Cisco

Configuring ssh

a.     Using the command prompt on **PC1**, Telnet to **S1**. The user EXEC and privileged EXEC password is **cisco**.

PC1 > Desktop > Command Propt   
PC>telnet 10.10.10.2  
pass : cisco

b.    Save the current configuration so that any mistakes you might make can be reversed by toggling the power for **S1**.  
S1>en  
pass : cisco  
S1#copy run start

c.     Show the current configuration and note that the passwords are in plain text. Enter the command that encrypts plain text passwords**.**  
S1#sh run

d.    Verify that the passwords are encrypted.  
S1#conf t  
S1(config)#service password-encryption  
S1(config)#end  
a.     Configure the domain name to be **netacad.pka**.  
S1#conf t  
S1(config)#ip domain-name netacad.pka

b.    Secure keys are needed to encrypt the data. Generate the RSA keys using a 1024 key length.  
S1(config)#crypto key generate rsa  
How many bits in the modulus [512] : 1024  
a.     Create an **administrator** user with **cisco** as the password.  
S1(config)#user administrator password cisco

b.    Configure the VTY lines to check the local username database for login credentials and to only allow SSH for remote access. Remove the existing vty line password.  
S1(config)#line vty 0 15  
S1(config-line)#no password  
S1(config-line)#no login  
S1(config-line)#login local  
S1(config-line)#transport input ssh  
S1(config-line)#exit

Configuring switch port security

Enable

Conf t

a.     Access the command line for **S1**and enable port security on Fast Ethernet ports 0/1 and 0/2.

Interface range fastEthernet 0/1-2

b.    Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

Switchport port-security

Switchport port-security maximum 1

c.     Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

Switchport port-security mac-address sticky

d.    Set the violation so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but packets are dropped from an unknown source.

Switchport port-security violation restrict

•http://www.cisco.com/c/dam/en/us/td/i/templates/blank.gif**protect**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.

•http://www.cisco.com/c/dam/en/us/td/i/templates/blank.gif**restrict**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.

•http://www.cisco.com/c/dam/en/us/td/i/templates/blank.gif**shutdown**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Exit

Exit

e.     Disable all the remaining unused ports. Hint: Use the **range**keyword to apply this configuration to all the ports simultaneously.

Conf t

Interface range fastEthernet 0/3-24

Shutdown

Interface range GigabitEthernet 1/1-2

Shutdown

Exit

Configuring troubleshooting switch port security

En

          Enter the command to view the port status. What is the state of the port?

show running-config

         Enable the port using the necessary command.

conf t

interface fa0/1

no sh

Skills Integration Challenge

         Configure **S1**with the following initial settings:

-       Hostname

-       Banner that includes the word **warning**

-       Console port login and password **cisco**

-       Encrypted enable password of **class**

-       Encrypt plain text passwords

-       Management interface addressing

En

Conf t

Hostname S1

Banner motd #warning#

Line console 0

Pass cisco

Login

Exit

Enable secret class

Service password-encryption

Int vlan 1

Ip add 10.10.10.2 255.255.255.0

No sh

Exit

         Configure SSH to secure remote access with the following settings:

-       Domain name of **cisco.com**

-       RSA key-pair parameters to support SSH version 2

-       Set SSH version 2

-       User **admin** with password **ccna**

-       VTY lines only accept SSH connections and use local login for authentication

Ip domain-name cisco.com

Crypto key generate rsa

1024

Ip ssh version 2

User admin pass ccna

Line vty 0 15

Login local

Transport input ssh

         Configure the port security feature to restrict network access.

-       Disable all unused ports.

-       Set the interface mode to access.

-       Enable port security to allow only two hosts per port.

-       Record the MAC address in the running configuration.

-       Ensure that port violations disable ports.

End

Conf t

Int range fa0/1-24, g1/1-2

Sh

Exit

Int range fa0/1-2

Switchport mode access

Switchport port-security maximum 2

Switchport port-security mac-address sticky

Switchport port-security violation shutdown

Configuring Vlan

**Step 1:**     **Create and name VLANs on S1.**

Create the following VLANs. Names are case-sensitive:

         VLAN 10: Faculty/Staff

         VLAN 20: Students

         VLAN 30: Guest(Default)

         VLAN 99: Management&Native

S1,2,3

En

Conf t

Vlan 10

Name faculty/staff

Vlan 20

Name students

Vlan 30

Name guest(default)

Vlan 99

Name Management&native

**Step 1:**     **Assign VLANs to the active ports on S2.**

Assign the VLANs to the following ports:

