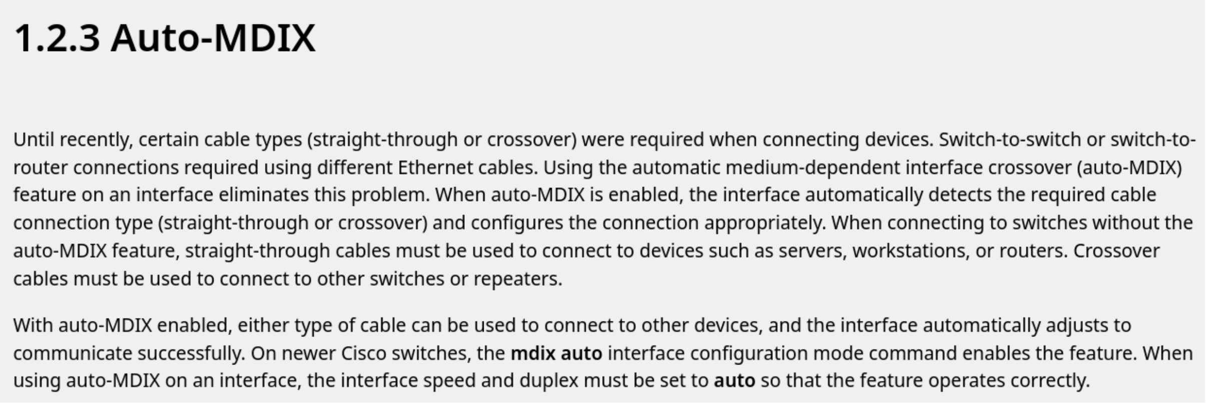


1.2.3 Auto-MDIX

Until recently, certain cable types (straight-through or crossover) were required when connecting devices. Switch-to-switch or switch-to-router connections required using different Ethernet cables. Using the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface eliminates this problem. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. When connecting to switches without the auto-MDIX feature, straight-through cables must be used to connect to devices such as servers, workstations, or routers. Crossover cables must be used to connect to other switches or repeaters.

With auto-MDIX enabled, either type of cable can be used to connect to other devices, and the interface automatically adjusts to communicate successfully. On newer Cisco switches, the **mdix auto** interface configuration mode command enables the feature. When using auto-MDIX on an interface, the interface speed and duplex must be set to **auto** so that the feature operates correctly.

Input errors” is the sum of all errors in datagrams that were received on the interface being examined. This includes runts, giants, CRC, no buffer, frame, overrun, and ignored counts. The reported input errors from the **show interfaces** command include the following:

- **Runt Frames** - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts. Malfunctioning NICs are the usual cause of excessive runt frames, but they can also be caused by collisions.
- **Giants** - Ethernet frames that are larger than the maximum allowed size are called giants.
- **CRC errors** - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error. Common causes include electrical interference, loose or damaged connections, or incorrect cabling. If you see many CRC errors, there is too much noise on the link and you should inspect the cable. You should also search for and eliminate noise sources.

“Output errors” is the sum of all errors that prevented the final transmission of datagrams out the interface that is being examined. The reported output errors from the **show interfaces** command include the following:

- **Collisions** - Collisions in half-duplex operations are normal. However, you should never see collisions on an interface configured for full-duplex communication.
- **Late collisions** - A late collision refers to a collision that occurs after 512 bits of the frame have been transmitted. Excessive cable lengths are the most common cause of late collisions. Another common cause is duplex misconfiguration. For example, you could have one end of a connection configured for full-duplex and the other for half-duplex. You would see late collisions on the interface that is configured for half-duplex. In that case, you must configure the same duplex setting on both ends. A properly designed and configured network should never have late collisions.

Telnet

Telnet uses TCP port 23. It is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. A threat actor can monitor packets using Wireshark. For example, in the figure the threat actor captured the username **admin** and password **ccna** from a Telnet session.

SSH

Secure Shell (SSH) is a secure protocol that uses TCP port 22. It provides a secure (encrypted) management connection to a remote device. SSH should replace Telnet for management connections. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices.

Store-and-Forward Switching

- The switch **receives the entire packet**, **checks for errors** (CRC check), and then forwards it.
- **More reliable** since it drops corrupted packets.
- **Slower** due to full packet buffering and error-checking.
- Used in **enterprise networks and data centers** where accuracy is critical.

Cut-Through Switching

- The switch **forwards the packet as soon as it reads the destination MAC address** (before receiving the full packet).
- **Faster** but may forward corrupted or incomplete packets.
- Used in **low-latency applications**, like gaming and financial trading.

Collision Domains

If a switch is connected to a **modern device**, it operates in **full-duplex** (no collisions). If connected to an **old hub**, it **downgrades to half-duplex**, meaning it enters a **collision domain** where devices must take turns sending data.

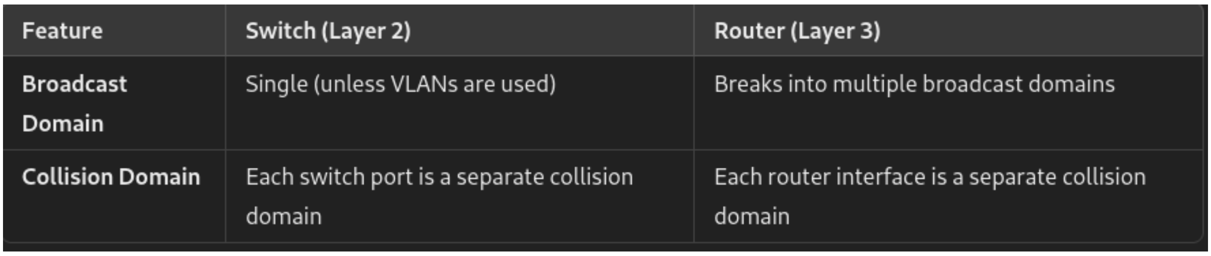
Broadcast Domain (Layer 2 - Switches)

A **broadcast domain** is the area where a broadcast frame (like an ARP request) is forwarded to all devices.

- **All ports on a switch** (or interconnected switches) belong to the **same broadcast domain** unless VLANs are used.
- **Issue:** Excessive broadcast traffic can slow down network performance.
- **Fix:** A **router or VLAN segmentation** can break a large broadcast domain into smaller, more efficient ones.

Example:

- A **single switch with 10 devices → 1 broadcast domain**
- **Two switches connected together** → Still **1 broadcast domain**
- **Router in between → 2 separate broadcast domains**



Feature	Switch (Layer 2)	Router (Layer 3)
Broadcast Domain	Single (unless VLANs are used)	Breaks into multiple broadcast domains
Collision Domain	Each switch port is a separate collision domain	Each router interface is a separate collision domain

Frame Forwarding

The decision on how a switch forwards traffic is based on the flow of that traffic. The term ingress describes the port where a frame enters a device. The term egress describes the port that frames will use when leaving the device. An Ethernet frame will never be forwarded out the port where it entered. For a switch to know which port to use to transmit a frame, it must first learn which devices exist on each port. As the switch learns the relationship of ports to devices, it builds a table called a MAC address table. Every frame that enters a switch is checked for new information to learn by examining the source MAC address of the frame and port number where the frame entered the switch. If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. Switch forwarding methods include store-and-forward and cut-through. Store-and-forward uses error-checking and automatic buffering. Cut-through does not error check. Instead it performs rapid frame switching. This means the switch can make a forwarding decision as soon as it has looked up the destination MAC address of the frame in its MAC address table.

Switching Domains

If an Ethernet switch port is operating in half-duplex, each segment is in its own collision domain. There are no collision domains when switch ports are operating in full-duplex. By default, Ethernet switch ports will autonegotiate full-duplex when the adjacent device can also operate in full-duplex. A collection of interconnected switches forms a single broadcast domain. Only a network layer device, such as a router, can divide a Layer 2 broadcast domain. The Layer 2 broadcast domain is referred to as the MAC broadcast domain. The MAC broadcast domain consists of all devices on the LAN that receive broadcast frames from a host. When a switch receives a broadcast frame, it forwards the frame out each of its ports, except the ingress port where the broadcast frame was received. Each device connected to the switch receives a copy of the broadcast frame and processes it. Switches can: interconnect LAN segments, use a MAC address table to determine egress ports, and can lessen or eliminate collisions entirely. Characteristics of switches that alleviate network congestion are fast port speeds, fast internal switching, large frame buffers, and high port density.

