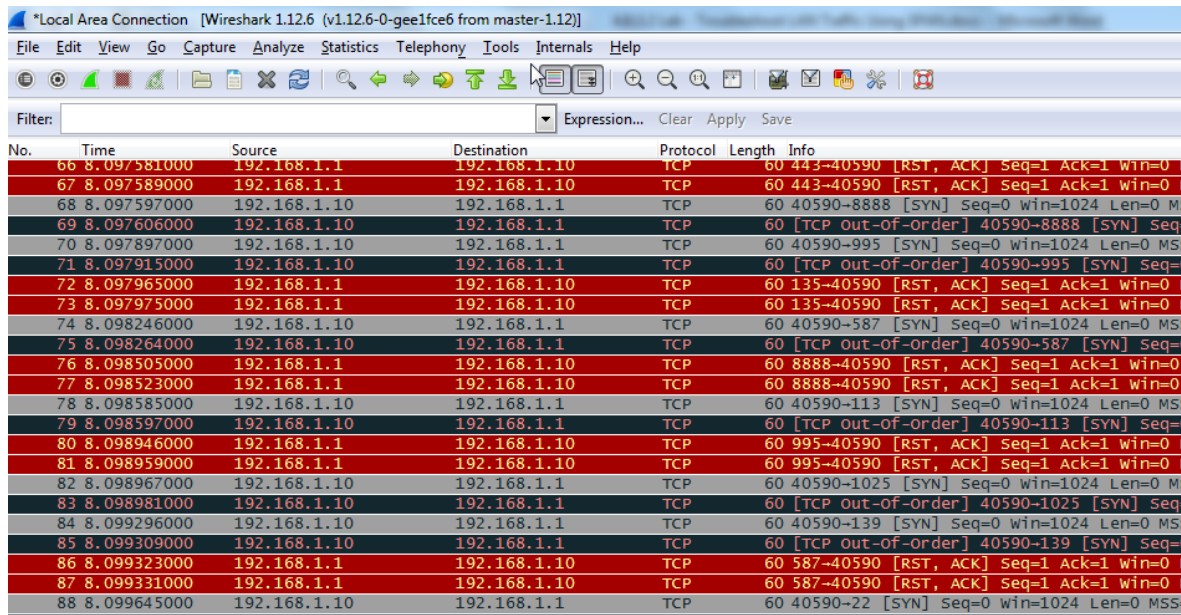


- c. The hypothetical attacker can now issue an intense scan on R1 at 192.168.1.1 (nmap -T4 -A -v 192.168.1.1). The scan result identifies an open port 23/Telnet.



Step 4: From PC-A Stop the Wireshark Capture and Examine the Captured SPAN Packets.

- a. Return to PC-A, and stop the Wireshark capture. Notice the non-standard traffic patterns between PC-C at 192.168.1.10 and R1 at 192.168.1.1. It is filled with Out-Of-Order segments and Connection resets (RST). This packet capture identifies PC-C as sending suspicious traffic to router R1.



No.	Time	Source	Destination	Protocol	Length	Info
66	8.097581000	192.168.1.1	192.168.1.10	TCP	60	443->40590 [RST, ACK] Seq=1 Ack=1 win=0
67	8.097589000	192.168.1.1	192.168.1.10	TCP	60	443->40590 [RST, ACK] Seq=1 Ack=1 win=0
68	8.097597000	192.168.1.10	192.168.1.1	TCP	60	40590->8888 [SYN] Seq=0 win=1024 Len=0 M
69	8.097606000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->8888 [SYN] Seq=
70	8.097897000	192.168.1.10	192.168.1.1	TCP	60	40590->995 [SYN] Seq=0 win=1024 Len=0 MS
71	8.097915000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->995 [SYN] Seq=
72	8.097965000	192.168.1.1	192.168.1.10	TCP	60	135->40590 [RST, ACK] Seq=1 Ack=1 win=0
73	8.097975000	192.168.1.1	192.168.1.10	TCP	60	135->40590 [RST, ACK] Seq=1 Ack=1 win=0
74	8.098246000	192.168.1.10	192.168.1.1	TCP	60	40590->587 [SYN] Seq=0 win=1024 Len=0 MS
75	8.098264000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->587 [SYN] Seq=
76	8.098505000	192.168.1.1	192.168.1.10	TCP	60	8888->40590 [RST, ACK] Seq=1 Ack=1 win=0
77	8.098523000	192.168.1.1	192.168.1.10	TCP	60	8888->40590 [RST, ACK] Seq=1 Ack=1 win=0
78	8.098585000	192.168.1.10	192.168.1.1	TCP	60	40590->113 [SYN] Seq=0 win=1024 Len=0 MS
79	8.098597000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->113 [SYN] Seq=
80	8.098946000	192.168.1.1	192.168.1.10	TCP	60	995->40590 [RST, ACK] Seq=1 Ack=1 win=0
81	8.098959000	192.168.1.1	192.168.1.10	TCP	60	995->40590 [RST, ACK] Seq=1 Ack=1 win=0
82	8.098967000	192.168.1.10	192.168.1.1	TCP	60	40590->1025 [SYN] Seq=0 win=1024 Len=0 M
83	8.098981000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->1025 [SYN] Seq=
84	8.099296000	192.168.1.10	192.168.1.1	TCP	60	40590->139 [SYN] Seq=0 win=1024 Len=0 MS
85	8.099309000	192.168.1.10	192.168.1.1	TCP	60	[TCP out-of-order] 40590->139 [SYN] Seq=
86	8.099323000	192.168.1.1	192.168.1.10	TCP	60	587->40590 [RST, ACK] Seq=1 Ack=1 win=0
87	8.099331000	192.168.1.1	192.168.1.10	TCP	60	587->40590 [RST, ACK] Seq=1 Ack=1 win=0
88	8.099645000	192.168.1.10	192.168.1.1	TCP	60	40590->22 [SYN] Seq=0 win=1024 Len=0 MSS