         VLAN 10: Fast Ethernet 0/11

         VLAN 20: Fast Ethernet 0/18

         VLAN 30: Fast Ethernet 0/6

S2,3

Int f0/6

Switchport access vlan 30

Switchport mode access

Int fa0/18

Switchport mode access

Switchport access vlan 20

Int f0/11

Switchport mode access

Switchport access vlan 10

Configuring Trunks

**Step 1:**     **Setting up trunk.**

En

Show vlan brief

S1

En

Conf t

Int g1/1

Switchport trunk native vlan 99

Switchport mode trunk

No sh

Int g1/2

Switchport mode trunk

Switchport trunk native vlan 99

No sh

Show interface trunk

S2,3

Show interface trunk

Conf t

Int g1/1

Switchport mode trunk

Switchport trunk native vlan 99

No sh

Troubleshooting a VLAN

         Ports assigned to the correct VLANs.

En

Show vlan brief (om vlan te checken)

Conf t

Int f0/11

Switchport access vlan 10

Interface f0/18

Switchport access vlan 20

No sh

Exit

         Ports configured for the correct mode.

Show interface switchport f0/06 (om modes te cheken)

Show interface trunk (om trunking te checken)

En

Conf t

Int g1/1

Switchport mode trunk

Switchport trunk native vlan 99

No sh

Troubleshooting a VLAN scenario 2

1. Masks en ip’s checken van pc’s
2. Vlans checken+ports : Show vlan brief (zorg dat alle vlans op elke switch bestaan)
3. Trunking ports checken: show interface trunk
4. Check or management vlan has ip

Skills integration challenge

S3

         IP addressing and default gateway configuration, according to the **Addressing Table**.

         Create, name, and assign VLANs according to the **VLANs and Port Assignment Table**.

         Assign the native VLAN 99 to the trunk port and disable DTP.

         Restrict the trunk to only allow VLANs 10, 20, 30, 88, and 99.

         Use VLAN 99 as the native VLAN on the trunk ports.

Ip default-gateway 172.31.88.1 (router default-gateway)

Vlan 10

Name Sales

Vlan 20

Name Production

Vlan 30

Name Marketing

Vlan 88

Name Management

Vlan 99

Name Native

Interface Vlan 88

Ip add 172.31.88.4 255.255.255.0

No sh

Int g1/2

Switchport mode trunk

Switchport trunk native vlan 99

Switchport trunk allowed 10,20,30,88,99

Switchport nonegotiate (disable DTP)

         Configure basic switch security on S3.

-       Encrypted secret password of **itsasecret**

-       Console password of**letmein**

-       VTY password of **c1$c0**(where 0 is the number zero)

-       Encrypted plain text passwords

-       MOTD banner with the message **Authorized Access Only!!**

-       Disable unused ports.

Enable secret itsasecret

Line console 0

Password letmein

Line vty 0 16

Password c1$c0

Exit

Service password-encryption

Banner motd #Authorized Access Only!!#

Int range f0/1-5

Sh

Int range f0/7-10

Sh

Int range f0/12-17

Sh

Int range f0/19-24

Sh

Int g1/1

Sh

Int f0/6

         Configure port security on **F0/6**.

-       Only two unique devices are allowed to access the port.

-       Learned MACs are added to the running configuration.

-       Secure the interface so that a notification is sent when there is a violation, but the port is not disabled.

Switchport mode access

Switchport port-security

Switchport port-security mac-address sticky

Switchport port-security maximum 2

Switchport port-security violation restrict

No sh

Exit

Interface vlan 88

Ip add 172.31.88.4 255.255.255.0

No sh

Int range f0/7-12

Switchport access vlan 10

Configuring Ipv4 interfaces

**Step 1:**     **Assign IPv4 addresses to R1 and LAN devices.**

Referring to the **Addressing Table**, configure IP addressing for **R1** LAN interfaces, **PC1** and **PC2**. The serial interface has already configured.

R1:

En conf t

Int g0/0

Ip address 172.16.20.1 255.255.255.128

No sh

Int g0/1

Ip address 172.16.20.129 255.255.255.128

No sh

Int s0/0/0

Ip add 209.165.200.255 255.255.255.252

No sh

Configuring And Verifying a Small Network

**Step 1:**     **Apply basic configurations to RTA.**

a.     Using the following information and the **Addressing Table**,configure RTA:

         Hostname and banner

         Line passwords set to **cisco**; encrypted password set to **class**

         IP addressing and descriptions on LAN interfaces

b.    Save the configuration.