VLANs

Virtual LANs (VLANs) provide segmentation and organizational flexibility in a switched network. A group of devices within a VLAN communicate as if each device was attached to the same cable. VLANs are based on logical connections, instead of physical connections.

As shown in the figure, VLANs in a switched network enable users in various departments (i.e., IT, HR, and Sales) to connect to the same network regardless of the physical switch being used or location in a campus LAN.

What is a VLAN (Virtual Local Area Network)?

A **VLAN (Virtual Local Area Network)** is a **logical segmentation** of a physical network into multiple isolated networks. VLANs allow devices to be grouped together based on **function, department, or security needs** rather than physical location.

Key Features of VLANs:

1. **Logical Segmentation** – Devices in a VLAN can communicate as if they were in the same physical network, even if they are on different switches.

2. **Improves Security** – VLANs isolate traffic, preventing unnecessary access between devices in different VLANs.

3. **Reduces Broadcast Traffic** – VLANs limit broadcast domains, reducing unnecessary network congestion.

4. **Enhances Performance** – Less congestion due to smaller, more manageable network segments.

5. **Flexibility** – VLANs can be reconfigured via software without physically changing network cables.

Types of VLANs

1. **Data VLAN** – Used to carry only user-generated traffic (e.g., PCs, printers).

2. **Voice VLAN** – Separates VoIP (Voice over IP) traffic from data traffic for better call quality.

3. **Management VLAN** – Used for remote administration of network devices.

4. **Native VLAN** – The default VLAN assigned to untagged traffic on a trunk link.

5. **Default VLAN** – The VLAN that all switch ports belong to by default (usually VLAN 1).

What is a VLAN Trunk?

A **VLAN Trunk** is a connection between network devices (typically switches) that **carries multiple VLANs over a single physical link**. It allows VLAN traffic to pass between switches while maintaining VLAN separation using **VLAN tagging (IEEE 802.1Q protocol)**.

VLAN Identifier (VLAN ID)

A **VLAN Identifier (VLAN ID)** is a unique number assigned to each VLAN in a network to distinguish traffic belonging to different VLANs.

🔹 What is a VLAN ID?

- VLAN IDs are **12-bit numbers** (0-4095) used in **IEEE 802.1Q tagging** to classify network traffic.
- Each **VLAN** is assigned a **unique VLAN ID** so that network devices can differentiate between traffic from multiple VLANs.
- VLAN IDs are added to **Ethernet frames** when they traverse **trunk links** between switches.

VLAN Tagging (IEEE 802.1Q)

🔹 What is VLAN Tagging?

- VLAN tagging is a process of adding a **VLAN identifier (Tag)** to an Ethernet frame.
- It ensures that switches and routers know which VLAN the frame belongs to when moving across a **trunk link**.
- The industry-standard protocol for VLAN tagging is **IEEE 802.1Q**.

🔹 How Does It Work?

- Normally, an Ethernet frame doesn’t contain VLAN information.

- When a frame is sent **over a trunk port**, a **4-byte VLAN tag** is added to the frame's header.
- This tag includes the **VLAN ID (VID)**, which tells the receiving switch which VLAN the frame belongs to.
- When the frame reaches its destination switch, the **VLAN tag is removed** before being forwarded to the endpoint.

🔹 **Example of VLAN Tagging:**

- A switch receives a frame from VLAN **10** and sends it over a **trunk link** to another switch.
- The **802.1Q tag (VLAN 10)** is added.
- The receiving switch **removes the tag** and delivers the frame to devices in VLAN 10.

Voice VLAN Tagging

Voice VLAN tagging is a mechanism that ensures high-priority handling of **VoIP (Voice over IP) traffic** in a network. It helps separate voice traffic from regular data traffic, ensuring **low latency, jitter, and packet loss** for VoIP calls.

What is DTP?

DTP (Dynamic Trunking Protocol) is a **Cisco proprietary protocol** used for **negotiating trunk links** between Cisco switches. It allows switches to automatically **form trunk connections** without requiring manual configuration.

Purpose: Automates the process of enabling or disabling trunking on a switch port.
Scope: Works **only on Cisco switches** (not supported by non-Cisco devices).

Overview of VLANs

Virtual LANs (VLANs) are a group of devices that can communicate as if each device was attached to the same cable. VLANs are based on logical instead of physical connections. Administrators use VLANs to segment networks based on factors such as function, team, or application. Each VLAN is considered a separate logical network. Any switch port can belong to a VLAN. A VLAN creates a logical broadcast domain that can span multiple physical

LAN segments. VLANs improve network performance by separating large broadcast domains into smaller ones. Each VLAN in a switched network corresponds to an IP network; therefore, VLAN design must use a hierarchical network-addressing scheme. Types of VLANs include the default VLAN, data VLANs, the native VLAN, management VLANs. and voice VLANs.

VLANs in a Multi-Switched Environment

A VLAN trunk does not belong to a specific VLAN. It is a conduit for multiple VLANs between switches and routers. A VLAN trunk is a point-to-point link between two network devices that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. When VLANs are implemented on a switch, the transmission of unicast, multicast, and broadcast traffic from a host in a particular VLAN are restricted to the devices that are in that VLAN. VLAN tag fields include the type, user priority, CFI and VID. Some devices add a VLAN tag to native VLAN traffic. If an 802.1Q trunk port receives a tagged frame with the VID that is the same as the native VLAN, it drops the frame. A separate voice VLAN is required to support VoIP. QoS and security policies can be applied to voice traffic. Voice VLAN traffic must be tagged with an appropriate Layer 2 CoS priority value.

VLAN Configuration

Different Cisco Catalyst switches support various numbers of VLANs including normal range VLANs and extended range VLANs. When configuring normal range VLANs, the configuration details are stored in flash memory on the switch in a file called vlan.dat. Although it is not required, it is good practice to save running configuration changes to the startup configuration. After creating a VLAN, the next step is to assign ports to the VLAN. There are several commands for defining a port to be an access port and assigning it to a VLAN. VLANs are configured on the switch port and not on the end device. An access port can belong to only one data VLAN at a time. However, a port can also be associated to a voice VLAN. For example, a port connected to an IP phone and an end device would be associated with two VLANs: one for voice and one for data. After a VLAN is configured, VLAN configurations can be validated using Cisco IOS **show** commands. If the switch access port has been incorrectly assigned to a VLAN, then simply re-enter the **switchport access vlan** *vlan-id* interface configuration command with the correct VLAN ID. The **no vlan** *vlan-id* global configuration mode command is used to remove a VLAN from the switch vlan.dat file.

