TNE20002/TNE70003 - Network Routing Principles

Portfolio Task – Scenario 6
Credit 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-C** expands your work to cover deployment of **PPP** as a point-to-point protocol between the ISP and gateway routers. For **Scenario 6-C**, you will extend the network you built in **Scenario 6-P** to provide support for PPP and CHAP.

Purpose

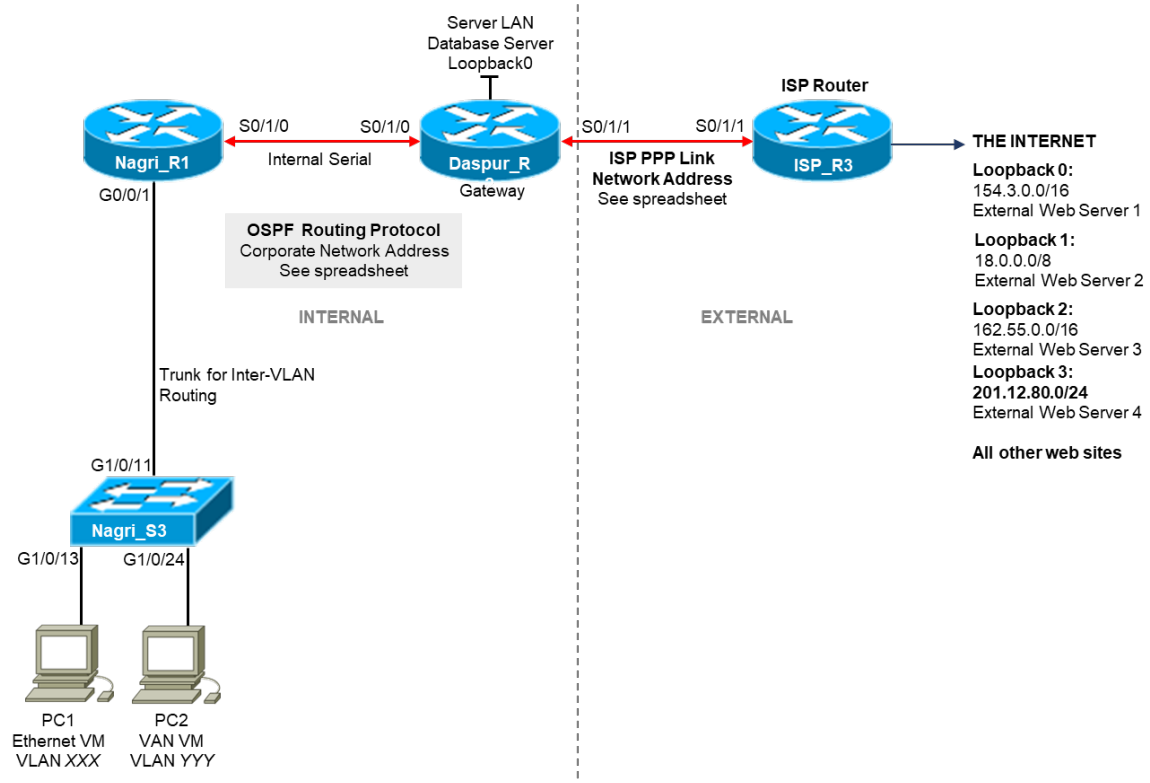
In this **Scenario** you will extend your work from the **Pass Task** by adding support for **PPP** and **CHAP** to manage the serial connection between your gateway router and the ISP. In this Scenario you will be introduced to the **new skill** in the deployment of **PPP** and **CHAP**.

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 6-P**.



Network Information

As this is an extension of the **Pass Task**, 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 Credit Task until you complete the Pass Task

Point-to-Point Protocol – PPP

New tasks in this Scenario include configuring the **Point-to-Point Protocol (DHCP)** and the **Challenge-Handshake Authentication Protocol (CHAP)** to manage the serial link between the gateway and ISP router. **PPP** is a simple encapsulation protocol to manage direct point-to-point links and encapsulate IP packets over that link. It can be used to allow IP connections over technologies where IP is not directly supported.

PPP is also commonly used where IP is directly supported such as between the ISP and their customer networks as it allows a simpler mechanism to track network utilization and also to apply network management rules. PPP also supports extensions to allow user authentication to protect access to known subscribers.