En

Conf t

Int g0/0

Ip add 10.10.10.1 255.255.255.0

No sh

Int g0/1

Ip add 10.10.20.1 255.255.255.0

No sh

Exit

Hostname RTA

Banner motd #Warning! Authorized Access Only !!#

Line console 0

Password cisco

Login

Exit

Line vty 0 15

Password cisco

Enable secret class

Service password-encryption

Int g0/0

Description LAN to PC1

Int g0/1

Description LAN to PC2

End

Copy running-config startup-config

**Step 3:**     **Configure SW1 for remote management.**

a.     Using the **Addressing Table**, configure the management interface for SW1.

b.    Configure the default gateway address.

c.     Save the configuration.

Conf t

Interface vlan 1

Ip add 10.10.10.2 255.255.255.0

No sh

Exit

Ip default-gateway 10.10.10.1

Copy running-config startup-config

Configuring Router-on-a Stick Inter-VLAN routing

**Step 1:**     **Create VLANs on S1.**

Return to **Realtime** mode and create VLAN 10 and VLAN 30 on **S1**.

**Step 2:**     **Assign VLANs to ports.**

a.     Configure interface F0/6 and F0/11 as access ports and assign VLANs.

         Assign **PC1** to VLAN 10.

         Assign **PC3** to VLAN 30.

Int f0/11

Switchport mode access

Switchport access vlan 10

No sh

Int f0/6

Switchport mode access

Switchport access vlan 30

No sh

**Step 1:**     **Configure subinterfaces on R1 using the 802.1Q encapsulation.**

a.     Create the subinterface G0/0.10.

         Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.

         Refer to the **Address Table** and assign the correct IP address to the subinterface.

b.    Repeat for the G0/0.30 subinterface.

Int g0/0.10

Encapsulation dot1q 10

Ip add 127.17.10.1 255.255.255.0

Int g0/0.30

Encapsulation dot1Q 30

Ip add 127.17.30.1 255.255.255.0

Exit

Interface g0/0

No sh

**Step 2:**     **Enable trunking.**

Int g1/1

Switchport mode trunk

Switchport trunk allowed vlan 10,30

No sh

Troubleshoot inter-VLAN

1. Check PC’s (ip,mask,gateway)
2. Port on switches and vlans
   1. Show ip interfaces
   2. Show vlan
   3. Show interface trunk
3. Check router subinterfaces (ip and vlans)
   1. Show ip interface brief
   2. Show running-config

Skills integration challenge

         Assign IP addressing to **R1** and **S1** based on the **Addressing Table**.

Interface g0/0

Ip address 172.17.25.2 255.255.255.252

No sh

         Configure inter-VLAN routing on **R1** based on the **Addressing Table**.

Int g0/1.10

Encapsulation dot1Q 10

Ip add 172.10.1 255.255.255.0

Int g0/1.20

Encapsulation dot1q 20

Ip address 172.17.20.1 255.255.255.0

Int g0/1.30

Encapsulation dot1q 30

Ip address 172.17.30.1 255.255.255.0

Int g0/1.88

Encapsulation dot1q 88

Ip address 172.17.88.1 255.255.255.0

Int g0/1.99

Encapsulation dot1q 99

Ip address 172.17.99.1 255.255.255.0

Interface g0/1

No sh

         Create, name and assign VLANs on **S1** based on the **VLAN and Port Assignments Table**. Ports should be in access mode.

Int range fa0/11-17

Switchport mode access

Switchport access vlan 10

Int range fa0/18-24

Switchport mode access

Switchport access vlan 20

Int range fa0/6-10

Switchport mode access

Switchport access vlan 30

         Configure **S1** to trunk, allow only the VLANs in the **VLAN and Port Assignments Table**.

Int g1/1

Switchport mode trunk

Switchport trunk allowed vlan 10,20,30,88,99

Switchport native vlan 88

Vlan 99

Name Management

Vlan 10

Name Faculty/Staff

Vlan 20

Name Students

Vlan 30

Name Guests(default)

Vlan 88

Name Native

         Configure the default gateway on **S1.**

Ip default-gateway 172.17.99.1

Interface VLAN 99

Ip add 172.17.99.10 255.255.255.0

No sh

         All ports not assigned to a VLAN should be disabled.

