Lab 10: Configuration of BGP & Servers (DHCP, DNS & Web)

Objectives

- To be familiar with BGP for inter-AS routing and its configuration.
- To be familiar with different servers and their configuration: DHCP, DNS, and Web.

Requirements

- Network simulation tool: Packet Tracer

Procedure

A: The network topology was created as per the provided diagram, and the appropriate IP addresses, subnet masks, and default gateways were configured on each router and PC. OSPF routing was set up within each AS, ensuring no OSPF routing was passed between ASes. BGP was configured on Router1 and Router2 to advertise networks between AS 100 and AS 200. Default routing was initially omitted, then added to test connectivity. Finally, BGP route information was redistributed into OSPF, and all configurations were saved.

B: The network topology was created according to the provided diagram. The interfaces between switches and routers were connected. DHCP was configured on Router0 for both Network 1 and Network 2. IP addresses were obtained for PCs and laptops within the specified DHCP pool ranges, excluding reserved IP ranges. The DHCP server configuration was verified using appropriate commands.

C: A web server and DNS server were configured with IP addresses 192.168.1.3 and 192.168.1.2, respectively. HTTP requests within the network were successful. DHCP was configured on Router0 to provide IP configurations to new PCs. OSPF routing was implemented, allowing successful inter-network HTTP responses. The DNS server was configured to forward DNS resolution requests to the Root DNS at 192.168.3.2.

Activities

Activity A

- **1-2.** Appropriate IP addresses of the corresponding router interfaces were set, and the IP address, subnet mask, and default gateway of each PC were configured.
- **3.** OSPF routing was set up within ASes, but OSPF was not passed between different ASes.
- **4.** Within the AS, ping tests were successful, but not between PCs in different ASes.
- **5-6.** BGP was configured on Router1 and Router2 to advertise all networks of AS 200 to AS 100 and vice versa.
- **7.** Initial ping tests failed due to the lack of default routing; foreign IPs were not identified, and no default path existed for packet transfer.
- **8-9.** Default routing was added, enabling successful ping tests between all PCs. (Default routing directed packets to the appropriate router for delivery to foreign IP addresses, establishing a path for communication.)
- **11-12.** Default routing was removed, and Router1 was configured to redistribute BGP route information into OSPF. Similarly, Router2 was configured to redistribute BGP route information into OSPF.
- **13.** Successful ping tests were conducted between inter-AS devices.
- **14.** The configurations in each router were saved.

Activity B

- **1.** All interface connections were made between switches and routers as specified.
- **2.** Initial attempts to obtain IP addresses via DHCP failed, resulting in APIPA addresses.
- **3-6.** DHCP server was configured on Router0 for both Network 1 and Network 2, and IP addresses were successfully obtained for each PC and laptop within the specified DHCP pool ranges.
- **7-10.** The IP address ranges from 192.168.1.1 to 192.168.1.20 in Network 1 and from 192.168.2.1 to 192.168.2.40 in Network 2 were excluded from the DHCP pool. IP addresses were successfully obtained, excluding these ranges.

- **12.** The output of 'show ip dhcp binding' command was observed.

```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.22     0090.0C57.BB08          --                      Automatic
192.168.1.23     000B.BE64.08CD          --                      Automatic
192.168.1.24     0001.9623.C451          --                      Automatic
192.168.2.42     0040.0B9D.480E          --                      Automatic
192.168.2.43     0002.16DB.B08D          --                      Automatic
192.168.2.44     0030.A340.7891          --                      Automatic
Router#
```

Activity C

- **1-2.** A web server for cisco.com and a DNS server were created with IP addresses 192.168.1.3 and 192.168.1.2, respectively.
- **3.** HTTP requests within the network for cisco.com were successful, but requests from outside the network failed.
- **4-6.** DHCP was configured on Router0, and a new PC was added. The new PC successfully made HTTP requests to cisco.com.
- **7-8.** OSPF routing was implemented, and HTTP responses were successful across networks.
- **9.** The DNS server at 192.168.1.2 was configured to forward DNS resolution requests to the Root DNS at 192.168.3.2. The network had a web server for cisco.com and another for packet.com, with successful HTTP responses for both.

Conclusion

In this lab, BGP was configured to enable inter-AS routing, and DHCP, DNS, and web servers were set up and verified. The successful configuration and testing of these protocols and services demonstrated the principles of network communication and the importance of proper routing and server setup.

Exercises

I. Why is BGP necessary to route network traffic between ASes? Explain.

Border Gateway Protocol (BGP) is necessary to route network traffic between Autonomous Systems (ASes) because it enables the exchange of routing information between different networks. BGP is an

Exterior Gateway Protocol (EGP) that maintains a table of IP networks or 'prefixes' which designate network reachability among autonomous systems. Its key functions include:

- **Scalability:** BGP can handle the large number of routes on the Internet, making it scalable to manage global Internet routing.
- **Policy-based routing:** BGP allows network administrators to implement routing policies that control the selection of paths, influencing the flow of traffic based on business and performance considerations.
- **Loop prevention:** BGP uses a path-vector mechanism to prevent routing loops, ensuring data packets do not get caught in an endless loop.
- **Inter-domain routing:** BGP is essential for exchanging routing information between different ASes, facilitating inter-domain routing which is critical for the operation of the Internet.

Without BGP, ASes would not be able to effectively share routing information, leading to a fragmented and disconnected Internet.

II. What is DHCP? Why is it used? Explain its importance.

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks. DHCP automates the process of configuring devices on IP networks, enabling them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP.

- **IP Address Management:** DHCP dynamically assigns IP addresses to devices, ensuring that each device has a unique address, which prevents conflicts.
- **Simplification:** It simplifies network administration by automating the configuration of IP addresses, subnet masks, gateways, and other network settings, reducing the need for manual configuration.
- **Efficient Use of IP Addresses:** DHCP allows for the reuse of IP addresses by leasing them for a specified period. Once a device no longer needs an IP address, it is returned to the pool for reassignment.
- **Support for Mobile Users:** DHCP provides seamless support for mobile users who change networks frequently, such as laptops moving between different Wi-Fi networks.

The importance of DHCP lies in its ability to ensure efficient and error-free network configuration, making network management easier and more scalable.

III. What is DNS? Why is it used? Explain its importance in the Internet system.

The Domain Name System (DNS) is a hierarchical and decentralized naming system that translates human-readable domain names (e.g., www.example.com) into numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

- **Ease of Use:** DNS makes it easier for users to access websites and other resources using memorable domain names instead of numerical IP addresses.
- **Scalability:** DNS is scalable and can handle the vast number of domain names on the Internet, organized in a hierarchical structure.
- **Redundancy and Reliability:** DNS employs multiple servers and redundancy to ensure reliability and availability. If one DNS server is unavailable, others can handle the requests.
- **Efficient Traffic Management:** DNS supports load balancing and can direct traffic based on various criteria, such as geographical location, improving the performance and speed of web services.

DNS is crucial for the functionality of the Internet, providing a foundation for domain name resolution and enabling seamless access to online resources. Without DNS, the Internet would be less accessible, and navigating it would be significantly more complex.