31277

ROUTING AND SWITCHING ESSENTIALS

STUDY NOTES

2019

UTS 2019

TABLE OF CONTENTS

TABLE OF CONTENTS 1
WEEK 1 – ROUTING CONCEPTS 2
WEEK 2 – IP ADDRESSING 7
WEEK 3 – SUBNETTING IP NETWORKS 9
WEEK 4 – STATIC ROUTING 10
WEEK 5 – DYNAMIC ROUTING 12
WEEK 6 – SWITCHED NETWORKS 15
WEEK 7 – VLANS 19
WEEK 8 – ACCESS CONTROL LISTS 22
WEEK 9 – DHCP AND NAT 24
WEEK 10 – IPv6 27
COMPLETE COMMAND LIST 31

WEEK 1 – ROUTING CONCEPTS

THE NETWORK LAYER

- OSI Layer 3 allows end devices to exchange data across a network
- Uses four processes to provide end-to-end transport:
  - Addressing of end devices – Unique IP addresses
  - Encapsulation – Adding IP header information to PDUs including source and destination IP addresses
  - Routing – Routers select the best path to direct packets
  - De-encapsulation – Destination hosts check if addresses match

ENCAPSULATING IP

- The transport layer segment is encapsulated by adding an IP header
- The IP header stays the same from the source to the destination host
- Layer by layer encapsulation enables the services at different layers to scale without affecting other layers

CHARACTERISTICS OF THE IP PROTOCOL

- Low overhead – Provides only the functions required to deliver a packet from the source to a destination without establishment of prior connection
- Tracking and managing flow of packets is performed by other layers (TCP)

BEST EFFORT DELIVERY

  - Considered "Unreliable" – Does not guarantee all packets will be received
  - No capability to manage and recover from undelivered, corrupt, or out of sequence packets, upper layer protocols must resolve these issues

MEDIA INDEPENDENT

  - Operates independently from the media that carries the data at lower layers of the protocol stack
  - Data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium
  - Network layer has a MTU (maximum transmission unit) size for PDUs

1.1 ROUTER INITIAL CONFIGURATION

ROUTER FUNCTIONS

- Connects one network to another network and routes traffic between
- Determines best route to the destination before forwarding traffic to the next router
- Routing table used to determine the most efficient path to reach the destination

ROUTERS ARE COMPUTERS

- A router is a specialized computer and requires the same components to operate:
  - Central Processing Unit (CPU)
  - Operating System (OS)
    - A Cisco Router uses the Cisco Internetwork Operating System (IOS)
  - Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)
    - Routers have specialised ports and network interface cards to interconnect devices to other networks

ROUTERS CHOOSE BEST PATHS

- The primary functions of a router are to:
  - Determine the best path to send packets
  - Forward packets toward their destination
- When a router receives a packet, the destination address is checked alongside the routing table to find the best path
  - When a match is found, the router encapsulates the packet into the DLL frame of the outgoing exit interface and then the packet is forwarded out that interface
- A router can handle different DLL frame encapsulations such as PPP

- Routers use the routing table like a map to discover the best path to a given network

PACKET FORWARDING MECHANISMS

- Routers support three packet-forwarding mechanisms:
  - Process switching
    - Slower and older
    - Packet is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table in order to determine the exit interface
    - Slow because it does this for every packet in a stream
  - Fast Switching
    - Common packet forwarding mechanism using a fast-switching cache to store the next-hop information
    - Packet is forwarded to the control plane where the CPU searches for a match in the fast-switching cache
    - If no match, it is forwarded to the exit interface
    - Packet flow information is also stored in the fast-switching cache for quick lookup
  - Cisco Express Forwarding – CEF
    - Fastest, most recent, and preferred method
    - CEF builds a Forwarding Information Base (FIB) and an adjacency table
    - Table entries are not packet-triggered like fast switching, but change-triggered when something changes in the network topology
    - FIB and adjacency tables contain all information a router would have to consider when forwarding a packet
    - FIB contains pre-computed reverse lookups, next hop information for routes including the interface and Layer 2 information

DEFAULT GATEWAYS

- Devices need an IP address, subnet mask, and default gateway for network access
- When a host sends a packet to a device that is on the same IP network, the packet is forwarded out the host interface to the destination device. The router does not need to get involved
- When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because the host device cannot communicate with devices outside of the local network
- The default gateway is the device that routes traffic from the local network to devices on remote networks
- Routers are also configured with their own default gateway

1.2 ROUTING DECISIONS

ROUTER SWITCHING FUNCTION

- The primary function of a router is to forward packets toward their destination
  - Uses a switching function to accept a packet on one interface and forward it out of another interface
  - The function also encapsulates the packets in the appropriate DLL frame
- When a router receives a packet from one network that is destined for another network, the router performs the following steps:
  - Step 1 – De-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet
  - Step 2 – Examines the destination IP address of the IP packet to find the best path in the routing table
  - Step 3 – If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface
- As a packet travels between devices, the Layer 3 IP addresses do not change, however the Layer 2 MAC addresses change at every hop

SENDING A PACKET

- For PC1 to send a packet to PC2, the following occurs:
  - PC1 determines if the destination IPv4 address is on the same network
  - Same network – PC1 will obtain the destination MAC address from its ARP cache or use an ARP request
  - Different network – PC1 forwards the packet to its default gateway
  - To determine the MAC address of the default gateway, PC1 checks its ARP table for the IPv4 address of the default gateway and its corresponding MAC address. An ARP request is sent if it is not found