Interface range f0/1-5

Sh

Configuring IPv4 Static and Default Routes

**Step 1:**     **Configure recursive static routes on R1.**

**(steunt op gateway van device)**

(ip route destination destination mask next hop)

Ip route 172.31.0.0 255.255.255.0 172.31.1.193

Ip route 172.31.1.196 255.255.255.252 172.31.1.193

Ip route 172.31.1.128 255.255.255.192 172.31.1.193

**Step 2: Configure directly attached static routes on R2.**

**(next hop is een interface)**

Ip route 172.31.1.0 255.255.255.120 Se0/0/0/0

Ip route 172.31.1.1202 55.255.255.192 Se0/0/1

**Step 3:**     **Configure a default route on R3.**

**(alle traffic verwijziging naar Se0/0/1)**

Ip route 0.0.0.0 0.0.0.0 Se0/0/1

Designing and Implementing a VLSM Addressing Scheme

**Step 1:**     **Configure IP addressing on Branch1 LAN interfaces.**

Int g0/0

Ip address 172.31.103.1 255.255.255.224

No sh

Int g0/1

Ip address 172.31.103.33 255.255.255.240

No

Int se0/0/0

Ip add 172.31.103.97 255.255.255.252

No sh

Int g0/0

Ip address 172.31.103.65 255.255.255.240

No sh

Int g0/1

Ip add 172.31.103.81 255.255.255.240

No sh

Int se0/0/0

Ip add 172.31.103.98 255.255.255.252

No sh

**Step 2:**     **Configure IP addressing on Room-312, including the default gateway.**

Interface vlan 1

Ip address 172.31.103.66 255.255.255.240

No sh

Exit

Ip default-gateway 172.31.103.65

**Step 3:**     **Configure IP addressing on PC-D, including the default gateway.**

Manueel ingeven

Congifuring IPv4 Route Summarization- Scenario 1

**Step 1:**     **Calculate a summary route on R1 to reach LANs on R3.**

a.     List the 172.22.1.128/27 and 172.22.1.160/27 networks in binary format.

172.22.1.128: 10101100.00010110.00000001.10000000

172.22.1.160: 10101100.00010110.00000001.10100000

b.    Count the left-most matching bits to determine the mask for the summary route. They have 26 left-most bits in common.

172.22.1.128: **10101100.00010110.00000001.10**000000

172.22.1.160: **10101100.00010110.00000001.10**100000

c.     Copy the matching bits and fill in the remaining bits with zeros to determine the summarized network address.

10101100.00010110.00000001.10000000

**Step 1:**     **Configure a summary route for R1.(recursive)**

Ip route 172.22.1.128 255.255.255.192 172.131.157.98

**Step 2:**     **Configure a summary route for R3.(directly attached)**

Ip route 172.31.157.0 255.255.255.128 se0/0/1

Configuring IPv4 Route Summarization

**Part 1:**     **Calculate Summary Routes**

Branch 1 routes:

172.22.70.(00000000)

172.22.70.(10000000)

Summary 172.22.70.0/24

Branch 2 routes:

172.22.(01000100).0

172.22.(01000101).0

Summary 172.22.68.0 /23 (11111110) (255-1)=254

HQ routes:

172.22.(01000000).0

172.22.(01000010).0

Summary 172.22.64.0 /22 (11111100) (255-3)=252

ISP routes:

172.22.(01000110).(00000000)

172.22.(01000110).(10000000)

172.22.(01000100).0

172.22.(01000101).0

172.22.(01000000).0

172.22.(01000010).0

Summary 172.22.64.0 /21 (11111000) (255-1-2-4)=248

**Step 1:**     **Configure the summary routes on the HQ router to other networks.**

a.     Configure a directly attached summary route on **HQ** to reach the **Branch1** LANs.

b.    Configure a recursive summary route on **HQ** to reach the **Branch2** LANs.

En

Conf t

Ip route 172.22.70.0 255.255.255.0 se0/0/0

Ip route 172.22.68.0 255.255.254.0 172.22.71.6

**Step 2:**     **Configure the summary routes on the Branch1 router to other networks.**

a.     Configure a recursive summary route on **Branch1** to reach the **HQ** LANs.

b.    Configure a recursive summary route on **Branch1** to reach the **Branch2** LANs.

En

Conf t

Ip route 172.22.64.0 255.255.252.0 172.22.71.1

Ip route 172.22.68.0 255.255.254.0 172.22.71.1

**Step 3:**     **Configure the summary routes on the Branch2 router to other networks.**

a.     Configure a directly attached summary route on **Branch2** to reach the **Branch1** LANs.

b.    Configure a recursive summary route on **Branch2** to reach the **HQ** LANs.

En

Conf t

Ip route 172.22.70.0 255.255.255.0 se0/0/1

Ip route 172.22.64.0 255.255.252.0 172.22.71.5

**Step 4:**     **Configure a summary route on ISP to reach all networks.**

En

Conf t

Ip route 172.22.64.0 255.255.248.0 se0/0/1

Configuring a floating static route

En

Conf t

Ip route 0.0.0.0 0.0.0.0 se0/0/0 (hoofdroute)

Ip route 0.0.0.0 0.0.0.0 se0/0/1 5 (back-up route)

Troubleshooting Static Route

Show ip route

No ip route (foute ip ) (foute mask)

Skills Integration Challenge

         Configure inter-VLAN routing on **R1** based on the **Addressing Table**.

