IPv4 Routing & LAN Switching

Fundamental Concepts

- **Networking Basics:**
  - A network is a collection of interconnected devices that can communicate with each other.
  - The Internet is a global network of interconnected networks.
  - IP addresses are used to identify devices on a network. IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses.
  - Subnetting divides a network into smaller, more manageable subnetworks.
  - The OSI (Open Systems Interconnection) model and TCP/IP (Transmission Control Protocol/Internet Protocol) model provide frameworks for understanding network communication.
- **Routers:**
  - A router is a networking device that forwards data packets between networks.
  - Routers operate at Layer 3 (Network Layer) of the OSI model.
  - Routers use routing tables to determine the best path for forwarding packets.
  - Routers can connect different types of networks, such as LANs (Local Area Networks) and WANs (Wide Area Networks).
- **Routing:**
  - Routing is the process of determining the best path for data packets to travel from source to destination.
  - Routing decisions are based on network topology, routing protocols, and routing metrics.
  - Routing involves building and maintaining routing tables.
  - **Forwarding:** The act of taking a packet and sending it out to the correct interface based on the routing table.

Routing Protocols

- Routing protocols are used by routers to exchange routing information and build routing tables.
- Routing protocols can be classified as interior gateway protocols (IGPs) or exterior gateway protocols (EGPs).
- IGPs are used within an autonomous system (AS), while EGPs are used between ASs.

- **Intra-Domain Routing Protocols (IGPs):**

- **RIP (Routing Information Protocol):**
  - A distance-vector routing protocol.
  - Uses hop count as the routing metric.
  - Updates are broadcasted every 30 seconds.
  - Limited to a maximum hop count of 15.
  - Simple to configure, but not suitable for large networks.
  - **RIPv2:** Version 2 of RIP, allows for VLSM and authentication.

- **OSPF (Open Shortest Path First):**
  - A link-state routing protocol.
  - Uses Dijkstra's algorithm to calculate the shortest path.
  - Uses cost as the routing metric, which is based on link bandwidth.
  - Updates are triggered by network changes.
  - Scalable and suitable for large networks.

  - **Link-state vs. Distance-vector:**
    - Distance-vector protocols (like RIP) share their entire routing table with neighbours.
    - Link-state protocols (like OSPF) share information about their directly connected links with all routers in the area.

- **Inter-Domain Routing Protocols (EGPs):**
  - **BGP (Border Gateway Protocol):**
    - A path-vector routing protocol.
    - Used to exchange routing information between ASs.
    - Uses path attributes to determine the best path.
    - Highly scalable and used for Internet routing.
    - **Path-vector:** BGP shares the path of AS numbers that a route traverses, allowing for policy based routing.

IPv4 Routing

- **IPv4 Addressing:**
  - IPv4 addresses are 32-bit addresses, represented in dotted-decimal notation (e.g., 192.168.1.1).
  - IPv4 addresses are divided into network and host portions.
  - Subnet masks are used to determine the network portion of an IP address.
  - Classes A, B, and C are the original IPv4 address classes.
  - CIDR (Classless Inter-Domain Routing) allows for more flexible allocation of IP addresses.

- **Routing Process:**
  - When a router receives a packet, it examines the destination IP address.
  - The router searches its routing table for the best match.
  - If a match is found, the router forwards the packet to the next hop.
  - If no match is found, the router drops the packet.
  - **Longest Prefix Match:** When a router is looking up a destination IP, it uses the longest prefix match. Meaning, it uses the most specific route in its routing table.

- **Static Routing:**
  - Manually configured routes.
  - Simple to configure for small networks.
  - Not suitable for large or dynamic networks.
  - Useful for default routes or specific network connections.
- **Dynamic Routing:**
  - Routes are automatically learned and updated by routing protocols.
  - Scalable and suitable for large networks.
  - Requires more configuration than static routing.

