# TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 3
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 3** builds upon the dynamically routed network you constructed in **Scenarios 1 and 2** and introduces you to a newer – and more actively used – dynamic routing protocol called **Enhanced Interior Gateway Routing Protocol** (EIGRP).

## Purpose

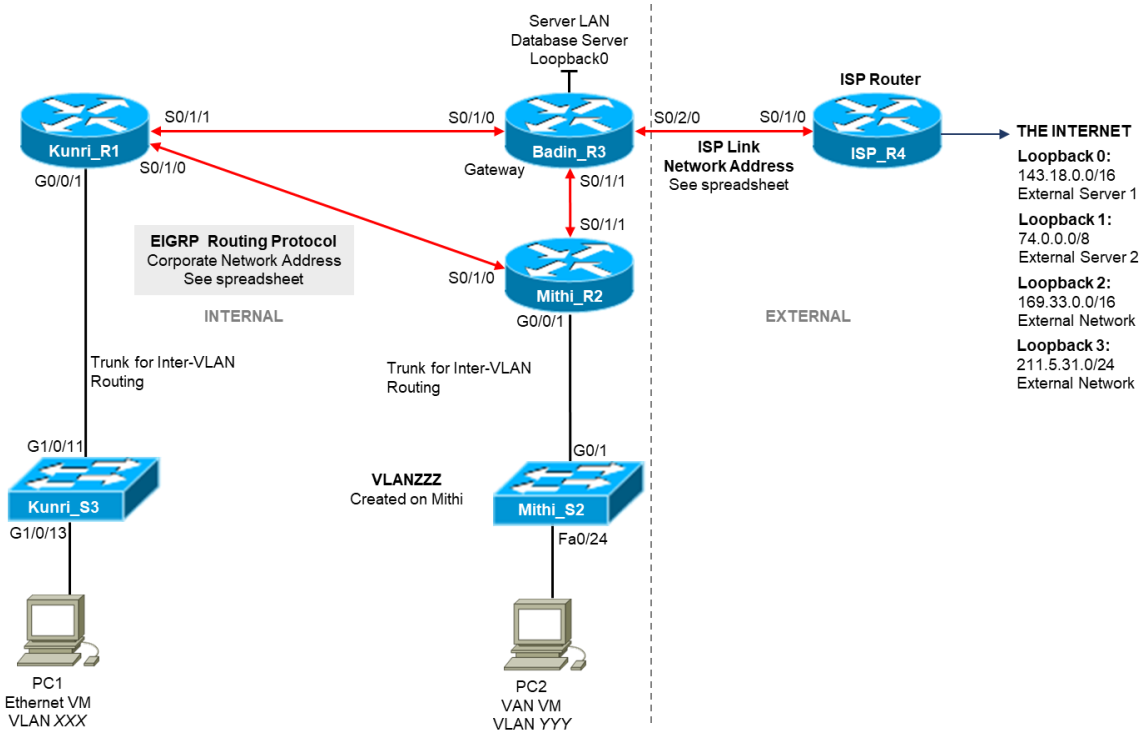
In this **Scenario** you will design and construct a network consisting of four routers and two switches. You will reinforce the skills you acquired in building an internal network using a Routing Protocol connected to an external network via a public IP address coupled with ACLs to protect segments of your network. In this Scenario you will be introduced to the **new skill** in the design and deployment of networks running the **Enhanced Interior Gateway Routing Protocol** (EIGRP)as your routing protocol.

## 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 3**. 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** | Peas | Kunri | 500 hosts |
| **VLANYYY** | Flour | Mithi | 200 hosts |
| **VLANZZZ** | Rice | Mithi | 50 hosts |
| **VLAN1** | - | Kunri and Mithi | 20 hosts on Kunri and 6 hosts on Mithi |
| **Internal Serial Links** | - | - | 3x 2 hosts |
| **Database Server LAN** | Loopback 0 | Badin | 18 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 Scenario 2 except for the routing protocol configuration. In this section will be a brief list of all requirements except for the routing protocol and ACLs. ACLs are configured after the network routing tables are established. 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.

## Routing Protocol – EIGRP

New tasks in this Scenario include configuring the EIGRP Dynamic Routing Protocol instead of RIPv2. For the most part, configuring EIGRP is very similar to configuring RIPv2. EIGRP needs to be configured on all internal corporate routers so that routing tables can be updated to self heal.

For this Scenario we will be deploying EIGRP. EIGRP is a more modern routing protocol that is occasionally used. While effective, it is only licensed on Cisco devices and therefore cannot be used unless all networking equipment within the corporate network is Cisco branded. Compared to RIPv2, EIGRP does a better job in determining routes, converges faster, and can immediately add an alternate route when a link breaks rather than waiting for a recalculation.

The main steps involved in running a EIGRP are basically the same as for RIPv2:

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

## EIGRP Configuration Information

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

```
router eigrp <as_number>
```

In this case, `<as_number>` refers to the EIGRP Autonomous System Number. Your router can participate in multiple EIGRP networks simultaneously. Each EIGRP network is identified by an Autonomous System number, note that the Autonomous System number is purely an internal parameter used by the EIGRP programs running on each router, it does not need to match the actual Autonomous System number owned by the corporation to participate in BGP (Core Internet) routing.

When configuring EIGRP for the internal network, any Autonomous System number can be used, but the value for `<as_number>` must be the same for all routers in the internal network. If not Autonomous System number is allocated in the network design, it is good practice to default to an Autonomous System number of 1.

