TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 2
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 2** builds upon the basic routing network you constructed in **Scenario 1** and adds security requirements in the form of **Access Control Lists** (ACLs).

Purpose

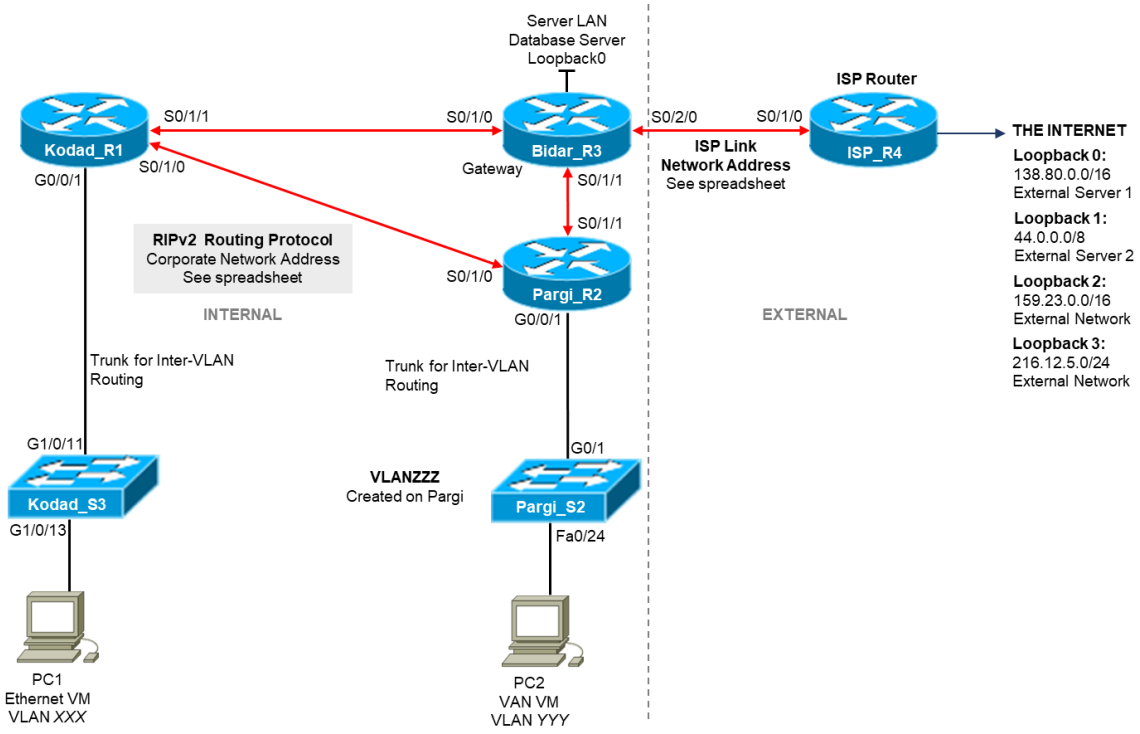
In this **Scenario** you will design and construct a network consisting of four routers and one switch. You will reinforce the skills you acquired in building an internal network using a Routing Protocol connected to an external network via a public IP address. You will then add a **new skill** in the design and deployment of **Access Control Lists** to protect segments of your internal network.

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 2**. 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	Eggs	Kodad	1,200 hosts
VLANYYY	Milk	Pargi	100 hosts
VLANZZZ	Bread	Pargi	50 hosts
VLAN1	-	Kodad and Pargi	18 hosts on Kodad and 18 hosts on Pargi
Internal Serial Links	-	-	3x 2 hosts

Database Server LAN	Loopback 0	Bidar	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

First Level Configuration

You are essentially rebuilding the network from Scenario 1 with an extra internal router and switch. This network also has alternate subnetting and IP address information. 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 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 RIPv2 between the three internal routers, with passive interfaces where appropriate. Do NOT advertise external IP subnets, instead use a default route on the gateway router and advertise the default route~~
- ~~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.

Access Control List Requirements

New tasks in this Scenario include configuring Access Control Lists (ACLs) to protect parts of your network. In essence, you will be designing and implementing ACLs for VLANXXX to implement:

- PCs in VLANXXX **denied HTTP** access to ISP **Loopback0** and permit **ALL** other access to **Loopback0** and the Internet
- PCs in VLANXXX **permitted only HTTP** access to ISP **Loopback1** and deny **ALL** other access to **Loopback1**
- PCs in VLANXXX **denied all** access to ISP **Loopback2**

- PCs in VLANXXX **permitted ALL** access to the rest of The Internet.

