**CCNA Routing and Switching  
Scaling Networks**  
  
**EIGRP Practice Skills Assessment - Packet Tracer**  
  
A few things to keep in mind while completing this activity:

1. Do not use the browser Back button or close or reload any exam windows during the exam.
2. Do not close Packet Tracer when you are done. It will close automatically.
3. Click the Submit Assessment button in the browser window to submit your work.

**Introduction**  
  
In Part I of this practice skills assessment, you will configure routing and ACLs. You will configure dynamic routing with EIGRP for IPv4 and static and default routes. In addition, you will configure two access control lists.  
  
In Part II of this practice skills assessment, you will configure the Company A network with RPVST+, port security, EtherChannel, DHCP, VLANs and trunking, and routing between VLANs. In addition you will perform an initial configuration on a switch, secure unused switch ports and secure SVIs. You will also control access to the switch management network with an access control list.  
  
**All IOS device configurations should be completed from a direct terminal connection to the device console from an available host.**  
**Some values that are required to complete the configurations have not been given to you. In those cases, create the values that you need to complete the requirements. These values may include certain IP addresses, passwords, interface descriptions, banner text, and other values.  
  
When you have been given a text value, such as a password, user name, DHCP pool name, ACL name, VLAN name, etc, you must enter these values exactly as they are given in these instructions. If the values do not match exactly, you may not receive credit for your configuration.**  
For the sake of time, many repetitive but important configuration tasks have been omitted from this activity. Many of these tasks, especially those related to device security, are essential elements of a network configuration. The intent of this activity is not to diminish the importance of full device configurations.  
  
You will practice and be assessed on the following skills:

* Configuration of initial device settings
* IPv4 address assignment and configuration
* Configuration and addressing of device interfaces
* Configuration of the EIGRP for IPv4 routing protocol
* Configuration of a default route
* Configuration of ACL to limit device access
* Configuration of switch management settings including SSH
* Configuration of port security
* Configuration of unused switch ports according to security best practices
* Configuration of RPVST+
* Configuration of EtherChannel
* Configuration of a router as a DHCP server
* Configuration of VLANs and trunks
* Configuration of routing between VLANs

You are required to do the following:  
  
Site-1:

* Configure initial device settings.
* Configure interfaces with IPv4 addresses, descriptions, and other settings.
* Configure and customize EIGRP for IPv4.

HQ:

* Configure interfaces with IPv4 addresses, descriptions, and other settings.
* Configure and customize EIGRP for IPv4.
* Configure named and numbered ACLs.
* Configure and propagate a default route through EIGRP for IPv4.

Site-2:

* Configure interfaces with IPv4 addresses, descriptions, and other settings.
* Configure DHCP pools and excluded addresses.
* Configure routing between VLANs.
* Configure EIGRP for IPv4.
* Configure EIGRP for IPv4 route summarization.
* Configure an ACL to limit access to the switch management network.

SW-A:

* Create and name VLANs.
* Configure EtherChannel.
* Configure trunking.
* Assign access ports to VLANs.
* Configure remote management settings.
* Activate and configure RPVST+.
* Secure unused switch ports.
* Configure port security.

SW-B:

* Create and name VLANs.
* Configure EtherChannel.
* Configure trunking.
* Assign access ports to VLANs.
* Configure remote management settings with SSH.
* Activate RPVST+.

SW-C:

* Create and name VLANs.
* Configure EtherChannel.
* Configure trunking.
* Assign access ports to VLANs.
* Configure remote management settings.
* Activate and configure RPVST+.

Internal PC hosts:

* Configure as DHCP clients.
* Assign Static IPv4 addresses where indicated.

**Tables**  
  
Note: You are provided with the networks that interfaces should be configured on. Unless you are told to do differently in the detailed instructions below, you are free to choose the host addresses to assign.  
  