VLAN Trunks

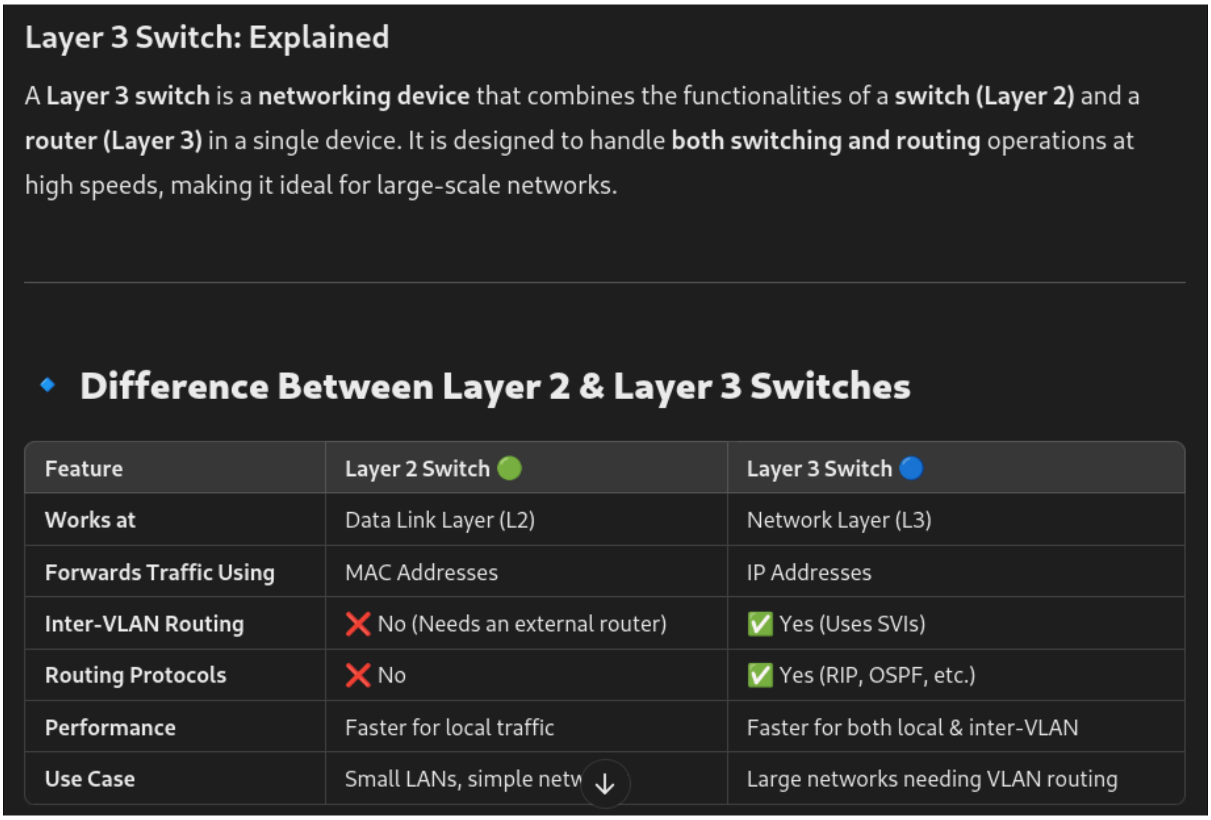
A VLAN trunk is an OSI Layer 2 link between two switches that carries traffic for all VLANs. There are several commands to configure the interconnecting ports. To verify VLAN trunk configuration use the **show interfaces** *interface-ID* **switchport** command. Use the **no switchport trunk allowed vlan** and the **no switchport trunk native vlan** commands to remove the allowed VLANs and reset the native VLAN of the trunk.

Dynamic Trunking Protocol

An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis only, between network devices. DTP is a Cisco proprietary protocol that manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP. To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. The **switchport mode** command has additional options for negotiating the interface mode including access, dynamic auto, dynamic desirable, and trunk. To verify the current DTP mode, issue the **show dtp interface** command.

Router-on-a-Stick: Inter-VLAN Routing with a Router on a Switch

A **router-on-a-stick** (RoaS) configuration is a method of **inter-VLAN routing**, where a **single router** is used to route traffic between multiple VLANs on a switch. It involves using a **trunk link** between the router and the switch, with **subinterfaces** configured on the router.



Layer 3 Switch: Explained

A **Layer 3 switch** is a **networking device** that combines the functionalities of a **switch (Layer 2)** and a **router (Layer 3)** in a single device. It is designed to handle **both switching and routing** operations at high speeds, making it ideal for large-scale networks.

🔹 Difference Between Layer 2 & Layer 3 Switches

Feature	Layer 2 Switch 🟢	Layer 3 Switch 🔵
Works at	Data Link Layer (L2)	Network Layer (L3)
Forwards Traffic Using	MAC Addresses	IP Addresses
Inter-VLAN Routing	❌ No (Needs an external router)	✅ Yes (Uses SVIs)
Routing Protocols	❌ No	✅ Yes (RIP, OSPF, etc.)
Performance	Faster for local traffic	Faster for both local & inter-VLAN
Use Case	Small LANs, simple netw	Large networks needing VLAN routing

Spanning Tree Algorithm (STA) and Spanning Tree Protocol (STP) Overview

STP (Spanning Tree Protocol) **prevents loops** in **Layer 2 networks (Ethernet LANs)** by creating a **loop-free topology**. It achieves this by using the **Spanning Tree Algorithm (STA)**, which follows a **four-step process**:

🔹 1. Elect the Root Bridge

- **What is the Root Bridge?**
  - The **Root Bridge** is the **central reference point** in STP.
  - All switches determine the **shortest path** to the Root Bridge.
- **How is it Elected?**

    - **Bridge Protocol Data Units (BPDUs)** are sent between switches.
    - Each BPDU contains a **Bridge ID (BID)**, which includes:
        - **Priority Value** (default: 32768)
        - **Extended System ID** (VLAN ID)
        - **MAC Address** (used as a tiebreaker)
    - The switch with the **lowest BID** (smallest priority + MAC) **becomes the Root Bridge**.

🔹 2. Elect the Root Ports

- **What is a Root Port?**
    - Each **non-root switch** selects **one Root Port** (RP).
    - The **Root Port** is the **fastest, least-cost** path to the Root Bridge.
- **How is it Selected?**
    - The **port with the lowest Path Cost** to the Root Bridge is elected as the Root Port.

- Path Cost is based on the **link speed**:

Link Speed	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4

10 Gbps	2

🔹 3. Elect Designated Ports

- **What is a Designated Port?**
    - A **Designated Port (DP)** is the **fastest** forwarding port on a **network segment**.
    - **Only one Designated Port exists per network segment**.
- **How is it Selected?**
    - The switch with the **lowest BID** wins.
    - If a tie occurs, the **lowest MAC address** wins.
    - **Designated Ports remain in the forwarding state**.

🔹 4. Elect Alternate (Blocked) Ports

- **What is an Alternate (Blocked) Port?**
    - Any port **not selected as a Root Port or Designated Port** becomes a **Blocked Port**.
    - **Blocked Ports do NOT forward traffic**, preventing loops.
- **How is it Selected?**

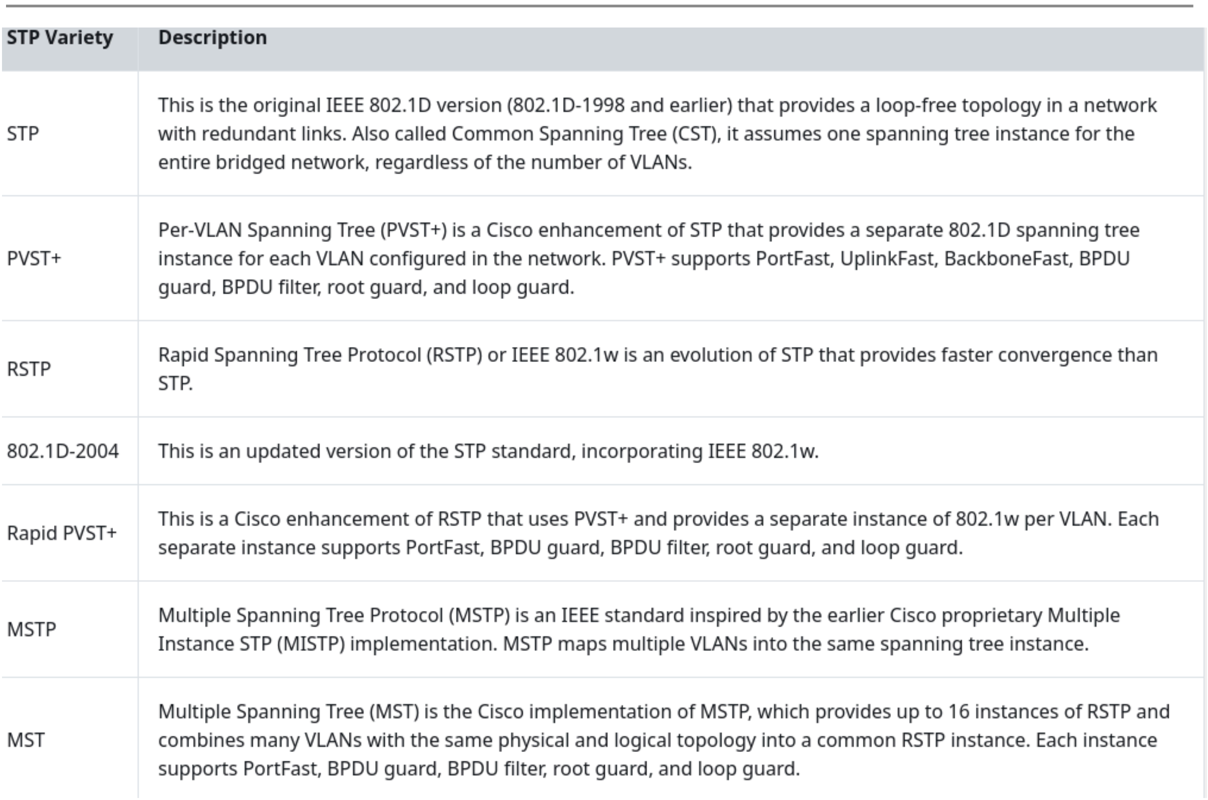
    - If multiple ports lead to the same network segment, the one with the **higher path cost** or **higher BID** is **blocked**.

