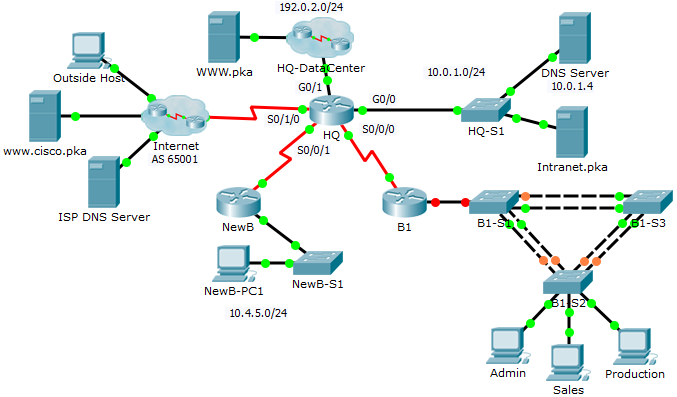
Packet Tracer – CCNA Skills Integration Challenge

1. Topology



1. Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask |
| **HQ** | G0/0 | 10.0.1.1 | 255.255.255.0 |
| G0/1 | 192.0.2.1 | 255.255.255.0 |
| S0/0/0 | 10.255.255.1 | 255.255.255.252 |
| S0/0/1 | 10.255.255.253 | 255.255.255.252 |
| S0/1/0 | 209.165.201.1 | 255.255.255.252 |
| **B1** | G0/0.10 | 10.1.10.1 | 255.255.255.0 |
| G0/0.20 | 10.1.20.1 | 255.255.255.0 |
| G0/0.30 | 10.1.30.1 | 255.255.255.0 |
| G0/0.99 | 10.1.99.1 | 255.255.255.0 |
| S0/0/0 | 10.255.255.2 | 255.255.255.252 |
| **B1-S2** | VLAN 99 | 10.1.99.22 | 255.255.255.0 |

1. VLAN Configurations and Port Mappings

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Number | Network Address | VLAN Name | Port Mappings |
| **10** | 10.1.10.0/24 | Admin | F0/6 |
| **20** | 10.1.20.0/24 | Sales | F0/11 |
| **30** | 10.1.30.0/24 | Production | F0/16 |
| **99** | 10.1.99.0/24 | Mgmt&Native | F0/1-4 |
| **999** | N/A | BlackHole | Unused Ports |

1. Scenario

In this comprehensive CCNA skills activity, the XYZ Corporation uses a combination of eBGP and PPP for WAN connections. Other technologies include NAT, DHCP, static and default routing, EIGRP for IPv4, inter-VLAN routing, and VLAN configurations. Security configurations include SSH, port security, switch security, and ACLs.

**Note**: Only **HQ**, **B1**, **B1-S2**, and the PCs are accessible. The user EXEC password is **cisco** and the privileged EXEC password is **class**.

1. Requirements

PPP

* Configure the WAN link from **HQ** to the Internet using PPP encapsulation and CHAP authentication.
* Create a user **ISP** with the password of **cisco**.
* Configure the WAN link from **HQ** to **NewB** using PPP encapsulation and PAP authentication.
* Create a user **NewB** with the password of **cisco**.

**Note**: The **ppp pap sent-username** is not graded by Packet Tracer. However, it must be configured before the link will come up between **HQ** and **NewB**.

eBGP

* Configure eBGP between **HQ** and the **Internet**.
* HQ belongs to AS 65000.
* The IP address for the BGP router in the Internet cloud is 209.165.201.2.
* Advertise the 192.0.2.0/24 network to the Internet.

NAT

* Configure dynamic NAT on HQ
* Allow all addresses for the 10.0.0.0/8 address space to be translated using a standard access list named **NAT**.
* XYZ Corporation owns the 209.165.200.240/29 address space. The pool, **HQ**, uses addresses .241 to .245 with a /29 mask. Bind the **NAT** ACL to the pool **HQ**. Configure PAT.
* The connections to the **Internet** and **HQ-DataCenter** are outside XYZ Corporation.

Inter-VLAN Routing

* Configure **B1** for inter-VLAN routing.
* Using the addressing table for branch routers, configure and activate the LAN interface for inter-VLAN routing. VLAN 99 is the native VLAN.

Static and Default Routing

* Configure **HQ** with a static route to the **NewB** LAN. Use the exit interface as an argument.
* Configure **B1** with a default route to **HQ**. Use the next-hop IP address as an argument.

EIGRP Routing

* Configure and optimize **HQ** and **B1** with EIGRP routing.
* Use autonomous system 100.
* Disable EIGRP updates on appropriate interfaces.

VLANs and Trunking Configurations

Note: Logging to the console is turned off on B1-S2 so that the Native VLAN mismatch messages will not interrupt your configurations. If you would prefer to view console messages, enter the global configuration command logging console.

* Configure trunking and VLANs on **B1-S2**.
* Create and name the VLANs listed in the **VLAN Configuration and Port Mappings** table on **B1-S2** only.
* Configure the VLAN 99 interface and default gateway.
* Set trunking mode to on for F0/1 - F0/4.
* Assign VLANs to the appropriate access ports.
* Disable all unused ports and assign the **BlackHole** VLAN.

**Port Security**

* Use the following policy to establish port security on the **B1-S2** access ports:
* Allow two MAC addresses to be learned on the port.
* Configure the learned MAC addresses to be added to the configuration.
* Set the port to send a message if there is a security violation. Traffic is still allowed from the first two MAC addresses learned.

SSH

* Configure **HQ** to use SSH for remote access.
* Set the modulus to **2048**. The domain name is **CCNASkills.com**.
* The username is **admin** and the password is **adminonly**.
* Only SSH should be allowed on VTY lines.
* Modify the SSH defaults: version 2; 60-second timeout; two retries.

DHCP

* On **B1**, configure a DHCP pool for the Sales VLAN 20 using the following requirements:
* Exclude the first 10 IP addresses in the range.
* The case-sensitive pool name is **VLAN20**.
* Include the DNS server attached to the **HQ** LAN as part of the DHCP configuration.
* Configure the **Sales** PC to use DHCP.

Access List Policy

* Because HQ is connected to the Internet, configure and apply a named ACL called **HQINBOUND** in the following order:
* Allow inbound BGP updates (TCP port 179) for any source to any destination.
* Allow inbound HTTP requests from any source to the **HQ-DataCenter** network.
* Allow only established TCP sessions from the Internet.
* Allow only inbound ping replies from the Internet.
* Explicitly block all other inbound access from the Internet.

Connectivity

* Verify full connectivity from each PC to **WWW.pka** and **www.cisco.pka.**
* The Outside Host should be able to access the webpage at WWW.pka.
* All the test in Scenario 0 should be successful.