Routing and Switching: Scaling Network v6 Case Study

Overview and Objectives

This case study allows students fully Design a complex network using skills gained throughout the course but build and configure only a prototype as seen in the following diagram, using Cisco Packet Tracer v7.2. This case study is not a trivial task. To complete it as outlined with all required documentation will be a significant accomplishment.

The case study scenario describes the project in general terms, and will explain why the network is being built. Following the scenario, the project is broken into a number of phases, each of which has a detailed list of requirements. It is important to read and understand each requirement to make sure that the project is completed accurately.

This case study requires the student to accomplish the following tasks:

- Set up the physical layout of the network using the diagram and accompanying narrative
- Correctly configure Network Devices with a basic configuration
- Correctly configure multi-area OSPF with MD5 authentication
- Correctly configure VLANs and 802.1q trunking
- Correctly configure STP
- Correctly configure Etherchannel when required
- Correctly configure Multi-area OSPF routing
- Correctly configure HSRP
- Correctly configure DHCP
- Correctly configure NAT
- Create and apply access control lists (ACLs) on the appropriate routers and interfaces
- Verify/test and document that all devices are operational and functioning according to the scenario guidelines
- Provide detailed documentation in a prescribed form as listed in the deliverables sections

Scenario:

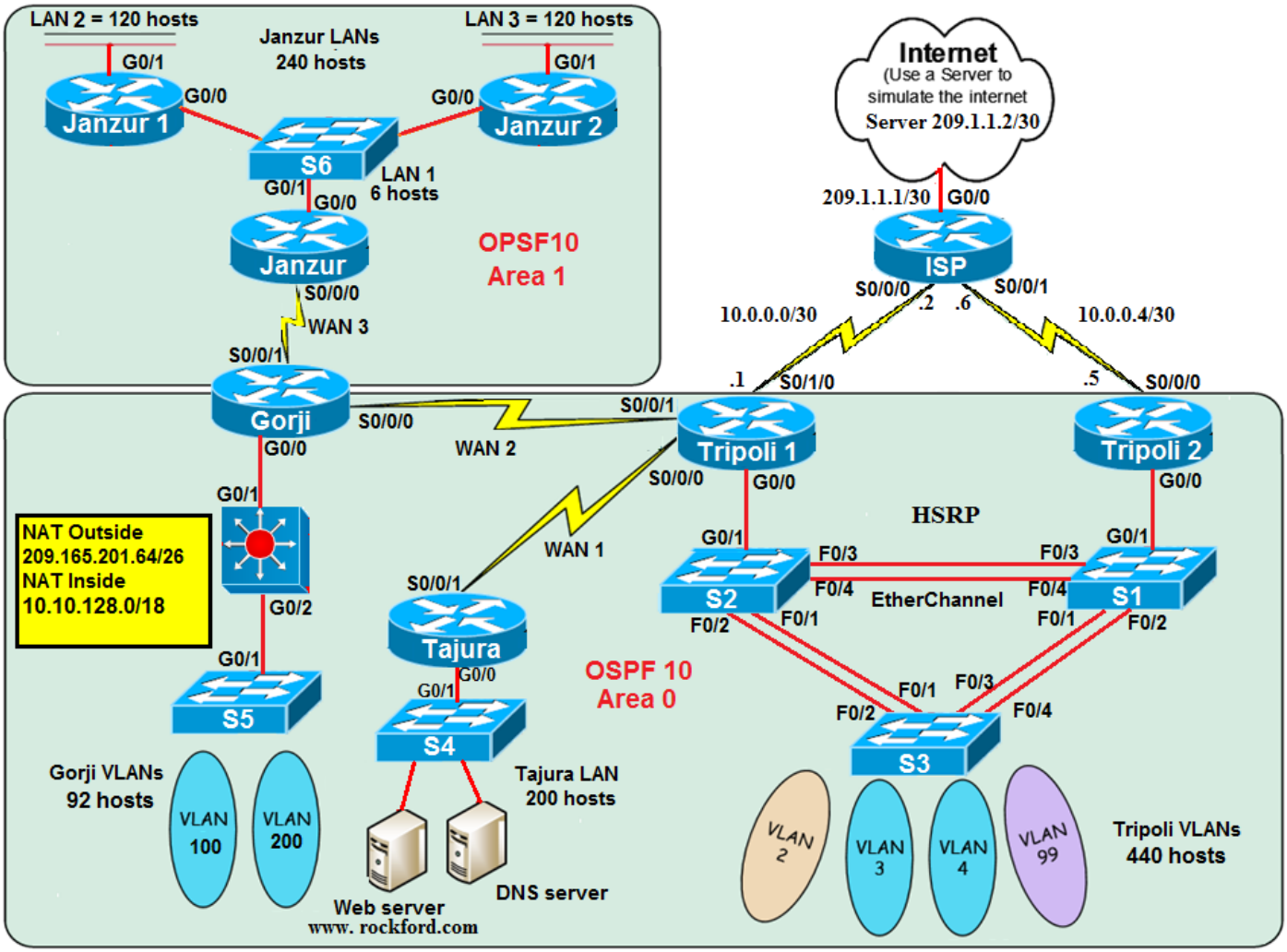
Rockford PLC is a large company who specialise in the manufacture of several models of cars. The company has been actively new employees throughout the year. Rockford realises that to aggressively compete in its market, the company needs change to its infrastructure that will support new models of cars and Internet access, allowing them to increase their productivity and to follow market trends. Rockford wants to use the internet to gain clients and find new opportunities.

