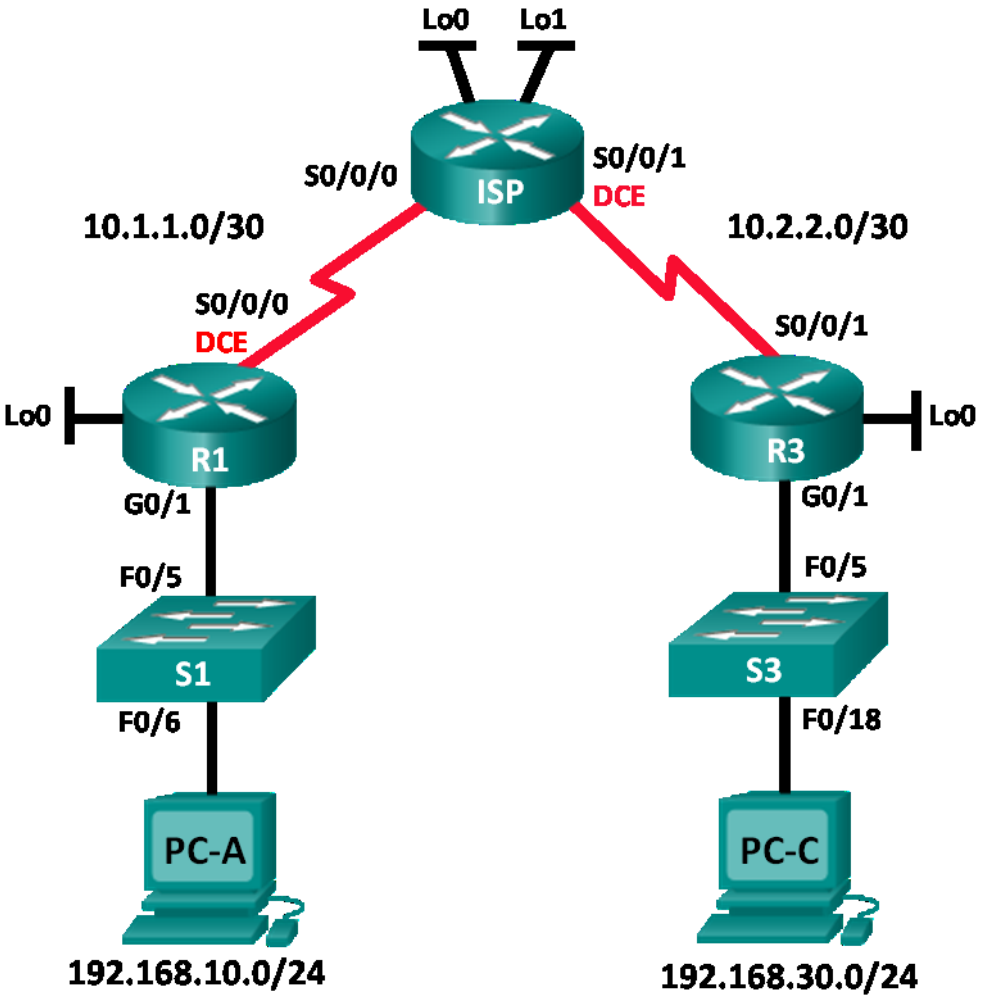
Lab – Configuring and Verifying Extended ACLs (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

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.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

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.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Create a loopback interface on R1.

d. Configure interface IP addresses as shown in the Topology and Addressing Table.

e. 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
```

```
ISP(config)# router ospf 1
ISP(config-router)# network 209.165.200.224 0.0.0.31 area 0
ISP(config-router)# network 209.165.201.0 0.0.0.31 area 0
ISP(config-router)# network 10.1.1.0 0.0.0.3 area 0
ISP(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 192.168.30.0 0.0.0.255 area 0
R3(config-router)# network 192.168.40.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 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? _____ Yes

b. From R1, ping PC-C and the loopback and serial interface on R3.

Were your pings successful? _____ Yes

c. From PC-C, ping PC-A and the loopback and serial interface on R1.

Were your pings successful? _____ Yes

d. From R3, ping PC-A and the loopback and serial interface on R1.

Were your pings successful? _____ Yes

e. From PC-A, ping the loopback interfaces on the ISP router.