🔹 BPDU (Bridge Protocol Data Units)

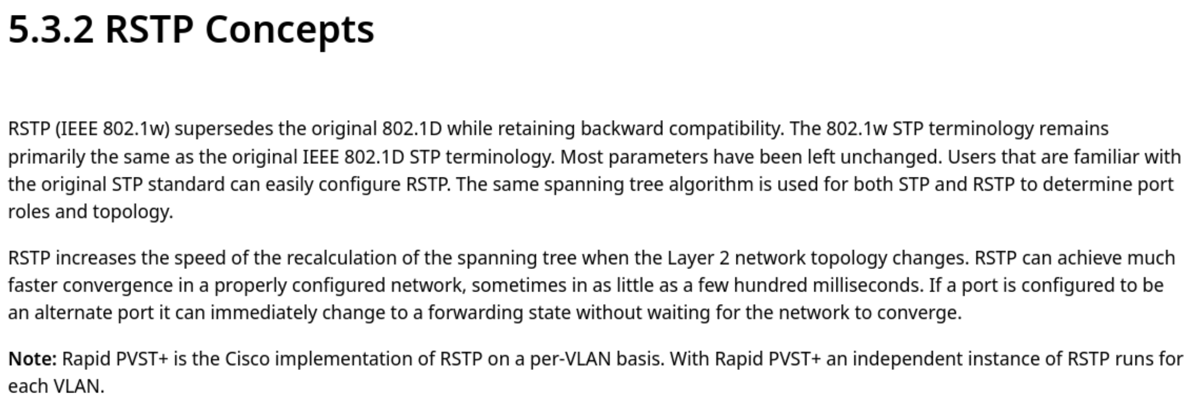
- **What are BPDUs?**
    - BPDUs are special STP messages **sent between switches** to:
        - Elect the **Root Bridge**.
        - Determine the **Root Port**.
        - Decide the **Designated Ports**.
        - Identify **Alternate (Blocked) Ports**.
- **What's Inside a BPDU?**
    - **Bridge ID (BID)** (Priority + MAC)
    - **Path Cost**
    - **Root ID (Root Bridge Information)**

What is BPDU?

A **BPDU (Bridge Protocol Data Unit)** is a **special network message** used by **Spanning Tree Protocol (STP)** to **prevent loops** in a Layer 2 Ethernet network.



STP Variety	Description
STP	This is the original IEEE 802.1D version (802.1D-1998 and earlier) that provides a loop-free topology in a network with redundant links. Also called Common Spanning Tree (CST), it assumes one spanning tree instance for the entire bridged network, regardless of the number of VLANs.
PVST+	Per-VLAN Spanning Tree (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
RSTP	Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1w is an evolution of STP that provides faster convergence than STP.
802.1D-2004	This is an updated version of the STP standard, incorporating IEEE 802.1w.
Rapid PVST+	This is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. Each separate instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.
MSTP	Multiple Spanning Tree Protocol (MSTP) is an IEEE standard inspired by the earlier Cisco proprietary Multiple Instance STP (MISTP) implementation. MSTP maps multiple VLANs into the same spanning tree instance.
MST	Multiple Spanning Tree (MST) is the Cisco implementation of MSTP, which provides up to 16 instances of RSTP and combines many VLANs with the same physical and logical topology into a common RSTP instance. Each instance supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.



5.3.2 RSTP Concepts

RSTP (IEEE 802.1w) supersedes the original 802.1D while retaining backward compatibility. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged. Users that are familiar with the original STP standard can easily configure RSTP. The same spanning tree algorithm is used for both STP and RSTP to determine port roles and topology.

RSTP increases the speed of the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. If a port is configured to be an alternate port it can immediately change to a forwarding state without waiting for the network to converge.

Note: Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. With Rapid PVST+ an independent instance of RSTP runs for each VLAN.

Purpose of STP

Redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops. A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices. This results in the network becoming unusable. Unlike the Layer 3 protocols, IPv4 and IPv6, Layer 2 Ethernet does not include a mechanism to recognize and eliminate endlessly looping frames. Ethernet LANs require a loop-free topology with a single path between any two devices. STP is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. Without STP, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly, bringing down a network. A broadcast storm is an abnormally high number of broadcasts overwhelming the network during a specific amount of time. Broadcast storms can disable a network within seconds by overwhelming switches and end devices. STP is based on an algorithm invented by Radia Perlman. Her spanning tree algorithm (STA) creates a loop-free topology by selecting a single root bridge where all other switches determine a single least-cost path.

STP Operations

Using the STA, STP builds a loop-free topology in a four-step process: elect the root bridge, elect the root ports, elect designated ports, and elect alternate (blocked) ports. During STA and STP functions, switches use BPDUs to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports. Each BPDU contains a BID that identifies the switch that sent the BPDU. The BID is involved in making many of the STA decisions including root bridge and port roles. The BID contains a priority value, the MAC address of the switch, and an extended system ID. The lowest BID value is determined by the combination of these three fields. The switch with the lowest BID will become the root bridge. Because the default BID is 32,768 it is possible for two or more switches to have the same priority. In this scenario, where the priorities are the same, the switch with the lowest MAC address will become the root bridge. When the root bridge has been elected for a given spanning tree instance, the STA determines the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge. After the root bridge has been determined the STA algorithm selects the root port. The root port is the port closest to the root bridge in terms of overall cost, which is called the internal root path cost. After each switch selects a root port, switches will select designated ports. The designated port is a port on the segment (with two switches) that has the internal root path cost to the root bridge. If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports and backup ports are in discarding or blocking state to prevent loops. When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria: lowest sender BID, then the lowest sender port priority, and finally the lowest sender port ID. STP convergence requires three timers: the hello timer, the forward delay timer, and the max age timer. Port states are blocking, listening, learning, forwarding, and disabled. In PVST versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs.

Evolution of STP.

The term Spanning Tree Protocol and the acronym STP can be misleading. STP is often used to refer to the various implementations of spanning tree, such as RSTP and MSTP. RSTP is an evolution of STP that provides faster convergence than STP. RSTP port states are learning, forwarding and discarding. PVST+ is a Cisco enhancement of STP that provides a separate spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard. Cisco switches running IOS 15.0 or later, run PVST+ by default. Rapid PVST+ is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN. When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, bypassing the STP listening and learning states and avoiding a 30 second delay. Use PortFast on access ports to allow devices connected to these ports, such as DHCP clients, to access the network immediately, rather than waiting for STP to converge on each VLAN. Cisco switches support a feature called BPDU guard which immediately puts the switch port in an error-disabled state upon receipt of any BPDU to protect against potential loops. Over the years, Ethernet LANs went from a few interconnected switches that were connected to a single router, to a sophisticated hierarchical network design. Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements as part of RSTP and MSTP. Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch.

What is PortFast?

PortFast is a Cisco feature that allows a switch port to bypass the normal **Spanning Tree Protocol (STP) states** and immediately transition **to the forwarding state**.

Why Use PortFast?

STP normally makes a port go through **Blocking → Listening → Learning** before reaching **Forwarding**. This delay (which can take **30-50 seconds**) can cause issues for end devices like **PCs, printers, or servers** that need an immediate network connection.

PortFast **skips these delays** and makes the port **active immediately**.

Where is PortFast Used?

PortFast should **only be enabled on access ports** (ports connected to end devices) and **never on trunk ports** (ports connecting switches), because enabling it on a trunk port **can create network loops**.

Link Aggregation

A link aggregation technology is needed that allows redundant links between devices that will not be blocked by STP. That technology is known as EtherChannel.

EtherChannel is a link aggregation technology that groups multiple physical Ethernet links together into one single logical link. It is used to provide fault-tolerance, load sharing, increased bandwidth, and redundancy between switches, routers, and servers.

"EtherChannel" links—basically, a way to bundle multiple physical links between switches into one logical connection for higher bandwidth and redundancy. Let me know if you need a simpler breakdown!

