TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 1
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 1** is used to deploy a basic routing network using dynamic routing protocols, in this particular case **RIPv2**.

Purpose

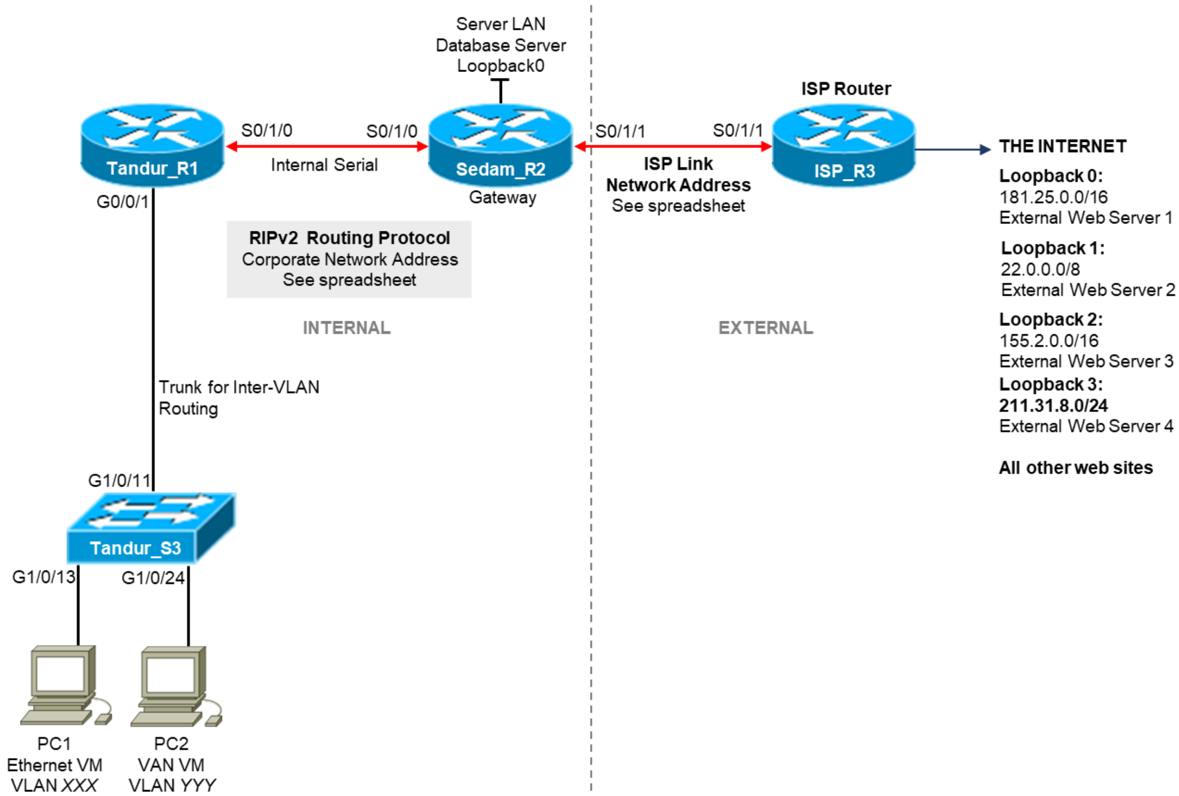
In this **Scenario** you will design and construct a network consisting of three routers and one switch using RIPv2. The skills attained in this Scenario will serve as a baseline for all remaining scenarios in this Portfolio.

