**Portfolio Task – Scenario 5**

**Introduction**

This Network Routing Principles **Scenarios** are a scaffolded approach to preparing you to succeed in your ultimate **Final Skills Assessments**. The **Scenarios** build on skills from previous **Scenarios** until all required components are covered. **Scenario 5** expands your work to cover deployment **of DHCP** on the Internal Network and **NAT** on the gateway router of the Internal Network. For **Scenario 5-P,** you will essentially repeat your work from **Scenario 4-P** to consolidate your knowledge in deployment of Interior Routing Protocols and ACLs before expanding on this in the **C/D** Tasks and in **Scenario 6-P.**

**Purpose**

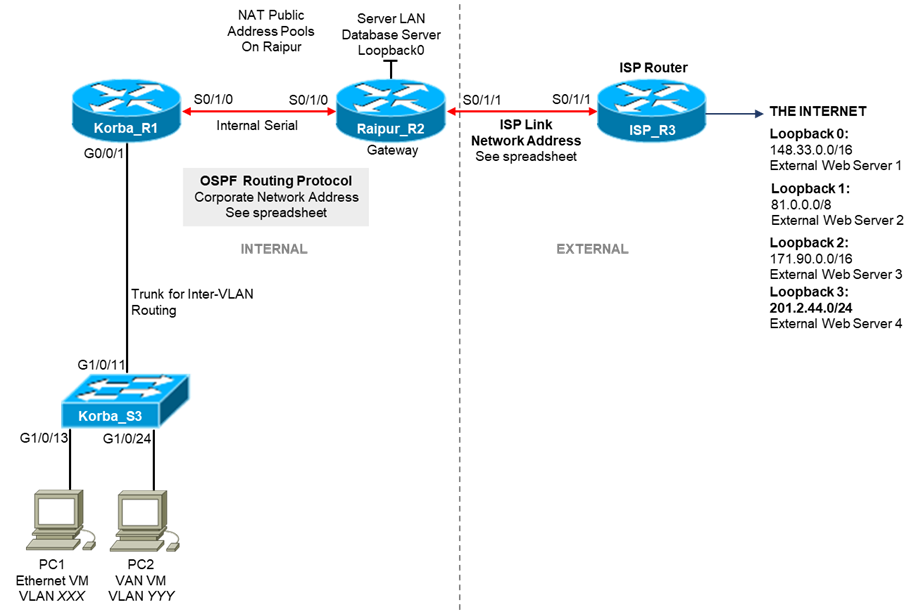
In this **Scenario** you will design and construct a network consisting of three routers and one switch, matching the hardware configuration of your Final Skills Assessment. You will consolidate the skills you acquired in building an internal network using a Routing Protocol connected to an external network via a public IP address coupled with ACLs to protect segments of your network. In this **Scenario** you will be repeating existing work in constructing a base network to later introduce new skills. **No new tasks** will be covered in **Scenario 5-P.**

**Methodology**

This portion of the handout contains the necessary information to design and build your network. Information on the assessment is at the end of the handout.

**Network Topology**

The Network topology is displayed in the figure below.



**Network Information**

The Network topology diagram refers to a number of network addresses and VLAN names. Please use the **provided spreadsheet on Canvas** to obtain your personalized network information for **Scenario 4**. The spreadsheet will provide:

* Corporate Network Address
* ISP Link Network Address
* **VLANXXX, VLANYYY,** and **VLANZZZ** VLAN Identification

**Subnetting**

The first task you must perform is to subnet your corporate network to create subnets for your VLANs. The subnetting requirements are:

