TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 5
Distinction Task

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-D** expands your work to cover deployment of **NAT** between the Internal and External Network. For **Scenario 5-D**, you will extend the network you built in **Scenario 5-P** and **Scenario 5-C** to provide support for NAT. This knowledge will be consolidated in **Scenario 6-P**.

Purpose

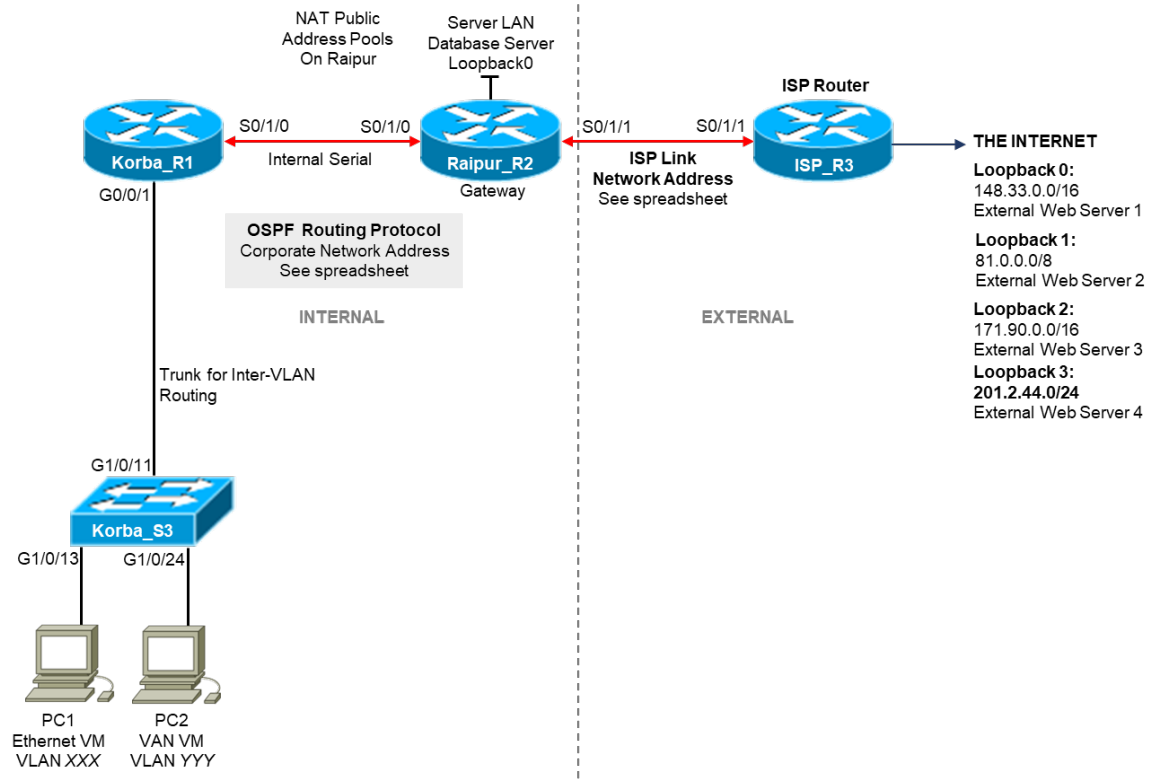
In this **Scenario** you will extend your work from the **Pass** and **Credit Task** by adding support for NAT between the Internal and External Network. In this Scenario you will be introduced to the **new skill** in the deployment of NAT on a gateway router. NAT is used to share a single public IP address with between devices inside the Corporate network. While large corporations typically own multiple IP addresses and do not require NAT, smaller companies and home users are typically allocated a single Internet IP address for their entire network and need to configure NAT to allow multiple devices simultaneous access to the Internet.

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 and is unchanged from **Scenario 5-P** and **Scenario 5-C**.



Network Information

As this is an extension of the **Pass** and **Credit Tasks**, you will not need to recalculate any network addresses of change the basic configuration of your network, you are extending the existing configuration only.

NOTE: Do NOT attempt the Distinction Task until you complete the Credit Task

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.

Assessment

The Scenario is assessed in class by your Lab Supervisor. When you have successfully configured and tested the Scenario, you will need to demonstrate functionality to your Supervisor. Upon successful demonstration, the Supervisor will ask you 1 or 2 questions about the Scenario in order to confirm that you completed the work and not another student. Upon successfully answering these questions, the Scenario will be marked as complete.

The due date for Scenario 5-D is at the start of the Lab in Week 10. As a distinction task, you are expected to complete this task on time unless you have a valid extension.

What Happens if I Fail

Failure in this task will result in the maximum possible Base Mark for your Portfolio being 36. Coupled with possible Bonus Marks, non completion will result in an absolute maximum Portfolio mark of 42/60.