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 1**. 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	Host Count
VLANXXX	French	600 hosts
VLANYYY	English	100 hosts
VLANZZZ	Hindi	50 hosts
VLAN1	-	18 hosts
Internal Serial Link	-	2 hosts

Database Server LAN	Loopback 0	40 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

First Level Configuration

Most of your configuration for this lab will be based on your skills attained from TNE10006/TNE60006 (Networks and Switching). You will start by essentially constructing a network with inter-VLAN routing and static IP address configuration only. As you now have more than one router in your network, you will also need to deploy routing tables across all the routers. This is the new material (using RIPv2) which will be explained later in the handout. Please refer to your older 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
- Disable the DNS service
- 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 port G1/0/24 as an access port on VLANYYY with port security settings consisting of a static mac address
- 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
- Configure a single static route on the ISP router to direct all traffic to the corporate network to **Sedam_R2**

Before continuing, you should run all necessary tests to confirm that the PCs have full connectivity between each other, and that all devices can communicate properly with other directly connected devices. Good practice should ensure you confirm that all networks are properly configured for direct communications before you work to interconnect them with a routing protocol. You should use your existing troubleshooting skills to verify this step.

Static Routes

In all our **Scenarios** – and in **standard Industry practice** – routing tables for subnets within a set of centrally managed routers (ISP, corporation, etc) are generally fully managed by **Routing Protocols**. In this case, always an **Interior Routing Protocol** of the type you will be learning about in this Unit. For the

Internet Core, routing tables to reach other major networks are also managed by Routing Protocols, however the routing protocol used is an **Exterior Routing Protocol** (**BGP** – Border Gateway Protocol) which is beyond the scope of this Unit

Despite this, we often remain with a special case where corporate networks, particularly smaller ones will not participate in BGP and therefore need an alternate configuration to connect to the Internet. Similarly, ISPs need to manage a way to route traffic from the wider Internet to private corporate networks. In these cases, we typically make use of static routes installed on the two edge routers that connect these networks together. A static route is a manually entered route (not automated via a Routing Protocol).

The corporate network will typically install a **Static Default Route** on its **gateway router** directing all traffic to the ISP. The Static Default Route is then **advertised** within the corporate such that all internal routers **are able** to reach the wider Internet.

The ISP will typically install a **Static Route** on its **edge router** directing all traffic for the corporate network to the company gateway router. The Static Route is then **advertised** within the ISP such that all external traffic routers is **properly routed** to the corporate network.

In this Scenario, **Sedam_R2** serves as the gateway router connected to the ISP. We need to install a static default route on this device with a destination IP address of the ISP edge router. The static default route is equivalent to the default route installed on end PCs where you specify the IP address of the router on your subnet.

To enter a default router on Cisco device, enter the command:

```
ip route <dest_network_address> <dest_subnet_mask> <gateway_address>
```

or:

```
ip route <dest_network_address> <dest_subnet_mask> <exit_interface>
```

Like when configuring the default route on a PC, the `<gateway_address>` is the IP address of the router you wish to direct packets to. For option 2, `<exit_interface>` is the interface on the local route to send packets out of. The preferred approach and Standard Industry Practice is to use Option 1 (`<gateway_address>`).

When entering the Default Static Route on **Sedam_R2**, the destination network is `0.0.0.0/0` . This network address and subnet mask pair refer to all IPv4 addresses on the Internet. As more specific routers are always preferred, this implies that the Static Default Route is only used for packets that do not match any other destinations. Within a corporate network, this means all packets with destinations in the wider Internet. When programming the `<gateway_address>`, we use the IP address installed on **s0/1/1** on the **ISP Router**.

We also need to install a Static Route on the ISP router directing external traffic to the Corporate network. In this case, the network address and subnet mask pair refer to the un-subnetted Corporare

Network Address, and the `<gateway_address>` refers to the IP address installed on **s0/1/1** on **Sedam_R2**.

Routing Protocol – RIPv2

New tasks in this Scenario include configuring a Dynamic Routing Protocol. Routing Protocols run on all routers and communicate with each other via a dedicated protocol to exchange information about network state. Using this information, they determine the best paths to remote networks, and dynamically update the routing tables so that all networks are reachable. In this Unit we concentrate on Interior Routing Protocols – Protocols that run only within a corporate network and populate routing tables to allow subnets within a corporate network to reach each other. Interior Routing Protocols do NOT run within the Internet Core, nor across multiple interior networks. The primary benefit of Routing Protocols is their ability to self-heal. When a network connection fails – whether due to failed router or broken cable – the routing protocol will detect the broken links, forward new information to all other routers in the network, and recalculate the Routing Tables. As such, the network will automatically select alternate paths to ensure that network connectivity is maintained.