EIGRP can be disabled using the command

```
no router eigrp <as_number>
```

To add extra configuration to EIGRP, you need to re-enter the `router eigrp <as_number>` command.

Specifying which interfaces you wish the EIGRP protocol to advertise to other routers is similar to RIP, except that there is an extra parameter called the wildcard mask.

```
network <network_address> <wildcard_mask>
```

Unlike RIPv2, using EIGRP we can – and should – specify actual subnets and not the parent classful network. The subnet is specified with `<wildcard_mask>`. To determine the value of `<wildcard_mask>`, you need to invert the subnet mask (swap all 1 bits to 0 and all 0 bits to 1). Further flexibility using the `<wildcard_mask>` is that we can use a single wildcard mask to effectively supernet the interface addresses and use a single command to advertise multiple interfaces.

The primary advantage of using a `<wildcard_mask>` is that the administrator can deliberately exclude some subnets from the routing protocol

The example below will advertise the subnet 186.64.32.0/22

```
network 186.64.32.0 0.0.3.255
```

As with RIPv2, we will want to have some interfaces configured as passive, the command to do so – `passive-interface <iface_name>` – is exactly the same as for RIPv2. EIGRP has the ability to set whether all interfaces on the router should be configured as passive by default. If you wish to do this you can use the command below, and then use the `no passive-interface <iface_name>` command to enable select interfaces.

```
passive-interface default
```

The command to advertise static routes in EIGRP is different than for RIPv2. To advertise static routes – for example the default route – to other routers via EIGRP, use the command below:

```
redistribute static
```

EIGRP uses the configured bandwith of a link to determine which links are more likely to be chosen when selecting the optimal path through the network. The configured link bandwidth differs from the actual bandwidth and changing this value does NOT reduce or increase the speed of traffic through the link. By default, EIGRP will use the actual link speed for calculations but this can be changed.

Useful debugging commands include

`show ip eigrp neighbours` – Prints information about directly connected routers running EIGRP. This can be useful to determine why routes are not showing as the neighbour is not visible. If this reports that an adjancency is not formed, it is likely that the interfaces on either side of the link do not have matching subnet masks

`show ip eigrp topology` – Prints information about currently selected and backup paths. Can be useful to determine if you have correctly configured the bandwidth link speeds

## EIGRP Requirements for Scenario

For the purposes of the Scenario, you must:

- Run EIGRP on all internal corporate routers with autonomous system number 65 – **Kunri**, **Mithi,** and **Badin**
- Configure the bandwidth for the point-to-point links between routers as:
  - **Badin**-**Mithi** – configure bandwidth 512
  - **Badin**-**Kunri** – configure bandwidth 64
  - **Kunri**-**Mithi** – configure bandwidth 128
- 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 – **Badin**
- Disable broadcasting on internal edge-networks (all interfaces connected PCs) – all sub-interfaces of **g0/0/1** on **Kunri** and **Mithi**

## 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 **permitted** ALL access to the Internet – all the other Servers.

Telnet ACLs

1. **ONLY** PCs in VLAN XXX **permitted** TELNET access to **Kunri** Router
2. **ONLY** PCs in VLAN XXX **denied** TELNET access to **Badin** Router

## Access Control Lists for Telnet Access

Refer to **Scenario 2** for earlier comments about generation of ACLs on Cisco devices. New to this task is the usage of ACLs to restrict telnet access to the router. ACLs are typically used on interfaces, either on traffic arriving or being queued to transmit, all relevant packets are matched against the rules in turn until it matches a rule. Once a rule is matched that action is taken and the packet is either discarded or it is allowed and is transmitted on to the next path.

To restrict telnet access, we are instead using the ACL to restrict access to a single application, in this case the telnet application. All remote access to routers and or switches via telnet or ssh occur via the `vty` configuration. `vty` is a virtual terminal which acts as a virtual console plugged into a virtual port on the device. When you telnet or ssh to a router or switch, the network connection is connected to the virtual terminal. As such, when you attach an ACL to the `vty` configuration, it acts on all packets arriving or leaving the virtual terminal, and hence can allow or restrict access to telnet or ssh.

Typically the ACL is applied in the `in` direction, to stop selected remote devices from accessing the telnet/ssh connection. In this case the ACL is always a standard ACL (works with source host addresses only, no destination hosts or protocol information). You would typically finish the ACL with either permit any (allow all non-denied hosts to connect via telnet/ssh) or deny any (deny all non-permitted hosts to connect via telnet/ssh)

A simple example of an ACL to restrict access to a subset of hosts is listed below

```
ip access list standard telnet_restrict
permit host 1.2.3.4
permit 200.56.73.128 0.0.0.127
deny all
```

This ACL will allow telnet access from the computer with IP address `1.2.3.4`, and from all hosts in the `200.56.73.128/25` subnet. All other hosts will be restricted.

It is still necessary to install the ACL

match against web traffic, you can either use:

```
line vty 0 4
password <telnet_password>
login
access-class telnet_restrict in
```

The first command will configure all 5 available `vty` interfaces on the router (interfaces 0-5). It will then enable telnet access (`login`) and set a password (`<telnet_password>`). Telnet will only function if a password is also set. Finally we install the ACL

## 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 3 is at the start of the Lab in Week 6. 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 3 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.**