|  |  |  |  |
| --- | --- | --- | --- |
| **Interface** | **Name** | **IP Address** | **Subnet Mask** |
| VLAN827 | Green | 28.0.0.1 | 255.255.248.0 |
| VLAN273 | Blue | 28.0.9.33 | 255.255.255.224 |
| VLAN195 | Grey | 28.0.8.1 | 255.255.255.0 |
| VLAN1 | Korba R1 | 28.0.9.65 | 255.255.255.240 |
| Internal Serial Link 1 | R1 S0/1/0 to R2 S0/1/0 | 28.0.9.81  28.0.9.82 | 255.255.255.252 |
| ISP Link 1 | R2 S0/1/1 | 201.45.33.1 | 255.255.255.252 |
| ISP Link 2 | R3 S0/1/1 | 201.45.33.2 | 255.255.255.252 |
| Database Server LAN | Loopback0 | 28.0.9.1 | 255.255.255.224 |
| Loopback0 | External Server 1 | 148.33.0.1 | 255.255.0.0 |
| Loopback1 | External Server 2 | 81.0.0.1 | 255.0.0.0 |
| Loopback2 | External Network | 171.90.0.1 | 255.255.0.0 |
| Loopback3 | External Network | 201.2.44.1 | 255.255.255.0 |
| PC1 | VLAN827 | 28.0.0.2 | 255.255.248.0 |
| PC2 | VLAN273 | 28.0.9.34 | 255.255.255.224 |
| Default Gateway | - | 28.0.9.65 | - |

**Basic Network Configuration**

You are essentially rebuilding the network from **Scenarios 4,** however there are fewer networking devices and subnets for you to construct. You will still be configuring the network using the **OSPF Routing Protocol.** Please refer to the previous Scenario Instructions, or more specifically your Lab Journal, if you need assistance in meeting the following requirements

* Check physical wiring on the devices
* Configure a MOTD and Hostnames on all devices
* Set the MOTD banned to include your student ID, name, and Lab time
* Configure the Switch with an enable password of **cisco,** the necessary VLANs, a management interface on VLAN1, a default gateway, and telnet access with password **cisco**
* Configure Switch ports G1/0/13 and G1/0/14 as access ports on VLANXXX with port security settings of (mac address sticky, max 4, violation protect), and port G1/0/24 as an access port on VLANYYY
* Configure all serial and loopback addresses on routers with interface descriptions
* Configure all routers connected to the switch with inter-VLAN routing using a trunk connection to the switch
* On the ISP router, configure only a static route to the Internal network

Before continuing, you should run all necessary tests to confirm that all the requirements listed above are properly configured.

**OSPF Requirements for Scenario**

For the purposes of the Scenario, you must configure OSPF on the internal routers as per the instructions below:

* Run OSPF on all internal corporate routers
* Configure the bandwidth for the point-to-point links between routers as:
  + **Raipur-Korba–** configure bandwidth 512
* Advertise all internal network addresses on all internal routers, advertising each subnet individually with an appropriate wildcard mask
* Advertise the default route installed on the gateway router – **Raipur**
* Disable broadcasting on internal edge-networks (all interfaces connected PCs) – all sub- interfaces of **g0/0/1 on Korba**

**ACL Requirements for Scenario**

The ACL security requirements for this Scenario are:

**Generic ACLs**

1. PCs in VLAN XXX **permitted** HTTP access to ISP Loopback 0 and deny ALL other access to this interface.
2. PCs in VLAN XXX **denied** PING requests to PCs in VLAN YYY
3. PCs in VLAN XXX **permitted** PING replies to PCs in VLAN YYY
4. PCs in VLAN XXX **permitted** ALL access to the Internet.
5. ALL access to the Internet – all the other Servers.
6. PCs in VLAN XXX **denied** PING access to PCs in VLAN XXX

**NOTE:** Requirements 2 and 3 above mean that PCs in VLAN YYY are able to ping PCs in VLAN XXX BUT that PCs in VLAN XXX CANNOT ping PCs in VLAN YYY.

**Telnet ACLs**

1. **ONLY** PCs in VLAN XXX **permitted** TELNET access to **Korba** Router
2. **ONLY** PCs in VLAN XXX **denied** TELNET access to **Raipur** Router

**Dynamic Host Configuration Protocol – DHCP**

New tasks in this Scenario include configuring the **Dynamic Host Configuration Protocol (DHCP)** to automatically assign network configuration to devices within the network. This releases ongoing work by system administrators as they no longer need to maintain network configuration on individual PCs, and network re-configuration is propagated via the DHCP server instead of having to reconfigure all end devices.