En

Conf t

Interface g0/0.10

Encapsulation dot1q 10

Ip address 172.31.10.1 255.255.255.0

Interface g0/020

Encapsulation dot1q 20

Ip address 172.31.20.1 255.255.255.0

Interface g0/0.30

Encapsulation dot1q 30

Ip address 172.31.30.1 255.255.255.0

Interface g0/0.88

Encapsulation dot1q 88

Ip address 172.31.88.1 255.255.255.0

Interface g0/0.99

Encapsulation dot1q 99 native

Ip address 172.31.99.1 255.255.255.0

Interface g0/0

No sh

Int s0/0/

Ip address 172.31.1.2 255.255.255.0

         Configure trunking on **S1**.

Interface g1/1

Switchport mode trunk

Switchport trunk allowed vlan 10,20,30,88,99

Switchport trunk native vlan 99

         Configure four directly attached static route on **HQ** to each VLANs 10, 20, 30 and 88.

Ip route 172.31.10.0 255.255.0 s0/0/0

Ip route 172.31.20.0 255.255.255.0 s0/0/0

Ip route 172.31.30.0 255.255.255.0 s0/0/0

Ip route 172.31.88.0 255.255.255.0 s0/0/0

         Configure directly attached static routes on **HQ** to reach **Outside Host**.

-       Configure the primary path through the Serial 0/1/0 interface.

-       Configure the backup route through the Serial 0/1/1 interface with a 10 AD.

Ip route 209.165.200.0 255.255.255.224 s0/1/0

Ip route 209.165.200.0 255.255.255.224 s0/1/1 10

         Configure directly attached primary and backup summary routes on **ISP** for the entire 172.31.0.0/17 address space.

-       Configure the primary path through the Serial 0/1/1 interface.

-       Configure the backup route through the Serial 0/1/0 interface with 25 AD.

Ip route 172.31.0.0 255.255.128.0 s0/1/1

Ip route 172.31.0.0 255.255.128.0 s0/1/0 25

         Configure a directly attached default route on **R1**.

Ip route 0.0.0.0 0.0.0.0 s0/0/0

Configuring RIPv2

**Step 1:**     **Configure RIPv2 on R1.**

a.     Use the appropriate command to create a default route on **R1** for all Internet traffic to exit the network through S0/0/1.

b.    Enter RIP protocol configuration mode.

c.     Use version 2 of the RIP protocol and disable the summarization of networks.

d.    Configure RIP for the networks that connect to **R1**.

e.     Configure the LAN port that contains no routers so that it does not send out any routing information.

f.     Advertise the default route configured in step 1a with other RIP routers.

g.    Save the configuration.

En

Conf t

Ip route 0.0.0.0 0.0.0.0 s0/0/1

Router rip

Version 2

No auto-summary

Network 192.168.1.0

Network 192.168.2.0

Passive-interface g0/0

Default-information originate

End

Copy running-config startup-config

**Step 2:**     **Configure RIPv2 on R2.**

a.     Enter RIP protocol configuration mode.

b.    Use version 2 of the RIP protocol and disable the summarization of networks.

c.     Configure RIP for the networks directly connected to **R2**.

d.    Configure the interface that contains no routers so that it does not send out routing information.

e.     Save the configuration.

Router rip

Version 2

No auto-summary

Network 192.168.2.0

Network 192.168.3.0

Network 192.168.4.0

Passive-interface g0/0

End

Copy running-config startup-config

**Step 3:**     **Configure RIPv2 on R3**

Repeat Step 2 on **R3**.

Router rip

Version 2

No auto-summary

Network 192.168.4.0

Network 192.168.5.0

Passive-interface g0/0

End

Copy running-config startup-config

Configuring OSPFv2

**Step 1:**     **Configure OSPF on the R1, R2 and R3.**

Use the following requirements to configure OSPF routing on all three routers:

-       Process ID 10

-       Router ID for each router: R1 = 1.1.1.1; R2 = 2.2.2.2; R3 = 3.3.3.3

-       Network address for each interface

-       LAN interface set to passive (do not use the **default** keyword)

Router ospf 10

Router-id 1.1.1.1

Network 172.16.1.0 0.0.0.255 area 0

Network 192.168.10.4 0.0.0.3 area 0

Network 172.16.3.0 0.0.0.3 area 0

Passive-interface g0/0

Configuring Standard ACLs

**Part 2:**     **Configure, Apply, and Verify a Standard ACL**

**Step 1:**     **Configure and apply a numbered standard ACL on R2.**

a.     Create an ACL using the number 1 on **R2**with a statement that denies access to the 192.168.20.0/24 network from the 192.168.11.0/24 network.