LAN Switching

- **LAN Switching Overview:**
  - Switches operate at Layer 2 (Data Link Layer) of the OSI model.
  - Switches forward data frames based on MAC addresses.
  - Switches create separate collision domains for each port.
  - Switches can create VLANs (Virtual LANs) to segment a network.
- **VLANs (Virtual LANs):**
  - VLANs logically divide a physical network into multiple broadcast domains.
  - VLANs improve network security and performance.
  - VLANs allow for flexible network design.
  - **VLAN Routing:**
    - Inter-VLAN routing is required for communication between VLANs.
    - Inter-VLAN routing can be performed by a router or a Layer 3 switch.

        - **Router-on-a-stick:** One method of inter-VLAN routing, where a router is connected to a switch via a trunk link.
        - **Layer 3 Switch:** A switch that can perform routing functions.

- **STP (Spanning Tree Protocol):**
    - Prevents Layer 2 loops in a switched network.
    - Selects a root bridge and blocks redundant paths.
    - Ensures a loop-free topology.
    - **STP Variants:** RSTP (Rapid STP), MSTP (Multiple STP).
    - **Bridge Protocol Data Units (BPDUs):** STP uses BPDUs to communicate and determine the network topology.

- **LAN Switching and IPv4 Routing Combined:**
    - Routers can be used to connect different VLANs, enabling communication between them.
    - Layer 3 switches combine the functions of a switch and a router, providing high-performance inter-VLAN routing.
    - The combination of switching and routing is essential for building scalable and efficient networks.

- **VTP (VLAN Trunking Protocol):**
    - Used to propagate VLAN information throughout a switched network.
    - Simplifies VLAN management.
    - Reduces the risk of VLAN configuration errors.
    - **VTP Modes:** Server, Client, Transparent.

VTP Configuration Steps

Step 1: Enter Global Configuration Mode

Switch> enable

Switch# configure terminal

Step 2: Set the VTP Domain Name

Assign a domain to group switches that share VLAN information. All switches in the domain must match.

Switch(config)# vtp domain MYDOMAIN

Replace MYDOMAIN with your desired domain name (e.g., "LabNetwork").

Step 3: Set the VTP Mode

Choose the appropriate mode for the switch:

- **Server Mode** (Default)
- Switch(config)# vtp mode server
- **Client Mode**
- Switch(config)# vtp mode client
- **Transparent Mode**
- Switch(config)# vtp mode transparent
- **Off Mode** (Disables VTP if supported)
- Switch(config)# vtp mode off

Step 4: Set a VTP Password (Optional)

Enhances security by ensuring only authorized switches join the VTP domain.

Switch(config)# vtp password MYSECRET

Replace MYSECRET with your password.

Step 5: Configure Trunk Links

VTP advertisements are sent over trunk links. Configure the interface as a trunk:

Switch(config)# interface gigabitEthernet0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

- *Replace gigabitEthernet0/1 with the correct interface.*
- *Use dot1q (IEEE 802.1Q) or isl (Cisco ISL) depending on network requirements.*

Step 6: Exit and Verify Configuration

Exit configuration mode and check VTP status:

Switch(config)# exit

Switch# show vtp status

Output includes:

- VTP Domain Name
- VTP Mode
- VTP Version (1, 2, or 3)
- Configuration Revision Number
- Number of VLANs

Additional Configuration Options

1. **Set VTP Version**
2. Switch(config)# vtp version 2

Version 2 supports Token Ring VLANs, while Version 3 adds private VLANs and better security.

3. **Enable VTP Pruning** (Reduces unnecessary VLAN traffic on trunks)
4. Switch(config)# vtp pruning

5. **Restrict VLANs on a Trunk** (Limit allowed VLANs)
6. Switch(config-if)# switchport trunk allowed vlan 10,20,30

Questions:

Q: When do we need routing protocols?

A: We need routing protocols when you have a network with multiple devices and need to ensure data packets are efficiently and reliably transmitted from one device to another, especially when the network topology is dynamic or complex.

Q: Protocols used in static routing.

A: Static routing involves manually configuring routes on routers, where the network administrator defines the path data packets should take, rather than relying on dynamic routing protocols that automatically update routes based on network conditions.

Q: Protocols used in Dynamic routing.

Dynamic routing protocols, which automatically update routing tables based on network changes, are categorized as Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs), with common examples including RIP, OSPF, EIGRP, and BGP.