DHCP is a server that is attached to the network containing hosts to be auto-allocated network configuration. Very large networks will often have a dedicated server running DHCP for multiple subnets simultaneously. Small and medium sized networks can get away with running DHCP services on the router servicing individual subnets. In this case, as all the VLANs are attached to the Korba router, we will be running the DHCP server directly on the Korba router.

The main steps involved in running a DHCP server are:

1. Enabling DHCP on the router
2. Create a DHCP pool to service a particular subnet/VLAN
3. Allocate the IP address ranges and subnet masks for each pool
4. Configure the default gateway for devices within the subnet to use

**DHCP Configuration Information**

In order to enable the DHCP service on a Cisco router, you need to issue the command:

*service dhcp*

DHCP can be disabled using the command

*no service dhcp*

Once the service is activated, you need to create a series of DHCP pools for each subnet you wish to automatically allocate IP addresses to. A pool is defined as a set of IP addresses managed by the DHCP server. Each DHCP pool is identified by its name. You can create a DHCP pool using the command:

*ip dhcp pool <pool\_name>*

The example below will create a pool with the name VLANBlue

*ip dhcp pool VLANBlue*

You can create as many DHCP pools as you require, typically it will be one for each subnet. The pool name does not need to encompass the VLAN number/name, however it is good practice to use a name that matches the use of the subnet. A good example of a pool name would be *accounting or sales >* command to enable select interfaces. The pool information is configured within the pool sub- configuration option. If you leave the pool configuration menu, you need to re-enter the *ip dhcp pool <pool\_name>* command to modify the pool configuration.

Within the pool sub-configuration, you must at a minimum specify the subnet information and the default gateway address to use. The DHCP server will select an unused IP address from the range of IP addresses in the subnet and provide the selected IP address, the subnet mask, and the nominated default gateway address to allow the end PC to self-configure its network configuration.

To specify the subnet information for the pool, use the following command within the pool sub- configuration mode:

*network <network\_address> <subnet\_mask>*

As the router is aware of which subnets are connected to which interfaces, it will automatically assign this pool to the relevant interface. Take care that the netadd and submask must exactly match the network configuration on the router interface for the nominated subnet.

You also need to specify the default gateway to be provided to all PCs within the subnet. Use the following command within the pool sub-configuration mode:

*default-router <gateway\_ip\_address>*

While not used in this Unit, DHCP also provides for other automatic configuration options that can be attached to the pool. Two common options include the DNS server (using the *dns-server <ip address>* command), the the domain name (PCs will append the domain after their hostname to configure their full URL) (using the *domain-name* *<url>* command).

Finally, we will often wish to exclude IP addresses from the pool managed by DHCP. At the very least we will want to exclude the gateway address from being allocated to PCs. In the real world, a subset of available IP addresses are often reserved for static allocation to servers in the LAN. In this case, we also do not want these IP addresses being managed by DHCP. IP Addresses are excluded outside of the pool in the global configuration, each exclusion provides a range of addresses that will NOT be allocated by the DHCP server. The command to do so is:

*ip dhcp excluded-address <lowest\_ip\_address> <highest\_ip\_address>*

The example below will ensure that the DHCP server never allocates the IP addresses *192.168.0.1, 192.168.0.2 or 192.168.0.3* to any PCs via DHCP, likely because they belong to the gateway router OR to static allocations within the subnet:

*ip dhcp excluded-address 192.168.0.1 192.168.0.3*

**NOTE:** There is no need to exclude the network or broadcast address as they can never be allocated by the DHCP server.

**Troubleshooting DHCP Configuration**

One of the most common mistakes people make is that the PCs have been configured statically. You will need to modify the PCs to use DHCP to obtain an IP address. On first change, the PC will attempt to get an IP address from the DHCP server. This could fail if you have not properly configured your DHCP. If this occurs, the DHCP allocation may not occur and you will need to manually force it to occur later on.

Alternatively, you may have incorrectly configured DHCP and need to modify it. In this case, you will need to force the PC to release the current DHCP allocation and request a new one. If you do not do this, the PC will persist with an old IP configuration and you will not be sure why it is not working.