The PPP protocol itself is rather simple and consists of two primary components:

1. A Link Control Protocol (LCP) which establishes the PPP link and ensures that both sides are properly synced
2. A Packet Encapsulation Protocol to actually encapsulate IP packets to send over the Point-to-Point link

Some implementations contain other protocols to help manage the link while running.

You can see PPP running over your Home Internet connection, usually in combination with some form of authentication protocol. PPP with authentication will manage your sign-in to your ISP with your username/password, and then data will be transferred over the PPP link. If your current Internet connection is Fibre-to-the-Home, you will be using a variant of PPP called PPPoE (PPP over Ethernet) where the PPP packets are directly encapsulated within an Ethernet Frame. In this case, your IP packets are encapsulated within a PPP Packet which is directly carried over Ethernet.

If you are connected via an xDSL or DOCSIS (Cable Modem) connection, then your ISP may choose to use PPPoE or PPPoA (PPP over ATM). ATM is the underlying protocol that runs between your xDSL/DOCSIS modem and the ISP. PPPoA will carry the PPP encapsulated IP packets directly within an ATM AAL5 datagram which is ultimately broken into ATM Cells. Alternatively, the ISP may choose to run PPPoE to simplify their configuration at the ISP Gateway. In this case, your IP packets will be encapsulated within PPP which is encapsulated inside an Ethernet Frame. The Ethernet Frame is then encapsulated over the ATM AAL5 infrastructure for transmission as ATM cells. This simplicity in the backend comes at the cost of increased overhead in carrying an extra Ethernet header for all IP packets.

To configure PPP without authentication on a Cisco device, PPP encapsulation needs to be enabled at both ends of the link.

PPP Configuration Information

PPP is enabled and disabled directly on the Serial Interface sub-configuration by using the command:

```
encapsulation ppp
```

And can be disabled using the command

```
no encapsulation ppp
```

Once the service is activated, you need to confirm that it is properly running by using the `show interface` command on the Serial Interface to confirm operation. You can also enable PPP debugging using:

```
debug ppp negotiation
```

```
debug ppp packet
```

Challenge-Handshake Authentication Protocol – CHAP

The **Challenge-Handshake Authentication Protocol (CHAP)** is used to provide some essence of security in using a PPP connection by adding username and password components to the **PPP LCP** communications to establish the PPP connection. Note that CHAP is not a secure protocol in that it protects communications to the ISP, nor does it encrypt the password during authentication. However given that the link is often a direct Point-to-Point link that can only be observed by the ISP, this security is typically deemed acceptable for most scenarios.

CHAP only manages the authentication portion of the PPP connection. In order to configure CHAP on a Cisco Router, you need to perform the following steps:

1. Create a username/password combination in the Router user database
2. Configure PPP on the Serial Point-to-Point link to use CHAP

CHAP Configuration Information

To create a username and associated password in the Cisco User database, use the following command where `<username>` is the **configured device name of the Router on the other side** of the Point-to-Point link:

```
username <username> password <password>
```

For example, to create a CHAP user for the **Daspur** Router to connect to the **Nagri** Router with the password **mychappassword**, you would use the command:

```
username Nagri password mychappassword
```

NOTE: Ensure you do not include any extra spaces at the beginning or end of the password.

NOTE: While the `<username>` will be different on both Routers (set to the alternate devices name), the password MUST be the same for both devices.

Once you have created the CHAP user account, you now need to configure the Serial Interface at each side of the link to use CHAP. This is enabled directly on the Serial Interface sub-configuration by using the command:

```
ppp authentication chap
```

Once CHAP is activated, you need to confirm that it is properly running by using the `show interface` command on the Serial Interface to confirm operation. You can also enable CHAP debugging using:

```
debug ppp authentication
```

PPP and CHAP Requirements for Scenario

For the purposes of the Scenario, you must:

- Run PPP with CHAP to manage the Serial Point-to-Point Link between the **Nagri** and **Daspur** routers
- Configure CHAP using the password **cisco**

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-C is at the end of the Lab in Week 11. As a credit 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 30. Coupled with possible Bonus Marks, non completion will result in an absolute maximum Portfolio mark of 36/60.