Port Aggregation Protocol (PAgP)

Port Aggregation Protocol (PAgP) is a **Cisco-proprietary protocol** designed to automate the formation of **EtherChannel** links. It ensures that multiple physical links between two Cisco switches (or between a Cisco switch and a compatible device) are bundled into a **single logical link**, increasing bandwidth and redundancy.

When PAgP is enabled on the interfaces, it sends out PAgP packets to detect compatible links and **negotiate** the formation of an EtherChannel. Once an EtherChannel is established, PAgP manages it by monitoring link health and consistency.

How PAgP Works

1. **PAgP Packets**

   ○ PAgP-enabled ports exchange packets every **30 seconds** to check link consistency and negotiate EtherChannel formation.

   ○ The protocol verifies that all participating ports have **matching settings** before aggregating them.

2. **Link Compatibility Check**
   Before forming an EtherChannel, PAgP ensures that:
   ✅ All ports have the **same speed** (e.g., 100 Mbps, 1 Gbps)
   ✅ All ports have the **same duplex mode** (full or half)
   ✅ All ports belong to the **same VLAN** (in access mode)
   ✅ All ports are either **all trunk ports or all access ports**

3. **Adding and Removing Links**

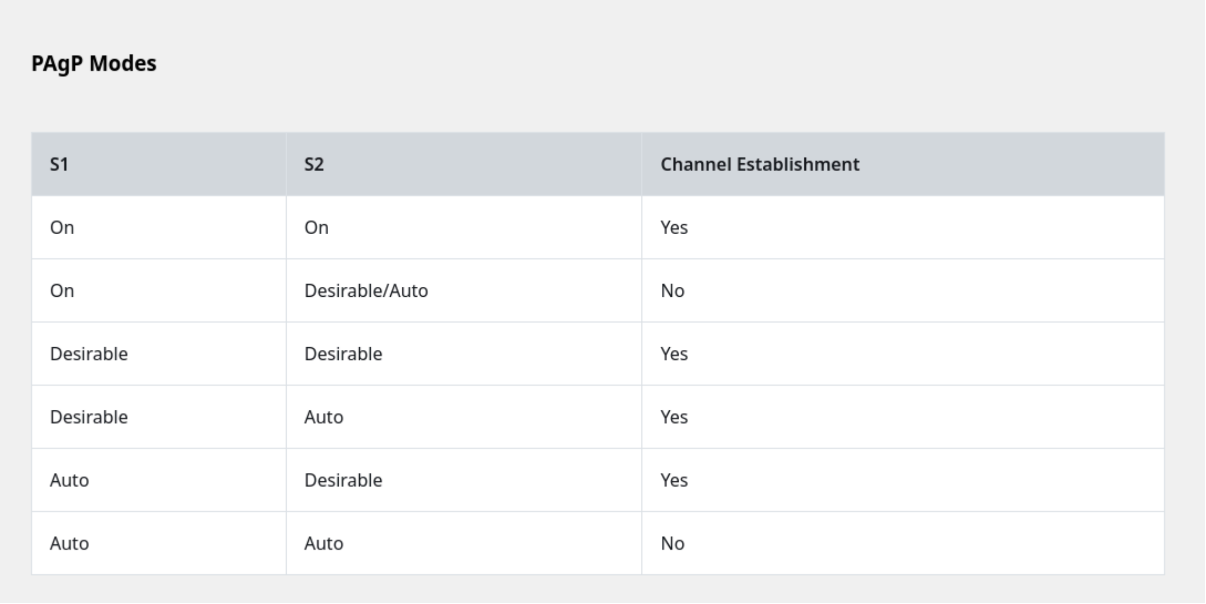
   ○ If a new link is added, PAgP verifies its compatibility before adding it to the channel.

   ○ If a link fails, PAgP **removes it dynamically** without affecting the rest of the EtherChannel.

4. **Spanning Tree Integration**

   ○ Once formed, EtherChannel **appears as a single logical port** to **Spanning Tree Protocol (STP)**.

   ○ This prevents STP from blocking individual links within the bundle, ensuring efficient path selection.



PAgP Modes

S1	S2	Channel Establishment
On	On	Yes
On	Desirable/Auto	No
Desirable	Desirable	Yes
Desirable	Auto	Yes
Auto	Desirable	Yes
Auto	Auto	No

LACP (Link Aggregation Control Protocol)

LACP (Link Aggregation Control Protocol) is an open-standard protocol that bundles multiple physical network links into a single logical link, improving bandwidth, redundancy, and reliability between switches. It works similarly to Cisco's proprietary PAgP but is designed to work across different vendor devices since it follows the IEEE 802.1AX standard (originally 802.3ad).

Why Use LACP?

1. **Increases Bandwidth: Multiple links act as one, increasing overall network speed.**

2. **Provides Redundancy: If one link fails, the remaining links continue to work.**

3. **Automatic Configuration: LACP detects and groups compatible links dynamically.**

4. **Multivendor Support: Unlike Cisco's PAgP, LACP works with non-Cisco devices.**

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to automatically assign **IP addresses** and other network configurations (like **subnet mask, gateway, and DNS servers**) to devices on a network. It eliminates the need for manual configuration, making network management more efficient.

How DHCP Works:

1. **DHCP Discover** – A device (client) sends a request for an IP address when it connects to a network.

2. **DHCP Offer** – The DHCP server responds with an available IP address.

3. **DHCP Request** – The client accepts the offered IP address.

4. **DHCP Acknowledgment (ACK)** – The server confirms the lease, and the client is assigned the IP for a specific period.

IPv6 link-local address

An **IPv6 link-local address** is a special type of address in IPv6 that is **automatically assigned** to every IPv6-enabled interface and is used for communication between nodes on the same link (or local network segment).

Key Characteristics of IPv6 Link-Local Addresses

1. **Always Starts with `FE80::/10`**

   - The first 10 bits are `1111111010`, meaning it falls within the `FE80::/10` range (e.g., `FE80::1`, `FE80::abcd:1234:5678:9abc`).

2. **Mandatory for All IPv6 Devices**

   - Every IPv6-enabled device **must have** a link-local address, even if it doesn't have a global or unique local address.

3. **Used for Local Communication Only**

- Link-local addresses **cannot** be routed across different networks; they are only valid within the same link.

4. **Automatically Assigned by OS**

    - The OS generates the link-local address automatically when an interface is enabled, even without a DHCP server or manual configuration.

Neighbor Discovery Protocol (NDP)

The **Neighbor Discovery Protocol (NDP)** is a key part of IPv6, replacing older IPv4 mechanisms like ARP (Address Resolution Protocol), ICMP Router Discovery, and ICMP Redirect. It operates using **ICMPv6 messages** to manage communication between nodes on the same local network.

What is ICMPv6?

ICMPv6 is an extension of the original **ICMP (Internet Control Message Protocol)** but is **specifically designed for IPv6 networks**. It helps in delivering error messages and operational queries necessary for maintaining the health and performance of an IPv6 network.

It supports several critical functions, including:

1. **Error Reporting** – Reporting issues in packet delivery.
2. **Diagnostics** – Providing network troubleshooting tools like `ping`.
3. **Neighbor Discovery Protocol (NDP)** – Replacing ARP (Address Resolution Protocol) in IPv6.
4. **Multicast Listener Discovery (MLD)** – Managing multicast group memberships.

IPv6 GUA (Global Unicast Address) Assignment

An **IPv6 Global Unicast Address (GUA)** is a **publicly routable** address used for internet communication, similar to IPv4 public addresses. It allows devices to communicate across networks, including the global internet.

SLAAC (Stateless Address Autoconfiguration) Explained

SLAAC (Stateless Address Autoconfiguration) is a method that allows IPv6 hosts to automatically configure their own **Global Unicast Address (GUA)** without requiring a DHCPv6 server. This is particularly useful in networks where DHCPv6 is not available or necessary.

How SLAAC Works

1. ICMPv6 Router Advertisement (RA) Messages

- IPv6 routers **send RA messages** periodically (every 200 seconds) or in response to a **Router Solicitation (RS) message** from a host.
- The RA message contains **prefix information** (e.g., `2001:db8::/64`) and other configuration details.