To force a Windows PC to release and renew its DHCP allocation, open a DOS cmd window and execute the following commands:

*ipconfig /release*

*ipconfig /renew*

Alternatively, you would like to check the DHCP allocations at the router running DHCP. The most useful commands are as below:

*show ip dhcp binding* – This command will list all the currently allocated IP addresses in the DHCP pools managed by this router. Each IP address will be listed along with the Ethernet MAC address of the PC with the allocated address, and the date the allocation was made

*show ip dhcp pool* – This command will list information about each pool configured on the router and the the current status of pool usage

**DHCP Requirements for Scenario**

For the purposes of the Scenario, you must:

* Run DHCP to provide IP addresses for all devices on VLANXXX and VLANYYY (two DHCP pools)
* The DHCP service should be run on Korba
* The DHCP pools should cover the range of IP addresses for those two VLANs
* You must exclude the first three IP addresses from being allocated by DHCP

**Network Address Translation – NAT**

New tasks in this Scenario include configuring Network Address Translation (NAT) to allow host inside a private network to share one (or more) public IP addresses to access the wider Internet. IPv4 addresses are a scarce resource, and smaller organisations are likely not to have enough to allocate a unique IP address to each host. Instead, they will use private IP addresses and a NAT to translate the addresses as packets exit and enter the Internal network.

A basic NAT will modify the source IP address of any packet leaving the internal network to one of the available public IP addresses allocated to the organization. In this way, a packet with a private source IP address will never be on the Internet. The NAT will store the mapping between the external and internal IP addresses such that when the return packet arrives at the NAT from the Internet (with a destination IP of the public IP address), the NAT can replace the destination IP with the internal (private) IP address, allowing the packet to make its way to the internal end host.

A more common form of NAT is more technically know as a PAT. In these cases, the NAT tracks not only the internal IP to public IP mapping, but also the internal port number to public port number mapping. This allows multiple TCP/UDP flows from different hosts inside the private network to share a single public IP address simultaneously. The NAT will translate the source IP address and source Port (for TCP/UDP) to one of the available public IP addresses and a currently unused public port number. The mapping from private IP:port to public IP:port will be managed within the NAT. When the return packet arrives from the Internet to a nominated public IP:port, the NAT will extract the internal IP:port from its database and replace the destination IP:port numbers in the packet, allowing it to reach the nominated application on the Internal network.

NAT is a very important tool that can allow networks to support more devices to access the Internet than their currently available pool of IP addresses.

The main steps involved in configuring NAT are:

1. Inform the gateway router of the available public IP addresses
2. Map which internal IP addresses are allowed to utilise which subset of public IP addresses
3. Inform the gateway router which interface forms the Internet (outside) of the NAT
4. Inform the gateway router which interfaces are participating on the internal (inside) side of the NATEnabling DHCP on the router
5. Create a DHCP pool to service a particular subnet/VLAN
6. Allocate the IP address ranges and subnet masks for each pool
7. Configure the default gateway for devices within the subnet to use

**NAT Configuration Information**

There are a number of components to perform in order to correctly configure NAT on a Cisco Device. The first step is to make sure that you are configuring NAT on your gateway device, the device where the public IP address is actually available.

While NAT can be configured to share a single IP address across all PCs, we are going to look at commands to share multiple public IP addresses amongst internal PCs.

The first step involves creating a pool of public IP addresses to use. If you wish to equally share all of your public IP addresses equally within your network, you will have to create a static pool. Alternatively, you can divide your public IP addresses into smaller subnets and allocate a range of IP addresses to different parts of your internal network. In this manner, you will guarantee that hosts in one part of your network will have a different public IP address range to hosts from another part. This can also be used to better share public IP resources.

