Assignment No. 2

Using a Network Simulator (e.g. packet tracer) Configure Routing Protocols

Problem Statement :

A] Configure EIGRP – Explore Neighbor-ship Requirements and Conditions, its K Values Metrics Assignment and Calculation.

B] OSPF – Explore Neighbor-ship Condition and Requirement, Neighbor-ship states, OSPF Metric Cost Calculation.

C] WLAN with static IP addressing and DHCP with MAC security and filters.

Theory:

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network to help automate routing decisions and configuration.

EIGRP allows a router to share information it knows about the network with neighboring routers within the same logical area known as an autonomous system. Contrary to other well known routing protocols, such as routing information protocol, EIGRP only shares information that a neighboring router would not have, rather than sending all of its information. EIGRP is optimized to help reduce the workload of the router and the amount of data that needs to be transmitted between routers.

EIGRP offers the following features:

- Fast convergence—The DUAL algorithm allows routing information to converge as quickly as any currently available routing protocol.
- Partial updates—EIGRP sends incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. This feature minimizes the bandwidth required for EIGRP packets.
- Less CPU usage than IGRP—This occurs because full update packets need not be processed each time they are received.
- Neighbor discovery mechanism—This is a simple hello mechanism used to learn about neighboring routers. It is protocol-independent.
- Scaling—EIGRP scales to large networks.

Enabling EIGRP

To create an EIGRP routing process, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **router eigrp** *autonomous-system*	Enables an EIGRP routing process in global configuration mode.
Step 2	Router(config-router)# **network** *network-number*	Associates networks with an EIGRP routing process in router configuration mode.

EIGRP sends updates to the interfaces in the specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

K-Values are the most confusing part of EIGRP. Usually newbies take K Values as EIGRP metric components. K Values are not the metric components in themself. They are only the place holder or influencer for actual metric components in metric calculation formula. So when we enable or disable a K value, actually we enable or disable its associate metric component.

EIGRP uses four components out of five to calculate the routing metric.

K-Value	Component	Description
K1	Bandwidth	Lowest bandwidth of the route
K2	Load	Worst load on the route based on the packet rate
K3	Delay	Cumulative interface delay of the route
K4	Reliability	Worst reliability of the route
K5	MTU	Smallest MTU in the route [Not used in route calculation]

EIGRP Metric Calculation Formula

EIGRP uses five components in the metric calculation formula. If all five components are enabled, it uses the following formula to produce a single 32 bits metric.

$$\left[\left(K_1\cdot\text{Bandwidth}_E+\frac{K_2\cdot\text{Bandwidth}_E}{256-\text{Load}}+K_3\cdot\text{Delay}_E\right)\cdot\frac{K_5}{K_4+\text{Reliability}}\right]\cdot 256$$

As mentioned earlier, by default Load, Reliability, and MTU are disabled. If a component is disabled, EIGRP does not use its value in the formula. If we exclude the disabled components, the above-listed formula changes into the following formula.

by default Load, Reliability, and MTU are disabled. If a component is disabled, EIGRP does not use its value in the formula. If we exclude the disabled components, the above-listed formula changes into the following formula.

Metrics =((10^7/Least Bandwidth)+ Cumulative Delay)*256

Cisco uses following the configuration values for Bandwidth and Delay.

Bandwidth = 10^7/ least bandwidth of the route [*Lowest bandwidth from all interfaces between source and destination*.]

Delay = cumulative delay of the route [*Sum of all outgoing interfaces' delay.*]

Open Shortest Path First (OSPF)

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than RIP networks.

OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors.

Enabling OSPF

To enable OSPF, you need to create an OSPF routing process, specify the range of IP addresses associated with the routing process, then assign area IDs associated with that range of IP addresses.
To enable OSPF, perform the following detailed steps:

	Command	Purpose
Step 1	**router ospf** *process_id* **Example:** hostname(config)# router ospf 2	This creates an OSPF routing process, and the user enters router configuration mode for this OSPF process. The *process_id* is an internally used identifier for this routing process. It can be any positive integer. This ID does not have to match the ID on any other device; it is for internal use only. You can use a maximum of two processes.
Step 2	**network** *ip_address mask* **area** *area_id* **Example:** hostname(config)# router ospf 2 hostname(config-router)# network 10.0.0.0 255.0.0.0 area 0	This step defines the IP addresses on which OSPF runs and to define the area ID for that interface.

Wireless Networking Security and MAC Address Filtering

How an end user client with a WLAN NIC accesses a LAN

- To allow clients to find the AP easily, the AP periodically broadcasts beacons, announcing its (SSID) Service Set Identifier, data rates, and other WLAN information.
- SSID is a naming scheme for WLANs to allow an administrator to group WLAN devices together.
- To discover APs, clients will scan all channels and listen for the beacons from the AP(s). By default, the client will associate itself with the AP that has the strongest signal.
- When the client associates itself with the AP, it sends the SSID, its MAC address, and any other security information that the AP might require based on the authentication method configured on the two devices.
- Once connected, the client periodically monitors the signal strength of the AP to which it is connected.
- If the signal strength becomes too low, the client will repeat the scanning process to discover an AP with a stronger signal. This process is commonly called roaming.

SSID and MAC Address Filtering

When implementing SSIDs, the AP and client must use the same SSID value to authenticate. By default, the access point broadcasts the SSID value, advertising its presence, basically allowing anyone access to the AP. Originally, to prevent rogue devices from accessing the AP, the administrator would turn off the SSID broadcast function on the AP, commonly called SSID cloaking. To allow a client to learn the SSID value of the AP, the client would send a null string value in the SSID field of the 802.11 frame and the AP would respond; of course, this defeats the security measure since through this query process, a rogue device could repeat the same process and learn the SSID value.
Therefore, the APs were commonly configured to filter traffic based on MAC addresses. The administrator would configure a list of MAC addresses in a security table on the AP, listing those devices allowed access; however, the problem with this solution is that MAC addresses can be seen in clear-text in the airwaves. A rogue device can easily sniff the airwaves, see the valid MAC addresses, and change its MAC address to match one of the valid ones. This is called **MAC address spoofing.**

WEP

WEP (Wired Equivalent Privacy) was first security solutions for WLANs that employed encryption. WEP uses a static 64-bit key, where the key is 40 bits long, and a 24-bit initialization vector (IV) is used. IV is sent in clear-text. Because WEP uses RC4 as an encryption algorithm and the IV is sent in clear-text, WEP can be broken. To alleviate this problem, the key was extended to 104 bits with the IV value. However, either variation can easily be broken in minutes on laptops and computers produced today.

WPA

Wi-Fi Protected Access (WPA) was designed by the Wi-Fi Alliance as a temporary security solution to provide for the use of 802.1x and enhancements in the use of WEP until the 802.11i standard would be ratified. WPA can operate in two modes: personal and enterprise mode. Personal mode was designed for home or SOHO usage. A pre-shared key is used for authentication, requiring you to configure the same key on the clients and the AP. With this mode, no authentication server is necessary as it is in the official 802.1 x standards. Enterprise mode is meant for large companies, where an authentication server will centralize the authentication credentials of the clients.

WPA2

WPA2 is the IEEE 802.11i implementation from the Wi-Fi Alliance. Instead of using WEP, which uses the weak RC4 encryption algorithm, the much more secure Advanced Encryption Standard (AES)–counter mode CBC-MAC Protocol (CCMP) algorithm is used.

Conclusion – EIGRP is an efficient routing protocol by using DUAL algorithm. OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Wireless Networking Security and MAC Address Filtering is an important aspects of wireless network.