R2(config)# **access-list 1 deny 192.168.11.0 0.0.0.255**

b.    By default, an access list denies all traffic that does not match a rule. To permit all other traffic, configure the following statement:

R2(config)# **access-list 1 permit any**

c.     For the ACL to actually filter traffic, it must be applied to some router operation. Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

R2(config)# **interface GigabitEthernet0/0**

R2(config-if)# **ip access-group 1 out**

**Step 2:**     **Configure and apply a numbered standard ACL on R3.**

a.     Create an ACL using the number 1 on **R3**with a statement that denies access to the 192.168.30.0/24 network from the **PC1** (192.168.10.0/24) network.

R3(config)# **access-list 1 deny 192.168.10.0 0.0.0.255**

b.    By default, an ACL denies all traffic that does not match a rule. To permit all other traffic, create a second rule for ACL 1.

R3(config)# **access-list 1 permit any**

c.     Apply the ACL by placing it for outbound traffic on the Gigabit Ethernet 0/0 interface.

R3(config)# **interface GigabitEthernet0/0**

R3(config-if)# **ip access-group 1 out**

Configuring Named Standard ACLs

**Step 2:**     **Configure a named standard ACL.**

Configure the following named ACL on **R1**.

R1(config)# **ip access-list standard File\_Server\_Restrictions**

R1(config-std-nacl)# **permit host 192.168.20.4**

R1(config-std-nacl)# **deny any**

**Note:** For scoring purposes, the ACL name is case-sensitive.

**Step 3:**     **Apply the named ACL.**

a.     Apply the ACL outbound on the interface Fast Ethernet 0/1.

R1(config-if)# **ip access-group File\_Server\_Restrictions out**

Configuring an ACL on VTY Lines

**Part 1:**     **Configure and Apply an ACL to VTY Lines**

**Step 2:**     **Configure a numbered standard ACL.**

Configure the following numbered ACL on **Router**.

Router(config)# **access-list 99 permit host 10.0.0.1**

Because we do not want to permit access from any other computers, the implicit deny property of the access list satisfies our requirements.

**Step 3:**     **Place a named standard ACL on the router.**

Access to the **Router** interfaces must be allowed, while Telnet access must be restricted. Therefore, we must place the ACL on Telnet lines 0 through 4. From the configuration prompt of **Router**, enter line configuration mode for lines 0 – 4 and use the **access-class**command to apply the ACL to all the VTY lines:

Router(config)# **line vty 0 4**

Router(config-line)# **access-class 99 in**

Skills Integration Challenge

a.     Divide 172.16.128.0/19 into two equal subnets for use on **Branch**.

1)     Assign the last usable address of the second subnet to the Gigabit Ethernet 0/0 interface.

2)     Assign the last usable address of the first subnet to the Gigabit Ethernet 0/1 interface.

3)     Document the addressing in the Addressing Table.

4)     Configure **Branch**with appropriate addressing

Int g0/0

Ip address 172.16.159.254 255.255.240.0

Int g0/1

Ip address 172.16.143.254 255.255.240.0

c.     Configure **HQ** and **Branch** with OSPF routing according to the following criteria:

         Assign the process ID 1.

         Advertise all three attached networks. Do not advertise the link to the Internet.

         Configure appropriate interfaces as passive.

Router ospf 1

Network 172.16.128.0 0.0.31.255 area 0

Network 192.168.0.0 0.0.0.3 area 0

Passive-interface g0/1

Passive-interface g0/0

Passive-interface s0/0/1 (niet naar internet)

Default-information originate

d.     Set a default route on **HQ** which directs traffic to S0/0/1 interface. Redistribute the route to **Branch**.

Ip route 0.0.0.0 0.0.0.0 s0/0/1

Skills Integration Challenge (DHCP)

         Create VLANs on **S2** and assign VLANs to appropriate ports. Names are case-sensitive

         Configure **S2** ports for trunking.

         Configure all non-trunk ports on **S2** as access ports.

Conf t

Vlan 10

Name Sales

Vlan 20

Name Production

Vlan 30

Name Marketing

Vlan 40

Name HR

Int range fa0/5-9

Switchport access vlan 10

Switchport mode access

No sh

Int range fa0/10-14

Switchport access vlan 20

Switchport mode access

No sh

Int range fa0/15-19

Switchport access vlan 30

Switchport mode access

No sh

Int range fa0/20-24

Switchport access vlan 40

Switchport mode access

No sh

Int range fa0/1-4

Switchport trunk allowed vlan 10,20,30,40

Switchport mode trunk

         Configure **R1** to route between VLANs. Subinterface names should match the VLAN number.