Access Control List Implementation

The simplest approach is to design and write your ACLs using Notepad, then to paste them into the routers as required for implementation. Design needs to be performed by identifying each individual requirement, and then to configure a single (or multiple) ACL rules to meet each requirement. You will need to carefully consider the order of your ACL rules as once a rule is matched, no further processing of rules will occur, the packet will either be permitted or dropped. As such, rule are generally written in order from most specific to least specific.

Typically, the last rule in an ACL will be to either permit all remaining traffic, or deny all remaining traffic. For this scenario stopping certain internal PCs from accessing external sites, the typical best-practice approach is to write specific rules to deny packets, and then finish with a single rule to permit all remaining traffic

Within a router, the instruction to create a NAMED ACLis:

```
ip access list extended <name>
```

For the purposes of this lab, you should use something like

```
ip access list extended ACLVLANXXX
```

You can delete an existing names ACL using:

```
no ip access list extended <name>
```

Individual rules within an ACL are written in the form:

```
deny|permit <protocol> <src> <dst> <port>
```

`deny` means packets matching the rule will be immediately discarded, `permit` results in matching packets being immediately forwarded. `<protocol>` can be `ip` for all IP packets, `tcp` for only TCP packets, or udp for only UDP packets.

Both `<src>` and `<dst>` can be written either as:

`<subnet address> <wildcard>` - to match a range of IP addresses

`host <ip address>` - to match a single IP address

any – to match all IP addresses (note that depending on where the rule is place and what direction, any can either mean the entire Internet, or all IP addresses within the subnet on an interface.

There are a range of options for `<port>`, but in most cases you will want to match against a specific port number. If the port number is well known, you can use either the port number of protocol name. For example to match against web traffic, you can either use:

```
eq 80

eq www
```

In order to complete the ACL requirements for this Scenario, a template will be posted below of the required rule structure. You will need to determine the relevant parameters to properly form the rules. This template should be entered into Notepad and then pasted into the Router for testing. Lines in the template in italic font are used to help explain the purpose of the ACL rule and are not to be included in your Notepad file for pasting

Delete the named ACL if it already exists
`no ip access-list extended ACLVLANXXX`
Recreate the named ACL
`ip access-list extended ACLVLANXXX`
Deny all PCs in VLANXXX HTTP access to ISP Loopback0 – you should use the subnet/wildcard form to specify the source and the host/address form to specify the destination. Permitting access will be done later
`deny tcp <source> <destination> eq www`
Permit all PCs in VLANXXX HTTP access to ISP Loopback1
`permit tcp <source> <destination> eq www`
Deny all other access to ISP Loopback1
`deny ip <source> <destination>`
Deny all PCs in VLANXXX access to ISP Loopback2 – note no port information specified for IP protocol match
`deny ip <source> <destination>`
Permit all other packets, this includes permitting all other access to ISP Loopback0 from the first requirement
`permit ip any any`

Note that these commands only create the ACL, we now need to install it on an interface on the router. To install the ACL, you need to enter the configuration for the relevant interface or sub-interface, and enter the command:

```
ip access-group <acl name> <direction>
```

Where `<acl name>` is the name of your ACL (eg. ACLVLANXXX) and `<direction>` is either `in` or `out` where:

`in` – All packets arriving at this interface will be matched against the ACL and either discarded or forwarded

`out` – All packets that have been queued to this interface after being routed will be matched against the ACL and either discarded or transmitted

In the case of restricting access to users of PCs in a portion of your network, you will typically match on `in`, capturing packets as they leave the subnet. In the case of restricting access to your network for external users, you will often match on `out`, capturing and discarding packets as they are about to be delivered to the final destination.

Other important things to understand about deploying ACL rules are:

Displaying all ACLs on the router

```
show access-lists
```

ACLs can count how many packets match each rule, you can reset these counts using

```
clear access-list counters
```

You can test your rules by clearing the count, then running the test traffic, and finally issuing the `show access-lists` command. The count will be increased for the rule that matched that packet. This way if the test is failing, you can which rule the packet is being matched against

Other things to remember:

1. Be aware that ACL names are case sensitive, as such the ACL names ACLVLANXXX is different to the ACL named AclVLanXXX
2. Bad rule order is often a cause of problems. You may want a packet to match a specific rule, but it instead matches an earlier rule resulting in incorrect handling of packets
3. Standard ACLs should typically be places as close to the destination network as possible, this is to ensure that you don't accidentally block traffic to unintended destinations
4. Extended ACLs should typically be placed as close to the source network as possible, this is to ensure traffic is dropped early and not create unnecessary congestion

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 2 is at the start of the Lab in Week 5. 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 2 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.**