Introduction to Networks Capstone Project

Objectives

In this activity, you will also be required to design an IPv4 and IPv6 addressing scheme. Documentation and presentation are also vital parts of this Capstone Project. You will also demonstrate your ability to design and implement a secure network utilizing passwords and banners, demonstrate knowledge in CDP.

Part 1: Create an addressing scheme.

Step 1: Design an IPv4 addressing scheme based on the following requirements.

The **168.131.0.0/17** network has the following addressing requirements:
- The Production department will require a subnet that supports 7843 IPv4 addresses
- The Marketing department will require a subnet that supports 6981 IPv4 addresses
- The Sales department will require a subnet that supports 3159 IPv4 addresses
- The Human Resource department will require a subnet that supports 3955 IPv4 addresses
- The Payroll department will require a subnet that supports 1800 IPv4 addresses
- The Accounting department will require a subnet that supports 963 IPv4 addresses
- The Research and Development department will require a subnet that supports 510 IPv4 addresses
- The IT department will require a subnet that supports 252 IPv4 addresses

Step 2: Create a table for each department.

The table should have the following:
- Subnet address
- Range of usable addresses
- Excluded addresses

Step 3: Design an IPv6 addressing scheme based on the following requirements.

The **2001:BD8:454E:C937:1:BDF4:ABCD:A000 /64** network has the following addressing requirements:
- The Wireless Network will require a subnet that supports 450 IPv6 addresses
- The IT department will require a subnet that supports 252 IPv6 addresses
- Building Security will require a subnet that supports 16 IPv6 addresses
- The Mail Room will require a subnet that supports 14 IPv6 addresses
- Custodial Staff will require a subnet that supports 10 IPv6 addresses
- The Lounge will require a subnet that supports 12 IPv6 addresses
- The link connecting the office building to the ISP will require 2 IPv6 addresses.

Step 4: Create a table for each department.

The table should have the following:
- Subnet address
- Range of usable addresses
- Excluded addresses

Step 5: Describe IPv6 addresses

a. Link local addresses are non-routable addresses. Give an example of how they can be used on a network.

b. IPv6 global unicast addresses can be assigned the following ways: static, stateful auto-configuration, stateless auto-configuration, and EUI-64. Explain when you would implement each method and why.

c. A /64 IPv6 address gives you more than18 Quintilian addresses that can be assigned to devices on your network. If this is the case, why does IPv6 put aside a private address range? What is the full range of IPv6 private addresses and how are can they be implemented on a network?

Part 2: Basic Device Security

Step 1:   You are required to configure all of the devices on the network. Due to budget issues, the company was not able to purchase new equipment. All switches and routers were purchased at lower prices from another company who had the equipment implemented within their own multi-VLAN network. The passwords for these devices are unknown. There is a mixture of Cisco Catalyst 3560v2 switches and 2911 routers.

a. Explain the preliminary procedures that must be completed before you can use these devices on your network. Outline the steps and commands for the above switches and routers. Describe what would happen if you did not complete these steps. Give two possible scenarios you would run into if you did not complete the procedures you listed.

Step 2:   After you have completed the preparation to implement the equipment on your network you will be preforming basic configurations on each device. Complete each step based on its requirements.

a. There are two employees in the company that will have access to network devices within the building. RJ the junior network technician is only allowed to execute commands in user EXEC level. Barry the senior network technician will have full access to all devices. Both users will be connecting via a console cable. Explain how you would secure and limit console access on the devices. How would you configure each device so that both technicians have individualized privileges? Explain the disadvantage of having a single global login for all users?

b. As part of the security policy, you will be implementing banner messages on each device. What would be included in an appropriate banner warning unauthorized users? Create a banner that can be implemented on each device. Describe the difference between a login banner and a message of the day banner. How are each configured? When would they each be displayed within CLI?

c. You are having a debate with your co-worker on which type of password you would use to secure privileged EXEC mode. He insists that you use an enable password because it will be easier to locate if forgotten. You obviously do not agree with his method of securing devices. Which method(s) would you implement that is a more secure than an enable password? Provide a valid argument to disprove his method of security. If your co-worker insists on using the enable password, explain which additional command you can use in order to provide further security.

d. Senior network administrators of this company will spend the majority of their time working remotely. You will need to configure remote access to the switches on the network. What configuration steps are required to allow a technician to access the switch from a remote site? What means of remote access would you use to ensure integrity and security? Outline the commands that you would use to set this type of access up. There would be certain situations when the less secure method of remote access would be required, explain the alternative method of remote connection and how it differs in terms of security and type of encryption. When would you be required to use this method?

Part 3: Remote Management

The Health and Hospital Corporation (HHC) network in New York City has off-site locations that span across the New York region. With limited amounts of network personnel, each of these sites requires a remote management system to all of its devices. Is there a way to configure your routers and switches to meet this requirement? If so, which method would you choose and why? According to the Health Insurance Portability and Accountability Act of 1996 (HIPPA) regulations, the privacy/security of hospital information is crucial. Why would you need to keep this in mind when selecting a method of remote connectivity? There will be certain situations when the less private/secure method of remote access would be required. What alternative method of remote access would we use in this circumstance and how does it differ in terms of security and type of encryption? Outline the commands that you would use to configure both types of remote access. Your commands should be separate for both switches and routers.

Part 4:   Cisco Discovery Protocol (CDP)

Step 1: Scenario #1

You were hired as a network administrator and your primary task is to map all of the devices on the network. There are hundreds of routers and switches that were never documented by former network technicians. After careful consideration, you decide to use CDP to complete this task.

a. Explain CDP and how it can be used to map devices on a network?

b. Which CDP commands can you use to discover devices on the network? Explain in detail the information that each displays.

c. If CDP were not available which alternative method would you use to accomplish this? Be creative.

Step 2: Scenario #2

Sara has just been hired as a junior network technician at a large IT group overseeing the NYCDOE network. One issue Sara saw on her monitor is that a section of the network is having connectivity issues. One of the switches on that part of the network flashes a syslog message that says **%CDP-4-DUPLEX_MISMATCH**.

a. Make a list of possible issues that may have triggered this syslog error.

b. Which commands can you use to troubleshoot this problem?