Were your pings successful? _____ Yes

f. From PC-C, ping the loopback interfaces on the ISP router.

Were your pings successful? _____ Yes

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?

_____

100 – 199 and 2000 to 2699

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?

_____

80 is the destination port. TCP port 80 is a well-known port used for the HTTP protocol.

To what interface should ACL 100 be applied?

_____

_____

There are two possible answers here: G0/1 and S0/0/0. Placing it on G0/1 could block the users on network 192.168.10.0/24 from getting to any other LANs attached to R1 such as the 192.168.20.0/24 network. For this reason you will place it on S0/0/0.

In what direction should ACL 100 be applied?

_____

_____

If G0/1 interface was used for the previous answer, ACL 100 should be applied going **in**. If student answered with S0/0/0, ACL 100 would be applied going **out**.

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.

_____

_____

_____

The pings failed. Message was "Reply from 192.168.10.1: Destination net unreachable." This is because of the implicit **deny any** at the end of every ACL. ACL 100 only allows out Web and SSH traffic.

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? _____ WEB-POLICY

In what direction is the ACL applied? _____ Out

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?

_____

The pings failed. Only web traffic is allowed to exit from the 192.168.30.0/24 network.

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? _____ 2 lines, numbered 10 and line 20

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?

Line 30. The last line in the ACL.

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? 2 lines, numbered 10 and 20

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? Yes

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

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

The ACLs on both R1 and R3 were still applied to their respective interfaces with the **ip access-group command**.

Reflection

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

ACLs can unintentionally block legitimate traffic from entering or leaving a network.

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

They both have their purpose and place in a network. A standard ACL is easy to write and configure if you need to permit or deny all traffic. The downside of a standard ACL is that it can only check source addresses

and has no granularity. Extended ACLs can be written to filter virtually any kind of traffic generated. However, they can be complex to configure and understand.

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?

_____

_____

_____

_____

OSPF updates originate from the serial interfaces on R1 and R3 and not from within the LAN. ACLs filter traffic passing through the router and not traffic sourced by the router. If an ACL had been placed on the ISP router, it may have blocked OSPF updates between R1 and R3, as well as other router-to-router communication. This could have resulted in loss of connectivity between the PC-A and PC-C LANs.

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.

Device Configs

Router R1

```
R1# show run
Current configuration : 1811 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain lookup
!
username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
interface Loopback0
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group 100 out
 clock rate 128000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 area 0
 network 192.168.20.0 area 0
!
ip http server
ip http authentication local
no ip http secure-server
!
access-list 100 remark Allow Web & SSH Access
access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
access-list 100 permit tcp any any eq www
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
 transport input all
!
end
```

Router ISP

```
ISP# sh run
Building configuration...
```

```
Current configuration : 1657 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain lookup
!
username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface Loopback1
 ip address 209.165.201.1 255.255.255.224
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 209.165.200.224 0.0.0.31 area 0
 network 209.165.201.0 0.0.0.31 area 0
!
ip http server
ip http authentication local
no ip http secure-server
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
 transport input all
!
end
```

Router R3

```
R3# show run
Building configuration...
Current configuration : 1802 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain lookup
ip domain name cisco.com
!
username admin privilege 15 secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
ip ssh version 1
!
interface Loopback0
 ip address 192.168.40.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group WEB-POLICY out
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.0 area 0
 network 192.168.40.0 area 0
!
ip http server
ip http authentication local
no ip http secure-server
!
ip access-list extended WEB-POLICY
 permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq www
 permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq www
 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
!
line con 0
 password cisco
 logging synchronous
```

```
 login
line vty 0 4
 login local
 transport input ssh
!
end
```

Switch S1

```
S1# sh run
Building configuration...
Current configuration : 1416 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
```

```
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.10.11 255.255.255.0
!
ip default-gateway 192.168.10.1
ip http server
ip http secure-server
line con 0
line vty 5 15
!
end
```

Switch S3

```
S3# show run
Building configuration...
Current configuration : 1416 bytes
version 15.0
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname S3
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
```

```
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
interface Vlan1
 ip address 192.168.30.11 255.255.255.0
!
ip default-gateway 192.168.30.1
ip http server
ip http secure-server
!
line con 0
line vty 5 15
!
end
```