En

Conf t

Interface g0/0.10

Encapsulation dot1q 10

Ip address 172.31.10.1 255.255.255.224

Interface g0/0.20

Encapsulation dot1q 20

Ip address 172.31.20.1 255.255.255.240

Interface g0/0.30

Encapsulation dot1q 30

Ip address 172.31.30.1 255.255.255.128

Interface g0/0.40

Encapsulation dot1q 40

Ip address 172.31.40.1 255.255.255.192

Int g0/0

No sh

Int g0/1

         Configure **R1** to act as a DHCP server for the VLANs attached to S2.

-       Create a DHCP pool for each VLAN. Names are case-sensitive.

-       Assign the appropriate addresses to each pool.

-       Configure DHCP to provide the default gateway address

-       Configure the DNS server 209.165.201.14 for each pool.

Ip dhcp pool VLAN\_10

Network 172.31.10.1 255.255.255.224

Default-router 172.31.10.1

Dns-server 209.165.201.14

Exit

Ip dhcp pool VLAN\_20

Network 172.31.20.1 255.255.255.240

Default-router 172.31.20.1

Dns-server 209.165.201.14

Exit

Ip dhcp pool VLAN\_30

Network 172.31.30.1 255.255.255.128

Default-router 172.31.30.1

Dns-server 209.165.201.14

Exit

Ip dhcp pool VLAN\_40

Network 172.31.40.1 255.255.255.192

Default-router 172.31.40.1

Dns-server 209.165.201.14

Exit

Int g0/1

Ip address dhcp

No sh

-       Prevent the first 10 addresses from each pool from being distributed to end devices.

Ip dhcp excluded-address 172.31.10.1 172.31.10.10

Ip dhcp excluded-address 172.31.20.1 172.31.20.10

Ip dhcp excluded-address 172.31.30.1 172.31.30.10

Ip dhcp excluded-address 172.31.40.1 172.31.40.10

Configuring Static NAT

**Step 1:**     **Configure static NAT statements.**

Refer to the Topology. Create a static NAT translation to map the **Server1** inside address to its outside address.

Conf t

Ip nat inside source static 172.16.16.1 64.100.50.1

**Step 2:**     **Configure interfaces.**

Configure the correct inside and outside interfaces.

Int se0/0/0

Ip nat outside

Int g0/0

Ip nat inside

Configuring Dynamic NAT

**Step 1:**     **Configure traffic that will be permitted.**

On **R2**, configure one statement for ACL 1 to permit any address belonging to 172.16.0.0/16.

Access-list 1 permit 172.16.0.0 0.0.255.255

**Step 2:**     **Configure a pool of address for NAT.**

Configure **R2** with a NAT pool that uses all four addresses in the 209.165.76.196/30 address space.

Ip nat pool POOL 209.165.76.196 209.165.76.199 netmask 255.255.255.252

**Step 3:**     **Associate ACL1 with the NAT pool.**

Ip nat inside source list 1 pool POOL (ip nat inside source list {ACL-NR} pool {POOL\_NAME}

**Step 4:**     **Configure the NAT interfaces.**

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Int se0/0/1

Ip nat inside

Int se0/0/0

Ip nat outside

Implementing Static and Dynamic NAT

**Step 1:**     **Configure traffic that will be permitted for NAT tranlations.**

On **R2**, configure a standard ACL named **R2NAT** that uses three statements to permit, in order, the following private address spaces:192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24.

Ip access-list standard R2NAT

Permit 192.168.10.0 0.0.0.255

Permit 192.168.20.0 0.0.0.255

Permit 192.168.30.0 0.0.0.255

**Step 2:**     **Configure a pool of addresses for NAT.**

a.     Configure **R2** with a NAT pool that uses the first two addresses in the 209.165.202.128/30 address space. The fourth address is used for static NAT later in Part 2.

Ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask 255.255.255.252

**Step 3:**     **Associate the named ACL with the NAT pool and enable PAT.**

Ip nat inside source list R2NAT pool R2POOL overload

**Step 4:**     **Configure the NAT interfaces.**

Configure **R2** interfaces with the appropriate inside and outside NAT commands.

Int fa0/0

Ip nat inside

Int se0/1/0

Ip nat outside

Int se0/0/0

Ip nat inside

Int se0/0/1

Ip nat inside

**Part 2:**     **Configure Static NAT**

Refer to the Topology. Create a static NAT translation to map the **local.pka** inside address to its outside address.