**Addressing Table:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **Network** | **Configuration Details** |
| **Site-1** | S0/0/0 | 192.168.100.20/30 | any address in the network |
| S0/0/1 | 192.168.100.28/30 | any address in the network |
| G0/0 | 192.168.8.0/24 | first host address |
| G0/1 | 192.168.9.0/24 | first host address |
| **HQ** | S0/0/0 | 192.168.100.20/30 | any address in the network |
| S0/0/1 | 192.168.100.36/30 | any address in the network |
| S0/1/0 | 203.0.113.16/29 | (The first address in this network is already in use on the ISP router. Any other address in the network can be assigned to this interface.) |
| **Site-2** | S0/0/0 | 192.168.100.28/30 | any address in the network |
| S0/0/1 | 192.168.100.36/30 | any address in the network |
| G0/1.2 | 10.10.2.0/24 | first address in the network |
| G0/1.4 | 10.10.4.0/24 | first address in the network |
| G0/1.8 | 10.10.8.0/24 | first address in the network |
| G0/1.15 | 10.10.15.0/24 | first address in the network |
| G0/1.25 | 10.10.25.0/24 | first address in the network |
| **SW-A** | SVI | 10.10.25.0/24 | the highest address in the network |
| **SW-B** | SVI | 10.10.25.0/24 | the second to the highest address in the network |
| **SW-C** | SVI | 10.10.25.0/24 | the third to the highest address in the network |
| **Oper 1A** | NIC | 192.168.8.0/24 | any available address in the network |
| **Clerk 1C** | NIC | 192.168.9.0/24 | any available address in the network |
| **Admin-A** | NIC | 10.10.15.0/24 | any available address in the network |
| **Admin-B** | NIC | 10.10.15.0/24 | any available address in the network |

**VLAN Switch Port Assignment Table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN** | **Name** | **Network** | **Device** | **Switch Ports** |
| **2** | sales | 10.10.2.0/24 | SW-A | Fa0/5 |
| SW-C | Fa0/7 |
| **4** | prod | 10.10.4.0/24 | SW-A | Fa0/10 |
| SW-C | Fa0/10 |
| **8** | acct | 10.10.8.0/24 | SW-A | Fa0/15 |
| SW-C | Fa0/15 |
| **15** | admin | 10.10.15.0/24 | SW-A | Fa0/24 |
| SW-C | Fa0/24 |
| **25** | SVI-NET | 10.10.25.0/24 | SW-A | SVI |
| SW-B | SVI |
| SW-C | SVI |
| **99** | null | N/A | SW-A | all unused ports |

**Port-Channel Group Interfaces:**

|  |  |  |
| --- | --- | --- |
| **Channel** | **Device** | **Interfaces** |
| **1** | SW-A | Fa0/1, Fa0/2 |
| SW-C | Fa0/1, Fa0/2 |
| **2** | SW-A | Fa0/3, Fa0/4 |
| SW-B | Fa0/3, Fa0/4 |
| **3** | SW-B | Fa0/5, Fa0/6 |
| SW-C | Fa0/5, Fa0/6 |

**Instructions**  
 **All configurations must be performed through a direct terminal connection to the device console lines from an available host.**  
  
**Part I: EIGRP Router Configuration**  
  
**Step 1: Plan the Addressing.**  
  
Determine the IP addresses that you will use for the required interfaces on the devices and LAN hosts. Follow the configuration details provided in the Addressing Table.  
  
**Step 2: Configure Site-1.**  
Configure **Site-1** with initial settings:

* Configure the router host name: **Site-1**. This value must be entered exactly as it appears here.
* Prevent the router from attempting to resolve command line entries to IP addresses.
* Protect device configurations from unauthorized access with an encrypted secret password.
* Secure the router console and remote access lines.
* Prevent system status messages from interrupting console output.
* Configure a message-of-the-day banner.
* Encrypt all clear text passwords.

**Step 3: Configure the Router Interfaces.**  
  
Use the information in the addressing table to configure the interfaces of all routers for full connectivity with the following:

* Configure IP addressing.
* Descriptions for the three connected interfaces of **HQ**.
* Configure DCE settings where required. Use a rate of **128000**.
* The Ethernet subinterfaces on Site-2 will be configured later in this assessment.

