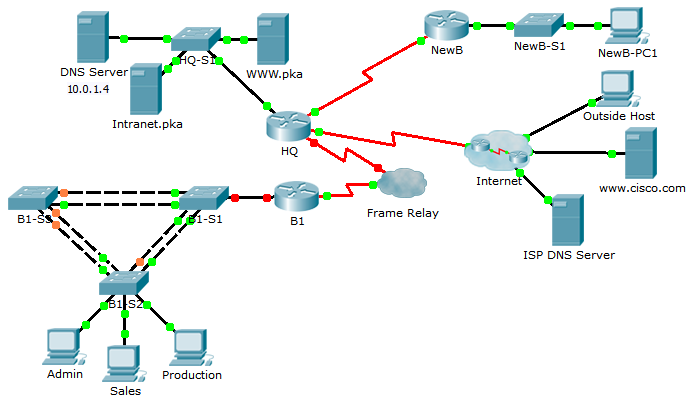
Packet Tracer – CCNA Skills Integration Challenge

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway  DLCI Mapping |
| **HQ** | G0/0 | 10.0.1.1 | 255.255.255.0 | N/A |
| S0/0/0.41 | 10.255.255.1 | 255.255.255.252 | DLCI 41 to B1 |
| S0/0/1 | 10.255.255.253 | 255.255.255.252 | N/A |
| S0/1/0 | 209.165.201.1 | 255.255.255.252 | N/A |
| **B1** | G0/0.10 | 10.1.10.1 | 255.255.255.0 | N/A |
| G0/0.20 | 10.1.20.1 | 255.255.255.0 | N/A |
| G0/0.30 | 10.1.30.1 | 255.255.255.0 | N/A |
| G0/0.99 | 10.1.99.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.255.255.2 | 255.255.255.252 | N/A |
| **B1-S2** | VLAN 99 | 10.1.99.22 | 255.255.255.0 | 10.1.99.1 |

1. VLAN Configurations and Port Mappings

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Number | Network Address | VLAN Name | Port Mappings |
| **10** | 10.1.10.0/24 | Admin | Fa0/6 |
| **20** | 10.1.20.0/24 | Sales | Fa0/11 |
| **30** | 10.1.30.0/24 | Production | Fa0/16 |
| **99** | 10.1.99.0/24 | Mgmt&Native | Fa0/1-4 |
| **999** | N/A | BlackHole | Unused Ports |

1. Scenario

In this comprehensive CCNA skills activity, the XYZ Corporation uses a combination of Frame Relay 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.

1. Requirements

**Note**: The user EXEC password is **cisco** and the privileged EXEC password is **class**.

SSH

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

Frame Relay

* Configure Frame Relay between **HQ** and **B1**.
  1. Refer to the Addressing Table for the IP address, subnet mask, and DLCI.
  2. **HQ** uses a point-to-point subinterface and DLCI 41 to connect to **B1**.
  3. The LMI type must be manually configured as **q933a** for **HQ** and **B1**.

PPP

* Configure the WAN link from **HQ** to the Internet using PPP encapsulation and CHAP authentication.
  1. Create a user **ISP** with the password of **cisco**.
* Configure the WAN link from **HQ** to **NewB** using PPP encapsulation and PAP authentication.
  1. **HQ** is the DCE side of the link. You choose the clock rate.
  2. Create a user **NewB** with the password of **cisco**.

NAT

* Configure static and dynamic NAT on HQ
  1. Allow all addresses for the 10.0.0.0/8 address space to be translated using a standard access list named **NAT**.
  2. XYZ Corporation owns the 209.165.200.240/29 address space. The pool, **HQ**, uses addresses .241 to .245 with a /29 mask.
  3. The **WWW.pka** website at 10.0.1.2 is registered with the public DNS system at IP address 209.165.200.246 and should be accessible from the **Outside** **Host**.

DHCP

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

Static and Default Routing

* Configure **HQ** with a default route to the **Internet** and a static route to the **NewB** LAN. Use the exit interface as an argument.

EIGRP Routing

* Configure and optimize **HQ** and **B1** with EIGRP routing.
  1. Use autonomous system 100 and disable automatic summarization.
  2. **HQ** should advertise the static and default router to **B1**.
  3. Disable EIGRP updates on appropriate interfaces.
  4. Manually summarize EIGRP routes so that the **B1** router only advertises the 10.1.0.0/16 address space to **HQ**.

Inter-VLAN Routing

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

VLANs and Trunking Configurations

* Configure trunking and VLANs on **B1-S2**.
  1. Create and name the VLANs listed in the **VLAN Configuration and Port Mappings** table on **B1-S2** only.
  2. Configure the VLAN 99 interface and default gateway.
  3. Assign VLANs to the appropriate access ports.
  4. Set trunking mode to on for Fa0/1 - Fa0/4.
  5. 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:
  1. Allow one MAC addresses to be learned on the port.
  2. Configure the first learned MAC address to stick to the configuration.
  3. Set the port to shut down if there is a security violation.

Access List Policy

* Because HQ is connected to the Internet, configure a named ACL called **HQINBOUND** in the following order:
  1. Allow inbound HTTP requests to the **WWW.pka** server.
  2. Allow only established TCP sessions from the Internet.
  3. Allow only inbound ping replies from the Internet.
  4. Explicitly block all other inbound access from the Internet.

Connectivity

* Verify full connectivity from each PC to **WWW.pka** and **www.cisco.pka.**