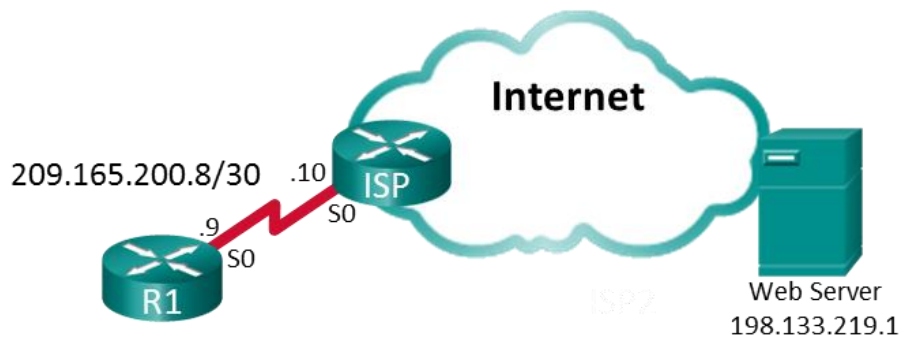
- b. The attacker on PC-C knowing that the router has an open port on 23 could attempt an additional brute force attack or DoS style attack, like a LAND attack. A LAND attack is a TCP SYN packet with the same source and destination IP address and port number. Using Zenmap, the command **nmap -sS 192.168.1.1 -S 192.168.1.1 -p23 -g23 -e eth0** is an example. Notice how the LAND attack sets both the source and destination IP addresses to 192.168.1.1 and both the source and destination port numbers to the open port at 23. Although R1 with IOS15 is not vulnerable to this older type of DoS attack, many older systems and servers are still vulnerable. This attack will crash vulnerable systems, by setting them into an infinite loop.

Reflection

In this scenario, SPAN was used to troubleshoot and identify the source of suspicious activity on the network? What other troubleshooting scenarios might SPAN be useful for?

Lab 15 – Configure IP SLA ICMP Echo

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	209.165.200.9	255.255.255.252	N/A
ISP	S0/0/0	209.165.200.10	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure IP SLA ICMP Echo on R1

Part 3: Test and Monitor the IP SLA Operation

Background / Scenario

An outside vendor has been contracted to provide web services for your company. As the network administrator, you have been asked to monitor the vendor's service. You decide to configure IP SLA to help with that task.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Serial cable as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for R1.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Configure an IP address for the router as listed in the Addressing Table.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** for the console and vty password, enable login.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Configure the default route for R1 to the ISP S0/0/0 IP address.
- Copy the running configuration to the startup configuration.

Step 4: Copy and paste the configuration to the ISP router.

The ISP router configuration is provided below. Copy and paste this configuration into the ISP router. Loopback 0 is being used to simulate the Web server shown in the Topology.

```
hostname ISP
no ip domain lookup
interface Loopback0
 ip address 198.133.219.1 255.255.255.255
interface Serial0/0/0
 ip address 209.165.200.10 255.255.255.252
 no shut
end
```

Step 5: Verify connectivity.

- a. From R1, you should be able to ping the ISP Serial interface IP address. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

- b. From R1, you should be able to ping the Web Server IP address. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure IP SLA ICMP Echo on R1

In Part 2, you configure an IP SLA ICMP Echo operation on R1. Use the following parameters for this operation:

- Operation-number: **22**
- ICMP Echo Destination Address: **198.133.219.1**
- Frequency: **20 seconds**
- Schedule Start: **Now**
- Schedule Life time: **Forever**

Step 1: Create an IP SLA Operation.

Step 2: Configure the ICMP Echo Operation.

Step 3: Set the rate the IP SLA operation repeats.

Step 4: Schedule the IP SLA ICMP Echo operation.

Step 5: Use show command to verify the IP SLA configuration.

Part 3: Test and Monitor the IP SLA Operation

In Part 3, you will simulate an outage of web services. This can be done by an administratively shutdown of the loopback 0 interface on the ISP router. You will then display the IP SLA operation statistics to monitor the effect of this test.

Step 1: Shutdown the loopback 0 interface on the ISP router.

```
ISP(config)# interface Lo0
ISP(config-if)# shutdown
ISP(config-if)#
*Nov 28 14:00:52.823: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
```

```
*Nov 28 14:00:53.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
ISP(config-if)#
```

Note: Wait a few minutes before executing Step 2.

Step 2: Activate the loopback 0 interface on the ISP router.

```
R2(config-if)# no shutdown
R2(config-if)#
*Nov 28 14:04:23.263: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Nov 28 14:04:24.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R2(config-if)#
```

Step 3: Issue the command used to display the IP SLA operation statistics on R1.

```
R1# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 22
  Latest RTT: 1 milliseconds
Latest operation start time: 18:44:45 UTC Thu Jan 28 2016
Latest operation return code: OK
Number of successes: 103
Number of failures: 10
Operation time to live: Forever
```

Note: You should see a failure count greater than zero if you waited more than 20 seconds before re-activating the loopback 0 interface on the ISP router.

The IP SLA configured in Part 2 will run forever. How would you stop the IP SLA from running but still leave the IP SLA configured to use at a future time?

Reflection

Using the lab's **show ip sla statistics** example, what does the failure count indicate about the Web Server?