Rockford PLC needs a network to be designed and implemented; the company has locations in four cities. All of the locations will be connected using leased-line serial links. All four locations will use OSPF routing process. Also, default static route must be used to access the internet.

One location, Tripoli, has a large and complex LAN. Due to the size and complexity, the company wants to create VLANs to control broadcasts, enhance security, and logically group users. The company also wants to use private addresses throughout the Autonomous System, DHCP over most of the LAN segments, and NAT implemented for Internet connectivity. The company also wishes to limit Internet access to Web traffic while allowing multiple protocols (not all) within its own WAN.

Although private addresses (RFC 1918) will be used, the company appreciates efficiency and address conservation in design. To minimize wasted address space, they have requested VLSM to be used when appropriate.

You are a junior network engineer and have been requested by a Rockford PLC to design an appropriate addressing scheme to fit their network requirements.



Phase 1: Addressing the WAN & LANs

Use the following instructions to complete Phase 1:

- Use 10.10.128.0/18 for internal addressing with IP subnet zero enabled.
- Apply /30 subnets on all serial interfaces.

- Assign an appropriately sized subnet for the Tripoli LANs, which has 440 devices:
  - VLAN 99: 10 hosts (Management VLAN)
  - VLAN 2: 120 hosts
  - VLAN 3: 60 hosts
  - VLAN 4: 250 hosts
- Assign an appropriately sized subnet for the Janzur LANs (LAN2+LAN3), which have 240 devices.
- Assign an appropriately sized subnet for the Janzur LAN1, which have 6 devices.
- Assign the appropriately sized subnet to the Tajura LAN, which has 200 hosts.
- Assign the appropriately sized subnet to the Gorji LANs, which has 92 hosts
  - VLAN 100: 60 hosts
  - VLAN 200: 30 hosts
  - VLAN 300: 2 hosts (Management VLAN)
- Document all of the addressing in tables.