In order to create a NAT pool of public IP addresses, we can use either of the following two commands

In order to enable the DHCP service on a Cisco router, you need to issue the command:

*ip nat pool <pool\_name> <first\_ip> <last\_ip> netmask <subnet\_mask>*

*ip nat pool <pool\_name> <first\_ip> <last\_ip> prefix-length <length>*

Assuming, you have been allocated the public IP network *200.57.64.33/29*, this means that the usable public IP addresses you own range from *200.57.64.33 to 200.57.64.39* with a subnet mask of *255.255.255.248*. You can create a single pool to cover this range using either of the following two commands:

*ip nat pool nat\_pool 200.57.64.33 200.57.64.39 netmask 255.255.255.248*

*ip nat pool nat\_pool 200.57.64.33 200.57.64.39 prefix-length 29*

Alternatively, you can create two equal sized pools to allocate to different subnets using:

*ip nat pool nat\_pool 200.57.64.33 200.57.64.35 prefix-length 30*

*ip nat pool nat\_pool 200.57.64.36 200.57.64.39 prefix-length 30*

The next step is to create a named ACL to nominate which range of internal IP addresses are allowed to access your NAT pool(s). You could use a simple ACL to allow internal hosts to access the entire Internet. An extended ACL can be used to limit which external hosts are accessible via the NAT. Below you will find the commands to create an extended ACL to allow all hosts in the range *192.168.1.0/24* to access the entire Internet.

*ip access-list extended natacl*

*permit ip 192.168.1.0 0.0.0.255 any*

Note that the ACL will match all addresses from *192.168.1.0/24* with any destination IP address.

**NOTE:** If you have multiple NAT pools, you should create an individual ACL for each NAT pool.

Once the Pools and ACLs have been created, we then need to attach each NAT pool with its allocated ACL. You can use either of the two commands below, they exhibit slight differences:

*ip nat inside source list <acl\_name> pool <nat\_pool\_name>*

*ip nat inside source list <acl\_name> pool <nat\_pool\_name> overloaded*

If you use the *overloaded* option, then the range of public IP addresses in the pool are shared with all internal IP addresses nominated in the ACL. If there are more internal addresses than public addresses, a single public address will be shared by multiple devices simultaneously. If overloaded is not specified, then at most one internal IP address will be allocated to each public IP address in the NAT pool. This will be reallocated as needed to allow all internal devices access to the Internet, but will limit the number of concurrent hosts that can access the Internet.

Finally, we need to tell NAT which interfaces on the router form the inside of the NAT (the internal private addresses) and which interfaces for the outside of the NAT (on the Internet). There will typically only be one external interface, there may be multiple internal interfaces. To configure an interface to participate in NAT, you will need to go that interface (or sub-interface) configuration and enter (ONLY) one of the following commands:

*ip nat inside*

*ip nat outside*

There are numerous other options where you can configure timeout values for the NAT database, ensuring that stale allocations are removed to free up network resources for other devices.

**Troubleshooting NAT Configuration**

Particularly when your Internal network is using public IP addresses AND you haven’t removed the static route you installed to map to all the corporate IP addresses, it may appear as thought your network is functioning when in fact it isn’t. You need to ensure that all traffic is being translated by the NAT. The two most useful commands that can provide information are:

*show ip nat translations* – This command will list all the current know internal traffic flows and show how they are mapped to the public NAT address pool

*show ip nat statistics* – This command will provide a more detailed overview of the current status of the NAT in the router, including the total NAT translations, and statistics about traffic mappings

It is likely that you will want to confirm that everything is functioning correctly. You can do this by initiating a flow and ensuring that it runs through the NAT. If you want to test again, you will need to remove the translation from the NAT to allow a new translation to be re-established. To clear a particular translation (found via *show ip nat translations*), you can use the command:

*clear ip nat translation <paramaeters>*

When using params, you will use the information provided by the output of *show ip nat translations.*

**NAT Requirements for Scenario**

For the purposes of the Scenario, you must:

* Use the NAT Public IP Address Pool provided by the ISP of 141.12.2.0/24
* Divide this pool into 3 sub-pools, do not use VLSM
* Allocate these three sub-pools to VLAN1, VLANXXX and VLANYYY
* Remove all static routes on the ISP Router that refer to the Corporate Network Address and replace it with a static route that maps only to the NAT Public IP Address Pool

You should verify this configuration by ensuring that when you access hosts on the Internet from the PCs in the corporate network, that appropriate entries show up when using the NAT troubleshooting commands.