2. Host Generates an IPv6 Address

Once the host receives an RA message, it:

1. Uses the advertised **network prefix** from the RA (e.g., `2001:db8::/64`).
2. Appends a **unique identifier** (usually derived from its MAC address using EUI-64 or generated randomly).
3. Creates its **Global Unicast Address (GUA)**, ensuring it doesn't conflict with others

SLAAC Deployment Models

SLAAC can be deployed in two ways:

1. SLAAC-Only Mode

- The host **fully configures its IPv6 address using SLAAC**.

- No DHCPv6 server is required.

- The RA message includes:
    - **Prefix Information** (`2001:db8::/64`)
    - **"Other Configuration" flag unset** (indicating no DHCPv6 is needed).
- The host must use **another method to obtain DNS information** (e.g., manual configuration or IPv6 Router Advertisement with RDNSS).

2. SLAAC with Stateless DHCPv6

- The host still **generates its own GUA using SLAAC**.
- However, it **relies on a stateless DHCPv6 server** for additional configuration, such as:
    - **DNS server addresses**
    - **NTP (Network Time Protocol) servers**
    - **Other network settings**
- The RA message includes:
    - **Prefix Information** for SLAAC
    - **"Other Configuration" flag set**, indicating the host should use DHCPv6 for extra details

SLAAC relies on a few fundamental components:

1. **IPv6 Router Advertisement (RA) Messages**: Sent by routers to announce network prefix and configuration options.
2. **IPv6 Router Solicitation (RS) Messages**: Sent by hosts to request an RA from the router.
3. **IPv6 Address Generation**: Based on the received network prefix and a unique identifier.

4. **Duplicate Address Detection (DAD)**: Ensures the generated address is unique.

FHRP (First Hop Redundancy Protocol) is a set of protocols that provide redundancy for the default gateway in a network. These protocols ensure that if the primary gateway (router) fails, another router takes over, allowing uninterrupted network access.

Types of FHRP Protocols

There are three main FHRP protocols:

1. HSRP (Hot Standby Router Protocol)

- **Cisco proprietary** (works only on Cisco devices).
- One router is the **active** gateway, and another router is in **standby** mode.
- If the active router fails, the standby router takes over **automatically**.
- Uses **Hello messages** (sent every 3 seconds) to monitor router health.
- Routers share a **virtual MAC address**, so end devices don't need reconfiguration.

Example HSRP Scenario:

- **Router 1** (Active) handles all traffic.
- **Router 2** (Standby) monitors **Router 1**.
- If **Router 1** goes down, **Router 2** takes over as the new active router.

---

2. VRRP (Virtual Router Redundancy Protocol)

- **Open standard** (works on devices from different vendors).

- Similar to HSRP but with minor differences:
    - Uses **faster timers** (Hello = 1 sec, Hold = 3 sec).
    - Supports **preemption** (higher priority routers can automatically take back control when they come online).
- Uses a **virtual IP address** that is shared among routers.

VRRP in Action:

- The router with the **highest priority** becomes the default gateway.
- If it fails, the next router in line takes over **immediately**.

---

3. GLBP (Gateway Load Balancing Protocol)

- **Cisco proprietary** like HSRP, but with a key difference:
- **Supports load balancing** across multiple routers, not just failover.
- Uses:
    - **Active Virtual Gateway (AVG)** – The main controller that assigns roles.
    - **Active Virtual Forwarders (AVFs)** – Routers that share the traffic load.
- Unlike HSRP & VRRP, which only have **one active router**, GLBP can use **multiple routers at the same time**.

GLBP Example:

- Instead of just one router handling all traffic, **Router 1 & Router 2 share the load**.

- If **one router fails**, the other takes over **without overloading**.

Network Attacks Today

- Distributed Denial of Service (DDoS) - This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization’s website and resources.
- Data Breach - This is an attack in which an organization’s data servers or hosts are compromised to steal confidential information.
- Malware - This is an attack in which an organization’s hosts are infected with malicious software that cause a variety of problems. For example, ransomware such as WannaCry, shown in the figure, encrypts the data on a host and locks access to it until a ransom is paid.

In networking, **NAC (Network Access Control)** is a security framework that controls and restricts access to a network based on a device’s security posture, identity, and compliance with security policies.

How NAC Works:

1. **Authentication:** Verifies the identity of users and devices before granting network access.

2. **Authorization:** Determines what resources the authenticated entity can access.

3. **Posture Assessment:** Checks if the device meets security policies (e.g., updated antivirus, no vulnerabilities).

4. **Enforcement:** Denies or limits access to non-compliant devices and may redirect them to a remediation network.

5. **Continuous Monitoring:** Keeps checking devices even after they gain access.

Cisco Email Security Appliance

Content security appliances include fine-grained control over email and web browsing for an organization’s users.

According to the Cisco's Talos Intelligence Group, in June 2019, 85% of all email sent was spam. Phishing attacks are a particularly virulent form of spam. Recall that a phishing attack entices the user to click a link or open an attachment. Spear phishing targets high-profile employees or executives that may have elevated login credentials. This is particularly crucial in today's environment where, according to the SANS Institute, 95% of all attacks on enterprise networks are the result of a successful spear phishing attack.

The Cisco ESA is a device that is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes. These are some of the functions of the Cisco ESA:

- Block known threats.
- Remediate against stealth malware that evaded initial detection.
- Discard emails with bad links (as shown in the figure).
- Block access to newly infected sites.
- Encrypt content in outgoing email to prevent data loss.

The **Cisco Web Security Appliance** (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.

Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

MAC Address Table Flooding (CAM Table Overflow Attack)

MAC address table flooding, also known as **CAM (Content Addressable Memory) table overflow attack**, is a Layer 2 attack targeting Ethernet switches. It exploits the way switches store and forward frames based on MAC addresses.

1. How a Switch Works (Before the Attack)

A switch maintains a **MAC address table (or CAM table)** that maps **MAC addresses** to specific **switch ports**. It works like this:

1. **Learning**: When a switch receives a frame, it checks the source MAC address and updates the table.

2. **Forwarding**: If the destination MAC is known, the switch sends the frame to the corresponding port. If unknown, it floods the frame to all ports (except the incoming one).

3. **Aging**: Entries in the MAC table expire after a certain period if no traffic is received.

---

2. The Attack: How MAC Address Table Flooding Works

Attackers exploit the limited size of the MAC table using these steps:

1. **Massive Fake MAC Addresses**

    ○ The attacker sends thousands of frames with **spoofed (fake) source MAC addresses**.

    ○ Each frame appears to come from a different device.

2. **CAM Table Overflows**

    ○ Since the MAC table has a limited number of entries (usually in the thousands), it fills up.

    ○ Legitimate devices can no longer be learned by the switch.

3. **Switch Fails & Starts Flooding**

    ○ The switch **fails to store new MAC addresses**.

- All incoming frames with unknown destinations get **flooded to all ports**.
- The switch now behaves like a **hub**, sending traffic to **all connected devices**.

4. **MITM (Man-in-the-Middle) or Sniffing**
    - The attacker can now **capture** network traffic by running packet-sniffing tools (e.g., Wireshark, Ettercap).
    - Normally, traffic meant for specific devices is only sent to them, but now **everyone receives it**, including the attacker.

---

3. Consequences of the Attack

- **Loss of Confidentiality**: Attackers can sniff sensitive data (passwords, financial data, etc.).
- **Network Congestion**: Flooded traffic increases **bandwidth usage** and may cause **network slowdowns**.
- **DoS (Denial of Service)**: Devices may lose connectivity as the switch is unable to function properly.

ARP Spoofing (Poisoning)

ARP (Address Resolution Protocol) is how devices in a **LAN (Local Area Network)** find the MAC address of another device. But **ARP has no authentication**, making it vulnerable to **spoofing (poisoning) attacks**. Attackers exploit this to intercept, modify, or redirect traffic.

---

1. How ARP Works (Before Attack)

Every device on a LAN uses ARP to resolve IP addresses to MAC addresses.

🔹 **Normal ARP Process:**

1. **Device A (192.168.1.10)** wants to send data to **Device B (192.168.1.20)**.
2. Device A sends an **ARP Request**:

   "Who has 192.168.1.20? Tell me your MAC address."
3. **Device B responds with an ARP Reply:**
   "192.168.1.20 is at **00:1A:2B:3C:4D:5E** (its MAC address)."
4. Device A stores this in its **ARP table** and sends packets to B's MAC address.

