**Portfolio Task – Scenario 6**

**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**

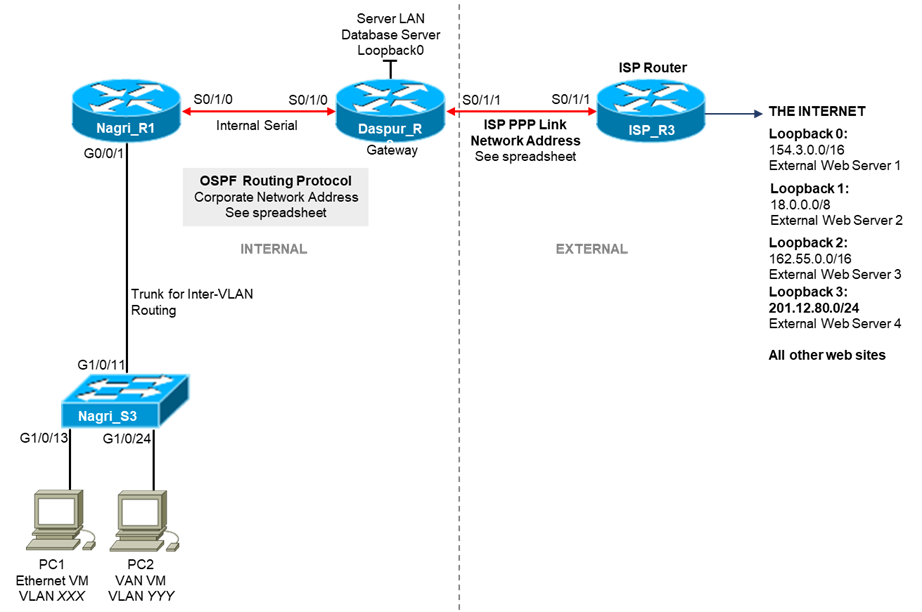
In this **Scenario** you will design and construct a network consisting of three routers and one switch, matching the hardware configuration of your Final Skills Assessment. You will consolidate the skills you acquired in building an internal network using a Routing Protocol connected to an external 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 4**. 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:

|  |  |  |  |
| --- | --- | --- | --- |
| **Interface** | **Name** | **IP Address** | **Subnet Mask** |
| VLAN827 | Dogs | 28.0.0.1 | 255.255.252.0 |
| VLAN273 | Cats | 28.0.4.1 | 255.255.255.0 |
| VLAN516 | Birds | 28.0.5.1 | 255.255.255.128 |
| VLAN1 | - | 28.0.5.161 | 255.255.255.248 |
| Internal Serial Link 1 | R1 S0/1/0 to R2 S0/1/0 | 28.0.5.169  28.0.5.170 | 255.255.255.252 |
| ISP Link 1 | R2 S0/1/1 | 191.22.43.1 | 255.255.255.252 |
| ISP Link 2 | R3 S0/1/1 | 191.22.43.2 | 255.255.255.252 |
| Database Server LAN | Loopback0 | 28.0.5.129 | 255.255.255.224 |
| Loopback0 | External Server 1 | 154.3.0.1 | 255.255.0.0 |
| Loopback1 | External Server 2 | 18.0.0.1 | 255.0.0.0 |
| Loopback2 | External Network | 162.55.0.1 | 255.255.0.0 |
| Loopback3 | External Network | 201.12.80.1 | 255.255.255.0 |
| PC1 | VLAN827 | 28.0.0.2 | 255.255.252.0 |
| PC2 | VLAN273 | 28.0.4.2 | 255.255.255.0 |
| Default Gateway | - | 28.0.5.161 | - |

**Basic Network Configuration**

You are essentially rebuilding the network from **Scenarios 5-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 DHCP 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

**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**