**Step 4: Configure inter-VLAN routing on Site-2.**  
  
Configure router **Site-2** to route between VLANs using information in the Addressing Table and VLAN Switch Port Assignment Table. The VLANs will be configured on the switches later in this assessment.

* Do not route the VLAN 99 network.

**Step 5: Configure EIGRP Routing and a default route.**  
  
  a. On **all** routers:

* Configure EIGRP for IPv4 to route between the internal networks. Use ASN **100**.
* Use the precise wild card masks for all network statements.
* You are not required to route the**SVI-NET** **VLAN** network over EIGRP.
* Prevent routing updates from being sent on the LAN networks.  Do not use the **default** keyword version of the command to do so.
* Prevent EIGRP for IPv4 from performing automatic route summarization on all routers.

  b. On the **HQ** router:

* Configure a default route to the Internet. Use the exit interface argument.
* Configure EIGRP for IPv4 to distribute the default route to the other routers.

**Step 6: Customize EIGRP for IPv4.**  
  
Customize EIGRP for IPv4 by performing the following configuration tasks:

* Set the bandwidth of the link between Site-1 and HQ to**128 kb/s**.
* Create a summary route for the LANs connected to SW-C. It should include all networks from 10.10.0.0 to 10.10.15.0.
* Do not include the **SVI-NET** **VLAN** network in the summary route.
* Configure EIGRP for IPv4 with the route summary so that it will be sent to the other routers. Be sure to configure the summary on all of the appropriate interfaces.

**Step 7: Configure Access Control Lists.**  
  
You will configure two access control lists in this step. You should use the **any** and **host** keywords in the ACL statements where appropriate. The ACL specifications are as follows:  
  
  a.  Restrict access to the vty lines on **HQ** with an ACL:

* Create a named standard ACL using the name **telnetBlock**. Be sure that you enter this name exactly as it appears in this instruction or you will not receive credit for your configuration.
* Allow only **Admin Host** to access the vty lines of **HQ**.
* No other Internet hosts (including hosts not visible in the topology) should be able to access the vty lines of **HQ**.
* Your solution should consist of **one** ACL statement.

  b.  Block ping requests from the Internet with an ACL:

* Use access list number **101**.
* Allow only **Admin Host** to ping addresses within the Company A network. Only echo messages should be permitted.
* Prevent all other Internet hosts (not only the Internet hosts visible in the topology) from pinging addresses inside the Company A network. Block echo messages only.
* All other traffic should be allowed.
* Your ACL should consist of **three** statements.
* Your ACL should be placed in the most efficient location as possible to conserve network bandwidth and device processing resources.

c. Control access to the management interfaces (SVI) of the three switches attached to **Site-2** as follows:

* Create a standard ACL.
* Use the number **1** for the list.
* Permit only addresses from the **admin** **VLAN** network to access any address on the **SVI-NET** **VLAN** network.
* Hosts on the  **admin** **VLAN** network should be able to reach all other destinations.
* Your list should consist of **one** statement.

**Part II: Switching and DHCP Configuration**  
  
**Step 1: Create and name VLANs.**  
  
On all three switches that are attached to Site-2, create and name the VLANs shown in the VLAN Table.

* The VLAN names that you configure must match the values in the table exactly.
* Each switch should be configured with all of the VLANs shown in the table.

**Step 2:  Assign switch ports to VLANs.**  
  
Using the VLAN table, assign the switch ports to the VLANs you created in Step 1, as follows:

* All switch ports that you assign to VLANs should be configured to **static access mode**.
* All switch ports that you assign to VLANs should be activated.

**Step 3:  Configure the SVIs.**  
  
Refer to the Addressing Table. Create and address the SVIs on all three of the switches that are attached to Site-2. Configure the switches so that they can communicate with hosts on other networks. Full connectivity will be established after routing between VLANs has been configured later in this assessment.  
 **Step 4:  Configure Trunking and EtherChannel.**  
  
  a. Use the information in the Port-Channel Groups table to configure EtherChannel as follows:

* Use LACP.
* The switch ports on both sides of Channels 1 and 2 should initiate negotiations for channel establishment.
* The switch ports on the**SW-B** side of the Channel 3 should initiate negotiations with the switch ports on **SW-C**.
* The switch ports on the **SW-C** side of Channel 3 should **not** initiate negotiations with the switch ports on the other side of the channel.
* All channels should be ready to forward data after they have been configured.

  b. Configure all port-channel interfaces as trunks.  
  
  c. Configure static trunking on the switch port on **SW-B** that is connected to **Site-2**.  
  