DHCP Snooping Attack – Detailed Explanation

A **DHCP Snooping Attack** happens when an attacker sets up a **rogue DHCP server** to hand out **malicious IP configurations** to devices in a network. This allows them to **redirect, block, or intercept** traffic, leading to MITM (Man-in-the-Middle) or Denial of Service (DoS) attacks.

---

1. How DHCP Works (Before Attack)

DHCP (Dynamic Host Configuration Protocol) is how devices in a network automatically get an IP address, subnet mask, default gateway, and DNS settings.

🔹 **Normal DHCP Process**

When a device (client) connects to a network, it follows this process to get an IP address from a **legitimate** DHCP server:

1. **DHCP Discover:**

    - The client **broadcasts** a request:

      "Hey, I need an IP address!"

2. **DHCP Offer:**
    - The **real** DHCP server replies:

      "Here's an IP address you can use: **192.168.1.50**."

3. **DHCP Request:**
    - The client asks to **confirm** the offered IP:

      "Yes, I'll take that IP: **192.168.1.50**."

4. **DHCP Acknowledgment (ACK):**
    - The server confirms:

      "Great! You're now on the network."

💡 Result:

The client gets a valid **IP, default gateway, and DNS settings**, allowing it to communicate on the network.

---

2. How a DHCP Snooping Attack Works

An attacker sets up a **fake (rogue) DHCP server** to **trick clients** into using malicious network settings.

🔴 Steps in a DHCP Snooping Attack

1. **Attacker sets up a fake DHCP server** on the LAN.
2. The fake server **responds faster** than the real DHCP server to client requests.
3. The victim’s device **receives an IP address from the attacker instead of the real DHCP server.**
4. The attacker **provides malicious network configurations**:
    - **Fake default gateway** → Routes all traffic **through the attacker** (MITM attack).
    - **Fake DNS server** → Redirects users to **phishing sites**.
    - **Wrong subnet mask** → Prevents communication with the real network (DoS attack).
5. The victim’s device unknowingly **sends data through the attacker**, allowing interception or blocking.

Example Scenarios

✅ MITM (Man-in-the-Middle) Attack

- Attacker makes the victim **use them as the gateway**.
- Captures or modifies traffic before forwarding it to the real destination.
- Can steal **login credentials, session tokens, and sensitive data**.

✅ Denial of Service (DoS) Attack

- Attacker assigns **wrong IP configurations**.
- The victim **can’t reach the internet or internal network**

DNS Redirection (Phishing)

- Attacker provides a **fake DNS server**.
- Users visiting "bank.com" get redirected to **attacker’s fake banking site**.

VLAN tagging is a method used to **identify and separate network traffic** in a switch environment by adding a VLAN identifier (VLAN ID) to

Ethernet frames. This ensures that devices in different VLANs remain isolated unless explicitly routed.

VLAN Hopping Attack

A **VLAN Hopping Attack** occurs when an attacker **bypasses VLAN segmentation** to gain unauthorized access to other VLANs. This allows them to **intercept traffic, launch attacks on restricted networks, or perform reconnaissance**.

---

1. How VLANs Work (Before Attack)

VLANs (Virtual Local Area Networks) separate network traffic at Layer 2 (Data Link Layer). They improve security and efficiency by **isolating** different departments or functions.

Normal VLAN Behavior

- Devices in **VLAN 10 cannot communicate** directly with devices in **VLAN 20** unless allowed by a **Layer 3 device (router/firewall)**.
- Trunk ports **allow traffic from multiple VLANs** to flow between switches **using VLAN tagging (802.1Q protocol).**

---

2. How a VLAN Hopping Attack Works

Attackers exploit **misconfigured switch settings** to send data across VLANs **without proper authorization**.

Two Main Types of VLAN Hopping Attacks

1. **Switch Spoofing** → Attacker tricks the switch into **thinking they are a trunk port**.
2. **Double Tagging** → Attacker **modifies VLAN tags** to jump VLANs.

---

1. Switch Spoofing Attack

Goal: The attacker **pretends to be a switch** to negotiate a trunk link.

How it Works

1. The attacker **connects to an access port** (normally assigned to a single VLAN).
2. They send **DTP (Dynamic Trunking Protocol) negotiation messages**, tricking the switch into **converting the port into a trunk port**.
3. Once the attacker's port becomes a trunk, they can **send and receive traffic for all VLANs**.

.

How Does STP Manipulation Work?

An attacker **spoofs BPDU packets** to:

1. **Claim they are the root bridge** by sending **lower Bridge ID (Priority + MAC Address)**.
2. Force switches to **recalculate the spanning tree**, making **the attacker's device the center of traffic flow**.
3. Once traffic flows through the attacker, they can:
   - **Intercept and manipulate** data.
   - **Perform Man-in-the-Middle (MITM) attacks**.
   - **Cause network instability** by repeatedly sending BPDUs.

There are several **types of Wireless Local Area Network (WLAN)** based on different standards and technologies. Here are the main types:

1. Based on IEEE Standards (Wi-Fi Standards)

WLANs are categorized by the **IEEE 802.11** standards, which define various Wi-Fi generations:

- **802.11a** (1999) – 5 GHz, max speed 54 Mbps, less interference

- **802.11b** (1999) – 2.4 GHz, max speed 11 Mbps, high interference
- **802.11g** (2003) – 2.4 GHz, max speed 54 Mbps, backward compatible with 802.11b
- **802.11n (Wi-Fi 4)** (2009) – 2.4 GHz & 5 GHz, max speed 600 Mbps, MIMO introduced
- **802.11ac (Wi-Fi 5)** (2013) – 5 GHz, max speed 3.5 Gbps, better bandwidth
- **802.11ax (Wi-Fi 6 & 6E)** (2019) – 2.4 GHz, 5 GHz, & 6 GHz, max speed 9.6 Gbps, better efficiency
- **802.11be (Wi-Fi 7)** (Upcoming) – 6 GHz, ultra-high speeds, low latency

2. Based on Network Infrastructure

- **Independent Basic Service Set (IBSS) / Ad-hoc WLAN**
    - Devices connect directly (peer-to-peer) without an access point (AP).
    - Used in temporary or small-scale networks.
- **Basic Service Set (BSS)**
    - Uses an **access point (AP)** for communication.
    - Most common in home and office networks.
- **Extended Service Set (ESS)**
    - Multiple APs connected to extend coverage.
    - Used in enterprise networks, universities, and malls.
- **Mesh WLAN**
    - Multiple APs dynamically connect to create a self-healing network.

    - Used in smart cities and industrial applications.

3. Based on Coverage & Deployment

- **Indoor WLAN** – Used in homes, offices, and buildings.
- **Outdoor WLAN** – Covers large areas like campuses, stadiums, or city-wide Wi-Fi.
- **Enterprise WLAN** – High-performance, secure networks in corporate environments.
- **Public WLAN (Hotspots)** – Open networks in cafes, airports, and malls.

4. Based on Frequency Bands

- **2.4 GHz WLAN** – Longer range, but more interference (crowded spectrum).
- **5 GHz WLAN** – Faster speeds, less interference, but shorter range.
- **6 GHz WLAN** – Wi-Fi 6E & 7, extremely high speeds, minimal congestion

Each type serves different needs, from casual browsing at home to high-speed enterprise networking.

WLANs are half-duplex, shared media configurations. Half-duplex means that only one client can transmit or receive at any given moment. Shared media means that wireless clients can all transmit and receive on the same radio channel. This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.

To resolve this problem, WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) as the method to determine how and when to send data on the network. A wireless client does the following:

1. Listens to the channel to see if it is idle, which means that is senses no other traffic is currently on the channel. The channel is also called the carrier.
2. Sends a request to send (RTS) message to the AP to request dedicated access to the network.
3. Receives a clear to send (CTS) message from the AP granting access to send.
4. If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
5. After it receives the CTS, it transmits the data.
6. All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

CAPWAP is based on LWAPP but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP establishes tunnels on User Datagram Protocol (UDP) ports. CAPWAP can operate either over IPv4 or IPv6, as shown in the figure, but uses IPv4 by default.

What is a Wireless LAN Controller (WLC)?

A **Wireless LAN Controller (WLC)** is a centralized device that manages, controls, and optimizes multiple **Access Points (APs)** in a wireless network. Instead of having standalone APs manage everything on their own, the WLC takes over high-level functions like authentication, security, and roaming, making large-scale Wi-Fi networks easier to manage and more efficient.

What is DTLS Encryption?