Note:

- Addresses will be assigned statically to hosts Tajura LAN, Janzur 1 LAN, Janzur 2 LAN and VLAN 99.
- Addresses will be assigned dynamically to hosts; refer to the DHCP section to this document for details**.**

Phase 2: Basic Router and Switch Configuration

Use the following instructions to complete Phase 2:

1. Configure each router with the following settings:
   - Configure **router name**
   - Console Password: **cisco**
   - Enable secret password: **class**
   - Banner MOTD: # Authorized Access Only#
   - encrypt all passwords
   - Use SSH for management connections
     - vty 0-4
     - Configure the domain name to be **cisco.com**.
     - Create an **admin** user with **cisco** as the password.
   - Configure the interfaces on all routers as documented in Phase 1.
   - Assign the first IP address available to routers
   - Configure descriptions in point-to-point interfaces:

     Link to *Router name*
   - Configure descriptions in LAN interfaces:

     Link to *LAN name*
2. Configure each switch with the following settings:
   - Configure **Switch name**
   - Console password: **cisco**
   - Enable secret password: **class**

- encrypt all passwords
- Banner MOTD: # Authorized Access Only#
- Configure a switch to remotely manage.
- Use SSH for management connections
  - vty 0-4
  - Configure the domain name to be **cisco.com**.
  - Create an **admin** user with **cisco** as the password.
- Configure interfaces descriptions only that connected with routers:

  Link to *Router name*

3. Use Table to document the final addressing scheme.

Phase 3: Configure VLANs

Use the following instructions to complete Phase 4:

1. Apply the switch configuration as follows:

   - STP (PVST +) - VTP Server (S1) -VTP Client (S2,S3)

2. Configure the Tripoli's LANs (2 routers and 3 switches) as follows:

- Create and name three Data VLANs and one Management VLAN
  - VLAN 99: Management
  - VLAN 100: Native
  - VLAN 2: HR
  - VLAN 3: Sales
  - VLAN 4: Production.
- Allow the routers to route between VLANs
- Configure switches S1, S2 and S3; assign:
  - FastEthernet ports 1-4 as trunks (802.1Q)
  - Configure Etherchannel when appropriate.
- Configure access layer switch S3; assign:
  - Port 6 to VLAN 99
  - Ports 7-10 to VLAN 2
  - Ports 11-14 to VLAN 3
  - Ports 14-20 to VLAN 4
  - Disable all unused ports and put them in Garbage VLAN.
- Connect G0/0 of the Tripoli's 2 routers to G0/1 of S1 and S2

3. Configure the Gorji's LANs as follows:
   - Create and name two Data VLANs and one Management VLAN
     - VLAN100: Sales
     - VLAN 200: Production.
     - VLAN 300: Management
   - Allow a multilayer switch to route between VLANs
   - Configure access layer switch S5; assign:
     - Ports 1-10 to VLAN 100
     - Ports 15-20 to VLAN 200
     - Disable all unused ports and put them in Garbage VLAN.
4. Connect one PC per VLAN (for testing purposes).
5. This documentation will serve as the deliverable item for Phase 3

Phase 4: Configuring Default Routes, OSPF Routing and HSRP

Use the following instructions to complete Phase 3:

- Configure **Multi-area OSPF** on Routers (Janzur, Gorji, Tajura, and Tripoli).
- Configure a summary (type 3) for area 1.
- To control the DR and BDR election on LAN 1, configure the Gigabit Ethernet 0/0 port of each router with the following OSPF interface priorities :
    - **Janzur 1**: 200
    - **Janzur 2**: 100
    - **Janzur**: **1** (This is the default priority)
- Configure a Default on Tripoli and redistribute the route into the OSPF process.
- Configure MD5 authentication between OSPF routers across all WAN links
- Adjust the Hello timer to 40 sec and Dead timers to 160 sec on the link between Janzur and Gorji.
- Verify that the Janzur, Gorji, Tajura, and Tripoli routers have connectivity through Layers 1-7.
- Provide the ability of the network to dynamically recover from the failure of a device acting as a default gateway to ISP. Use **first-hop redundancy protocol** (HSRP) to provide the mechanism.
- Capture and save the four router configuration files. Edit the text file, and include comments.
- This documentation will serve as the deliverable item for Phase 4.