Ip nat inside source static 192.168.20.254 209.165.202.131

Configuring Port Forwarding on a wireless router

**Part 1:**     **Configure Port Forwarding**

a.     From the web browser on **LaptopA**, access **LA** by entering the LAN IP address, 192.168.0.1. The username is **admin** and the password is **cisco123**.

b.    Click **Applications & Gaming**. In the first dropdown on the left, choose **HTTP**and then enter 192.168.0.2 in the “To IP Address” column. This configures **LA**to forward port 80 to 192.168.0.2. Check the **Enabled** box next to the address column.

c.     Scroll to the bottom and click **Save Settings**.

Verifying and Troubleshooting NAT Configurations

Show running-config

Skill Integration Challenge

**Cnt-Sw**

         Configure remote management access including IP addressing and SSH:

-       Domain is cisco.com

-       User **CAdmin** with password **itsasecret**

-       Crypto key length of 1024

-       SSH version 2, limited to 2 authentication attempts and a 60 second timeout

-       Clear text passwords should be encrypted.

Ip domain-name cisco.com

Username Admin password letmein

Crypto key generate rsa

Ip ssh version 2

Ip ssh authentication-retries 2

Ip ssh time-out 60

Service password-encryption

Line vty 0 15

Login local

Transport input ssh

         Configure, name and assign VLANs. Ports should be manually configured as access ports.

Vlan 15

Name Servers

Vlan 30

Name PCs

Vlan 45

Name Native

Vlan 60

Name Management

Int vlan 60

Ip address 10.10.10.146 255.255.255.240

No sh

Exit

Ip default-gateway 10.10.10.145

Int range fa0/11-20

Switchport mode access

Switchport access vlan 15

Int range fa0/1-10

Switchport mode access

Switchport access vlan 30

Int g0/1

         Configure trunking.

Switchport mode trunk

Switchport trunk native vlan 45

         Implement port security:

-       On Fa0/1, allow 2 MAC addresses that are automatically added to the configuration file when detected. The port should not be disabled, but a syslog message should be captured if a violation occurs.

Int f0/1

Switchport port-security maximum 2

Switchport port-security mac-address sticky

Switchport port-security violation restrict

-       Disable all other unused ports.

Int range f0/2-10, g0/2, f0/12-24

Sh

         Configure inter-VLAN routing.

Int g0/0.15

Encapsulation dot1q 15

Ip address 10.10.10.161 255.255.255.224

Int g0/0.30

Encapsulation dot1q 30

Ip address 10.10.10.193 255.255.255.192

Int g0/0.45

Encapsulation dot1q 45 native

Ip address 10.10.10.129 255.255.255.240

Int g0/0.60

Encapsulation dot1q

Ip address 10.10.10.145 255.255.255.240

Int g0/0

No sh

         Configure DHCP services for VLAN 30. Use **LAN**as the case-sensitive name for the pool.

Ip dhcp pool LAN

Network 10.10.10.192 255.255.255.192

Default-router 10.10.10.193

         Implement routing:

-       Use OSPF process ID 1 and router ID 1.1.1.1

-       Configure one network statement for the entire **192.168.45.0/24** address space

-       Disable interfaces that should not send OSPF messages.

Router ospf 1

Router-id 1.1.1.1

Network 10.10.10.0 0.0.0.255 area 0

Passive-interface g0/0

Passive-interface s0/1/0

Default-information originate

Exit

-       Configure a default route to the Internet.

Ip route 0.0.0.0 0.0.0.0 s0/1/0

         Implement NAT:

-       Configure a standard, one statement ACL number 1. All IP addresses belonging to the **192.168.45.0/24** address space are allowed.

Access-list 1 permit 10.10.10.0 0.0.0.255

-       Refer to your documentation and configure static NAT for the File Server.

Ip nat inside source static 10.10.10.162 198.133.219.130 {inside ip} {outside ip}

-       Configure dynamic NAT with PAT using a pool name of your choice, a /30 mask, and these two public addresses:

**64.100.32.56 and 64.100.32.57**

Ip nat pool INTERNET 198.133.219.128 198.133.219.129 netmask 255.255.255.252

Ip nat inside source list 1 pool INTERNET overload

Int g0/015

Ip nat inside

Int g0/0.45

Ip nat inside

Int g0/0.60

Ip nat inside

Int s0/0/0

Ip nat inside

Int s0/0/1

Ip nat inside

Int s0/1/0

Ip nat outside

DHCP pc aanzetten op pc