FORWARDING TO THE NEXT HOP

- When R1 receives the Ethernet frame from PC1, the following occurs:
  - R1 examines the destination MAC address if it matches its receiving interface, it copies the frame into its buffer
  - R1 identifies the Ethernet Type field as 0x800 which indicates the Ethernet frame contains an IPv4 packet
  - R1 de-encapsulates the Ethernet frame, to determine the destination IPv4 address
  - If the destination address does not match any of the directly connected networks, R1 searches the routing table
  - When a route is found the IPv4 packet is encapsulated in a new Ethernet frame with the destination MAC address of the IPv4 address of the next-hop router
  - R1 must resolve the next-hop IPv4 address with a destination MAC address by ARP, if not in its ARP cache

PACKET ROUTING

- R2 examines the destination MAC address if it matches its receiving interface, it copies the frame into its buffer
- R2 determines that that frame contains an IPv4 packet in the data portion and de-encapsulates the Ethernet frame
- The routing table is searched to find a corresponding route for the destination IPv4 address
- If the exit interface is not Ethernet, R2 does not have to resolve the next-hop IPv4 address with a MAC address
- The packet is encapsulated into a new DL frame used by the exit interface and sent out the Serial 0/0/0 exit interface
- There are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of broadcast

REACHING THE DESTINATION

- R3 copies the data link PPP frame into its buffer
- R3 de-encapsulates the data link PPP frame
- R3 searches the routing table for the destination
- If the destination is directly connected, packet can be sent directly
- If the exit interface is a directly connected Ethernet network, R3 must resolve the destination IPv4 address of the packet with a destination MAC address by either finding it in its ARP cache or sending out an ARP request

ROUTING DECISIONS

- A key function of routers is to determine the best path to send packets
- A routing table search results in one of three path determinations:
  - Directly connected network – Destination IP address belongs to a network that is directly connected to the router, the packet is forwarded out of that interface
  - Remote network – Destination IP address of the packet belongs to a remote network, the packet is forwarded to another router
  - No route determined – Destination IP address does not belong to a connected network and not in the routing table, packet is sent to Gateway of Last Resort

BEST PATH

- Determining the best path to a destination network involves the evaluation of multiple paths and selecting the optimum or shortest path to reach it
- Metric – Value that is used to measure the distance to a given network
- The best path to a network is the path with the lowest metric
- Each dynamic routing protocol has its own rules to update a routing table:
  - Routing Information Protocol (RIP) – Hop count
  - Open Shortest Path First (OSPF) – Cisco's cost based cumulative bandwidth
  - Enhanced Interior Gateway Routing Protocol (EIGRP) – Bandwidth, delay, load, reliability

LOAD BALANCING

- If a router has two or more paths with identical metrics to the same destination, the router will forward the packets using both paths equally
- The routing table contains a single destination network but has multiple exit interfaces – One for each equal cost path – Known as equal cost load balancing
- If configured correctly, load balancing can increase effectiveness and performance
- Equal cost load balancing can be configured to use dynamic and static routing

- EIGRP supports unequal cost load balancing

ADMINISTRATIVE DISTANCE

- Routing table may have multiple route sources for the same destination network
- Each routing protocol may prefer a different path to reach the same destination
- The Cisco IOS uses what is known as the administrative distance (AD) to determine which route to install in the routing table
- The AD represents the "trustworthiness" of the route. Lower = more trustworthy

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

1.3 ROUTER OPERATION

THE ROUTING TABLE

- The routing table of a router stores information about:
  - Directly connected routes – Obtained from the active router interfaces
  - Remote routes – Networks connected to other routers that are learned from dynamic routing protocols or are statically configured
- Data file in RAM storing information about connected and remote networks
- The routing table contains next hop associations telling the router what the next hop is for a destination network

ROUTING TABLE SOURCES

- On a Cisco router, the **show ip route** command can be used to display the IPv4 routing table
- Additional route information in the routing table includes: How the route was learned, how long the route has been in the table, and which interface to send out of to reach a destination
- Sources of the routing table entries are identified by a code:
  - L – Local Route interfaces (router)
  - C – Directly connected interfaces
  - S – Static routes
  - D – Learned dynamically from another router using EIGRP routing
  - O – Learned dynamically from another router OSPF routing

REMOTE NETWORK ROUTING ENTRIES

- Routing table entries contain:
  - Route source – How the route was learned
  - Destination network – Address of the remote network
  - Administrative distance – Trustworthiness of the route
  - Metric – Value assigned to reach the remote network; lower the better
  - Next-hop – The IPv4 address of the next router to forward the packet to
  - Route timestamp – How much time has passed since the route was learned
  - Outgoing interface – Exit interface to forward packet out of

DIRECTLY CONNECTED INTERFACES

- A new router without any configured interfaces will have an empty routing table
- Before interface is considered up/up and added to routing table, interface must:
  - Be assigned a valid IPv4 or IPv6 address
  - Be activated with the no shutdown command
  - Receive a carrier signal from another device such as a router, switch, or host
- When the interface is up, the network interface is added to the routing table

DIRECTLY CONNECTED ROUTING TABLE ENTRIES

- An active directly connected interface creates two routing table entries:
  - Source "C" identifies the route as a directly connected network
  - Source "L" identifies the IPv4 address assigned to the router's interface
- The table entry shows the destination network and the outgoing interface