**Step 5:  Configure Rapid PVST+.**  
Configure Rapid PVST+ settings as follows:  
  
  a. Activate Rapid PVST+ and set root priorities.

* All three switches should be configured to run Rapid PVST+.
* **SW-A** should be configured as root primary for VLAN 2 and VLAN 4 using the default primary priority values.
* **SW-A** should be configured as root secondary for VLAN 8 and VLAN 15 using the default secondary priority values.
* **SW-C** should be configured as root primary for VLAN 8 and VLAN 15 using the default primary priority values.
* **SW-C** should be configured as root secondary for VLAN 2 and VLAN 4 using the default secondary priority values.

  b. Activate PortFast and BPDU Guard ontheactive**SW-C** switch access ports.

* Configure PortFast on all access ports that are connected to hosts.
* Activate BPDU Guard on all access ports that are connected to hosts.

**Step 6:  Configure switch security.**  
You are required to complete the following only on some of the devices in the network for this assessment. In reality, security should be configured on all devices in the network.  
  
  a. Secure unused switch ports. Following security best practices, do the following on **SW-A** only:

* Shutdown all unused switch ports.
* Configure all unused switch ports as static access ports.
* Ensure that all unused switch ports have been assigned to **VLAN 99**.

  b. Configure port security on all active access ports on **SW-A**.

* Each switch port should accept only **two** MAC addresses before a security action occurs.
* The learned MAC addresses should be recorded in the running configuration.
* If a security violation occurs, the switch ports should provide notification that a violation has occurred but not place the interface in an err-disabled state.

  c. On **SW-B**, configure the virtual terminal lines to accept only SSH connections.

* Use a domain name of **ccnaPTSA.com**.
* Use a modulus value of **1024**.
* Configure SSH version **2**.
* Configure the vty lines to only accept SSH connections.
* Configure user-based authentication for the SSH connections with a user name of **netadmin** and an encrypted secret password of **SSHsecret9**. The user name and password must match the values provided here exactly in capitalization, punctuation, and spelling.
* In order to test the SSH connection, you will need further configure **SW-B**.

**Step 7: Configure Site-2 as a DHCP server for the hosts attached to the SW-A and SW-B switches.**  
  
Configure three DHCP pools as follows:

* Create a DHCP pool for hosts on VLAN 2 using the pool name **vlan2pool**.
* Create a DHCP pool for hosts on VLAN 4 using the pool name **vlan4pool**.
* Create a DHCP pool for hosts on VLAN 8 using the pool name **vlan8pool**.
* All VLAN pool names must match the provided values above exactly.
* Exclude the **first five** addresses from each pool.
* Configure a DNS server address of **192.168.200.225**.
* All hosts should be able to communication with hosts on other networks.

**Step 8: Configure host addressing.**

**Note: This assessment is a simulation of a working network. Due to the complexities of the protocols and technologies that are simulated in this network, some connectivity tests may not succeed even though the network has been properly configured. If all required configurations are complete, your score will not be affected.**

All hosts should be able to ping each other and the two external servers after they have been addressed.

* Hosts on VLANs 2, 4, and 8 should be configured to receive addresses dynamically over DHCP.
* Hosts on VLAN 15 should be addressed statically as indicated in the addressing table. Once configured, the hosts should be able to ping hosts on other networks.
* Hosts on the LANs attached to **Site-1** should be statically assigned addressing that enables them to communicate with hosts on other networks.

*Last Updated: December, 2015*  
  
ID: 0  
  
***Version 3.0  
Created in Packet Tracer 6.2 and Marvel 2.0.5  
All contents are Copyright © 1992 - 2016 Cisco Systems, Inc. All rights r***