TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 6
Pass 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 6** expands your work to cover deployment of **PPP** as a point-to-point protocol between the ISP and gateway routers. For **Scenario 6-P**, you will essentially repeat all of the work from **Scenario 5-P**, **Scenario 5-C** and **Scenario 5-D** to consolidate your knowledge in deployment of Interior Routing Protocols, ACLs, DHCP, and NAT before expanding on this in the **C** Task.

Purpose

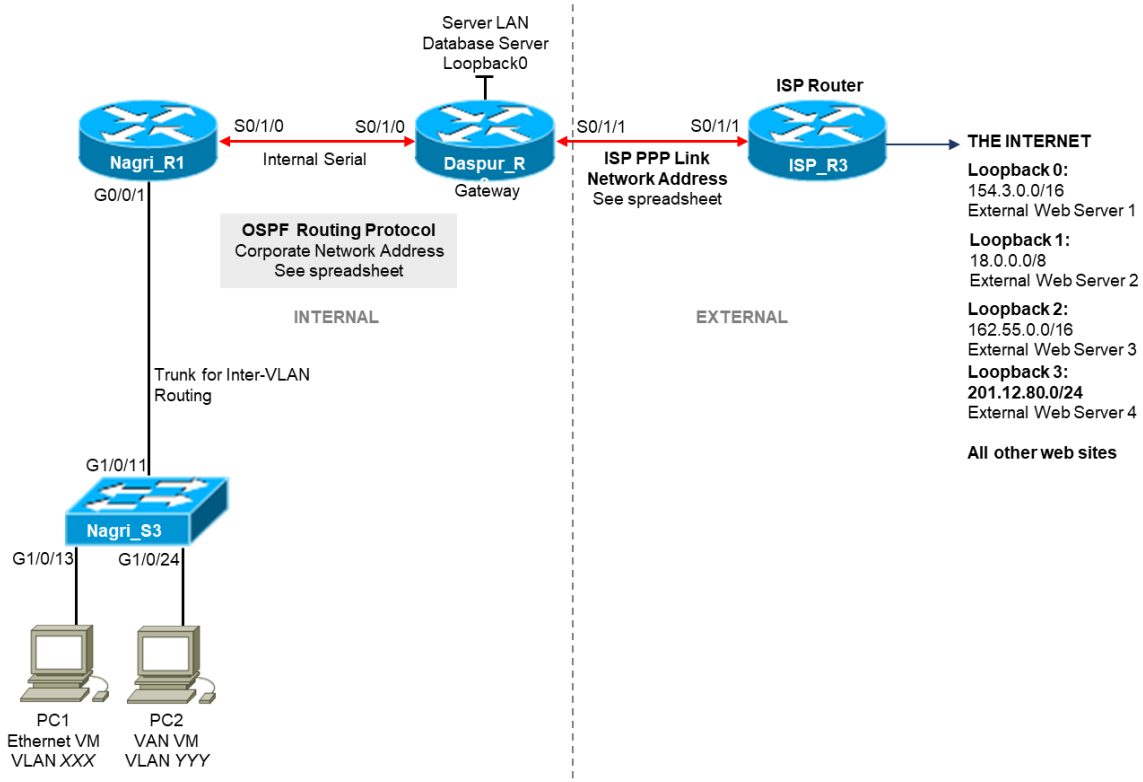
In this **Scenario** you will design and construct a network consisting of three routers and one switch, matching the hardware configuration of your Final Skills Assessment. You will consolidate the skills you acquired in building an internal network using a Routing Protocol connected to an external network via a public IP address coupled with ACLs to protect segments of your network, DHCP to automate configuration, and NAT to allow sharing of public IP addresses. 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 6-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 6**. 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:

Network	VLAN Name/Interface	Connected Switches	Host Count
VLANXXX	Dogs	Nagri	800 hosts
VLANYYY	Cats	Nagri	200 hosts
VLANZZZ	Birds	Nagri	120 hosts
VLAN1	-	Nagri	6 hosts
Internal Serial Links	-	-	2 hosts

Database Server LAN	Loopback 0	Daspur	20 hosts

Please have a copy of your working in case it is needed during assessment. You will need to document your assignment of IP addresses to Router Interfaces and PC Hosts

NOTE: You may use a subnetting Calculator to calculate the subnets but you should be able to do it more quickly without one

Basic Network Configuration

You are essentially rebuilding the network from **Scenarios 6-P/C/D**. 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 Public IP Address Range `135.12.64.0/25` 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:
  - **Daspur**-**Nagri**– configure bandwidth 256
- 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 – **Daspur**

- Disable broadcasting on internal edge-networks (all interfaces connected PCs) – all sub-interfaces of **g0/0/1** on **Nagri**

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 **Daspur** (not **Nagri** as per Scenario 5)
- The DHCP pools should cover the range of IP addresses for those two VLANs
- You must exclude the first four IP addresses from being allocated by DHCP

As we are moving the DHCP configuration from the **Nagri** router (as per Scenario 5) to the **Daspur** router. To make this function you will need to configure the DHCP helper IP address on **Nagri** using the xxxx command.

NAT Requirements for Scenario

For the purposes of the Scenario, you must:

- Use the NAT Public IP Address Pool provided by the ISP of 135.12.64.0/25
- Divide this pool into 3 sub-pools, do not use VLSM
- Allocate these three sub-pools to VLAN1, VLANXXX and VLANYYY
- When allocating the sub-pools, use NAT overloading

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.

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. PCs in VLAN YYY **denied** ALL access to the Database Server LAN
6. PCs in VLAN YYY **permitted** ALL access to the Internet

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 **Nagri** Router
2. **ONLY** PCs in VLAN XXX **denied** TELNET access to **Daspur** Router

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 6 is at the end of the Lab in Week 11. As a pass task, later completions are accepted, however tardiness will increase your workload later in semester so you should target completion by the due date.

NOTE: The final date for assessment of Scenario 6 is in Week 12. Failure to complete by Week 12 will result in failing this task

What Happens if I Fail

Failure in this task will result in you **failing** the Unit. You must successfully complete this task before the end of semester. **If you fail to complete this task you will ONLY be afforded an opportunity to complete if you successfully complete all other tasks required to pass the Unit.**