For this Scenario we will be deploying RIPv2. RIP is an older routing protocol that is not used in practice, however is excellent as a first pass as it is easier to understand, and easier to debug when things are not working as expected. The processes you use to configure RIPv2 will reflect across to more modern protocols in later Scenarios.

The main steps involved in running a Routing Protocol are:

1. Enabling the routing protocol
2. Configuring the routing protocol on the router which interfaces and/or networks should be advertised to other routers in the corporate network
3. Validating that the Routing Protocol is properly configured

RIPv2 Configuration Information

In order to enable the RIPv2 routing protocol on a Cisco router, you need to issue the command:

```
router rip
```

RIP can be disabled using the command

```
no router rip
```

To add extra configuration to RIP, you need to re-enter the `router rip` command to enter RIP configuration mode.

You can specify which version of RIP to use with the version command. Only RIPv2 supports VLSM subnetting, you will need to use the following command

```
version 2
```

On each router, you need to specify which interfaces you wish the routing protocol to advertise to other routers in the network. All specified interfaces will have their network location information broadcast to other routers running the same routing protocol. The routing protocol will use this information to automatically populate the routing tables.

For RIP, you specify which interfaces to include in the routing protocol using the network command as per below

```
network <network_address>
```

In this command, `<network_address>` must be an unsubnetted class A/B/C network address. RIP will find all subnets within `<network_address>`, which interfaces those subnets are connected to, and then broadcast those subnets to other routers. As an example, the command

```
network 165.63.0.0
```

Will find all subnets of `165.63.0.0/16` on the router, and send that information to other routers

Occasionally you will have interfaces that contain networks that you wish to advertise to other routers, but you will not need – or want – to send broadcast messages on. These are typically edge networks where there are only end-devices – and not other routers – connected to. In this case, RIP will normally continuously send routing broadcast information to these interfaces. This consumes unnecessary traffic on this internal network. As such, while we are still required to advertise this interface (because other routers need to learn about the network) we will want to disable sending of advertisements on these interfaces. This is done using the following command within the RIP configuration.

```
passive-interface <iface_name>
```

For examples, the command `passive-interface g0/0/1` will disable sending updates out this interface. Note that it is possible to disable broadcasts (using the `passive-interface` command) on sub-interfaces as well.

Gateway routers within organisations will typically have a default route pointing to the ISP router. This will route all traffic to subnets which are not known to the ISP. For the entire corporate network to function, all routers need a default gateway programmed to redirect traffic to the gateway router. Just as with internal networks, we don't want to program this manually, as broken connection can cause the default route to fail. We need to use the routing protocol (in this case RIP) to broadcast the default route. This can be done issuing the following command on the router with the static default route programmed

```
default-information originate
```

Useful debugging commands include

`show ip rip database` – Prints information on the internal RIP tables used to calculate routes `show ip rip neighbours` – Prints information about directly connected routers running RIP. This can be useful to determine why routes are not showing as the neighbour is not visible

RIPv2 Requirements for Scenario

For the purposes of the Scenario, you must:

- Run RIPv2 on all internal corporate routers – **Tandur_R1** and **Sedam_R2**
- Advertise all internal network addresses on all internal routers
- Advertise the default route installed on the gateway router – **Sedam_R2**
- Disable broadcasting on internal edge-networks (all interfaces connected PCs) – all sub-interfaces of **g0/0/1** on **Tandur_R1**

Testing and Evaluation

Once everything is complete, all PCs, switches, and routers should be able to successfully ping all other devices in the network and in the ISP. This should be implemented where the only statically installed routes are the static routes on the ISP router and the default route on the gateway router. All other entries in the routing tables should be automatically entered via RIPv2, or exist because the network is directly connected.

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 1 is at the start of the Lab in Week 3. 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 1 is in Week 7. Failure to complete by Week 7 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 Week 7. **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.**