Phase 5: Configuring ACLs

Use the following instructions to complete Phase 5:

1. Configure a Standard ACL to filter traffic.
   The ACL should:
   - Deny only VLAN 100 and VLAN 200 users access to VLAN 4 (Production), permit all others
2. Configure a Named Standard ACL to filter traffic.
   The ACL should:
   - Permit the HR (VLAN 2), Janzur 1 LAN and Janzur 2 LAN users to access the Tajora LAN, deny all others.
3. Use an ACL to control SSH access to all routers.
   The ACL should:
   - Allow SSH session to all routers from the Management VLAN (VLAN 99) only; SSH sessions from all other networks should be denied.
4. Document the ACL configuration in a table.
5. This will serve as the deliverable item for Phase 5.

Phase 6: Configuring DHCP

DHCP Services

- DHCP should provide services to the following LANs hosts:
  - Tripoli's VLAN 2, VLAN 3 and VLAN 4
  - Gorji's VLANs
- DHCP should pass the following parameters to the hosts:
  - IP address and Subnet Mask
  - Default Gateway
  - DNS address
- The Gorji router will perform the DHCP services. Configure Janzur using the DHCP pools documented in Phase 1.
- Configure DHCP services on the Gorji router as follows:
  - Exclude the first 10 IP addresses from each pool (to be used for printers, servers, and so on)
  - Connect one PC per VLAN/LAN (for testing purposes) and Configure PCs to obtain its IP address automatically.
- Recapture and save the Gorji routers configuration file. Edit the text file, and include comments.
- This documentation will serve as the deliverable item for Phase 6.

Phase 7: Configuring PAT and Static NAT

The Tripoli's (1) routers will perform NAT. Configure the routers as follows:

1. Configure Static NAT to translate the public local IP address 200.10.10.65/26 to a private local IP address 10.10.X.X (the internal Web Server residing on the Tajora LAN)

2. Configure Dynamic NAT as follows:
   - Define the NAT pool. The pool consists of public network address 200.100.10.64/26. Exclude first 10 addresses from this pool (to be use for servers, when required).
   - Define an access control list, which will translate for all internal (10.10.128.0/18) addresses.
   - Establish PAT source translation, specifying the NAT pool and the ACL defined in the previous steps.
   - Specify the inside and the outside NAT interfaces.
3. Connect a web server to Tripoli's G0/0 port to simulate an ISP server.
   - Configure this Server as follows:
     - Configure the IP address and subnet mask as 209.1.1.2/30.
     - Configure the default gateway to be 209.1.1.1.

4. Connect a web server to Tajora LAN, configure the server with an IP address, subnet mask and a default gateway.
   - Enable a simple web page (www. rockford.com) that will tell users that they have reached the web server.
5. Recapture and save the Tripoli's routers configuration file. Edit the text file, and include comments.
6. Document NAT configuration in a chart; it will serve as the deliverable item for Phase 7.

Phase 8: Verification and Testing

Use the following instructions to complete Phase 8:

- Verify communication between various hosts in the network. Troubleshoot and fix any problems in the network until it works properly. Document the results of the tests in a table.

Phase 9: Documenting the Network

The final task in this case study is to write a formal report should be provided that contains all of the design documents as well as all the supporting worksheets (see the case study requirements; Overview and Objectives on page 1) with your recommendations.

The design documentation should include: device configurations, a list of the number and types of networking devices selected for this design, logical and physical diagrams, subnetting scheme, and network testing verifications. The completed tables from Phase 1, Phase 2, Phase 3, Phase 4, Phase 6, Phase 7, and Phase 8, should be included with the final deliverable items.

The documentation should be complete and should contain enough information to allow a third party to properly install and configure or troubleshoot the network without requesting additional information.

Hand in arrangement:

- The deadline for submission of this Case Study is 11.59am on 15 Jan 2019.
- How to submit Case Study to email address (hmswhmsw@yahoo.com):
  - **Email Subject**
    - Subject: CCNA3 Case Study – Department - your Name
    - Attached Files:
      - **CCNA3 Case Study – Department - your Name.Docx/PDF**
      - **CCNA3 Case Study – Department - your Name.pkt**