Datagram Transport Layer Security (DTLS) is a security protocol that provides encryption, authentication, and integrity protection for **datagram-based applications**. It is essentially **TLS (Transport Layer Security) adapted for UDP (User Datagram Protocol)** instead of TCP.

Since UDP does not guarantee packet delivery or order, DTLS adds mechanisms to **handle packet loss, reordering, and retransmissions** while still providing strong encryption.

How DTLS Works

DTLS operates similarly to **TLS**, but with modifications to handle UDP's unreliable nature. Here's how it works:

1. **Handshake Process**

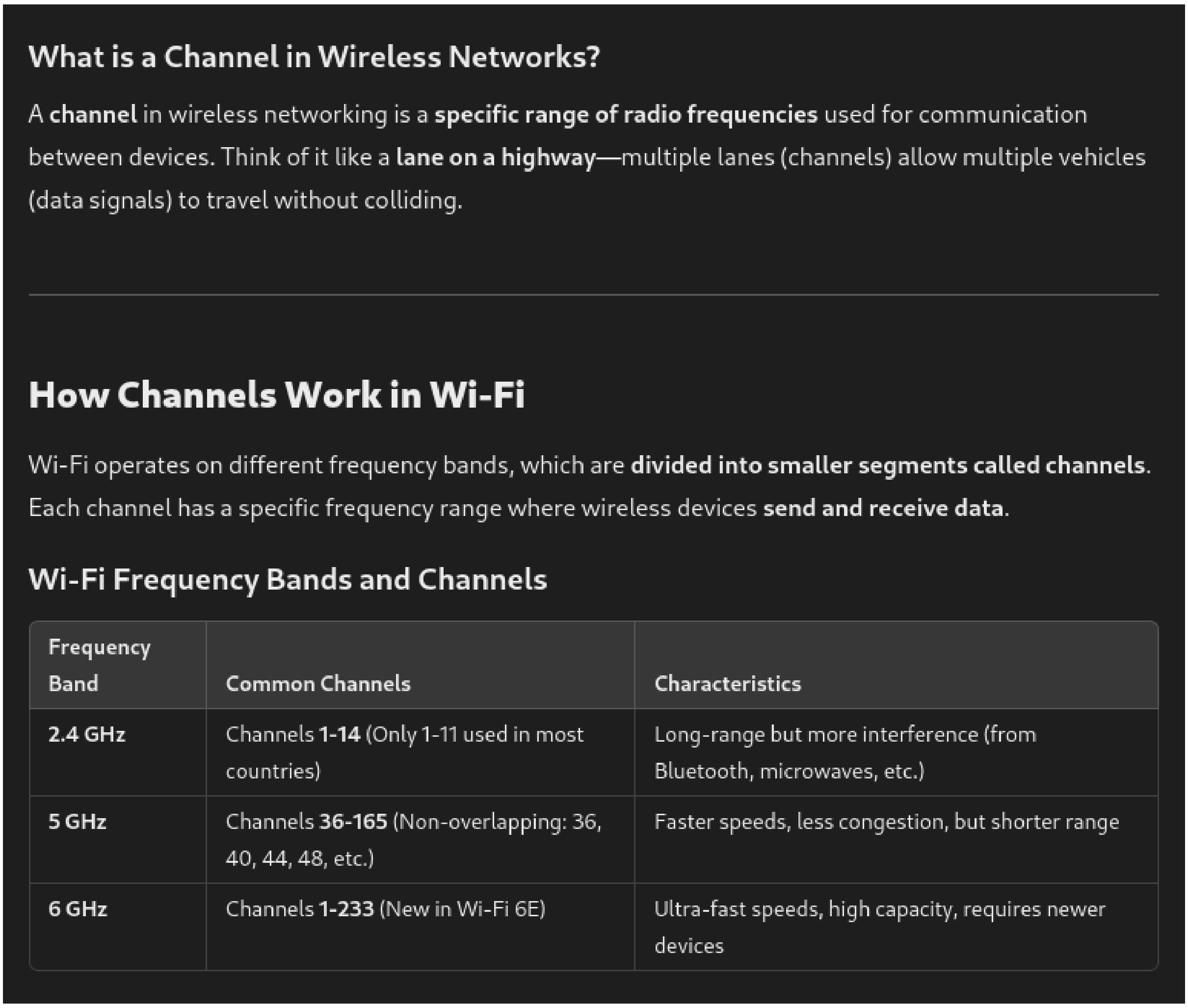
    - A **client and server exchange cryptographic keys** using **asymmetric encryption** (e.g., RSA, Diffie-Hellman).
    - They negotiate encryption algorithms (e.g., AES-GCM, ChaCha20).
    - Mutual authentication is performed using certificates or pre-shared keys.

2. **Encryption & Integrity**

    - Once the handshake is complete, data is encrypted using **symmetric encryption** (e.g., AES, ChaCha20).

- Message integrity is ensured using **HMAC (Hash-Based Message Authentication Code)**.

3. **Packet Handling & Reliability**
   - Since UDP doesn't provide retransmission, DTLS implements a **retransmission timer** for lost packets.
   - DTLS can detect **out-of-order** packets and properly reassemble them.



What is a Channel in Wireless Networks?

A **channel** in wireless networking is a **specific range of radio frequencies** used for communication between devices. Think of it like a **lane on a highway**—multiple lanes (channels) allow multiple vehicles (data signals) to travel without colliding.

How Channels Work in Wi-Fi

Wi-Fi operates on different frequency bands, which are **divided into smaller segments called channels**. Each channel has a specific frequency range where wireless devices **send and receive data**.

Wi-Fi Frequency Bands and Channels

Frequency Band	Common Channels	Characteristics
2.4 GHz	Channels **1-14** (Only 1-11 used in most countries)	Long-range but more interference (from Bluetooth, microwaves, etc.)
5 GHz	Channels **36-165** (Non-overlapping: 36, 40, 44, 48, etc.)	Faster speeds, less congestion, but shorter range
6 GHz	Channels **1-233** (New in Wi-Fi 6E)	Ultra-fast speeds, high capacity, requires newer devices

Frequency Channel Saturation in Wireless Networks

Wireless networks use radio frequency (RF) channels to communicate, but when too many devices compete for the same channel, channel saturation occurs. This overcrowding leads to interference, packet loss, and degraded network performance.

To reduce saturation and improve efficiency, several techniques have been developed to manage and optimize frequency usage.

What is a Frequency Band?

A **frequency band** is a specific range of radio wave frequencies used for wireless communication. Think of it like a **radio station**—each station (band) broadcasts at a different frequency to avoid interference.

In Wi-Fi and other wireless technologies, **frequency bands determine how fast and far data can travel**.

Why Do Frequency Bands Matter?

- **2.4 GHz** = Best for **long range, basic browsing**.
- **5 GHz** = Best for **speed and performance**.
- **6 GHz** = Best for **future-proof high-speed networks**.

Frequency-Hopping Spread Spectrum (FHSS)

FHSS is a **wireless communication technique** that **rapidly switches (hops) between multiple frequency channels** to **send data**. It was used in the original **802.11 Wi-Fi standard** and is still found in **Bluetooth, walkie-talkies, and some cordless phones**.

Orthogonal Frequency-Division Multiplexing (OFDM)

OFDM is a **wireless transmission technique** where a **single channel is split into multiple sub-channels** that transmit data simultaneously. These sub-channels are **orthogonal (mathematically independent)**, meaning they can **overlap without interfering** with each other.

This method is used in **Wi-Fi (802.11a/g/n/ac), LTE, 5G, and other modern wireless communication systems** because it improves **speed, efficiency, and resistance to interference**.

WLAN Deployment

The number of users supported by a WLAN depends on the geographical layout of the facility, including the number of bodies and devices that can fit in a space, the data rates users expect, the use of non-overlapping channels by multiple APs in an ESS, and transmit power settings.

When planning the location of APs, the approximate circular coverage area is important (as shown in the figure), but there are some additional recommendations:

- If APs are to use existing wiring or if there are locations where APs cannot be placed, note these locations on the map.
- Note all potential sources of interference which can include microwave ovens, wireless video cameras, fluorescent lights, motion detectors, or any other device that uses the 2.4 GHz range.
- Position APs above obstructions.
- Position APs vertically near the ceiling in the center of each coverage area, if possible.
- Position APs in locations where users are expected to be. For example, conference rooms are typically a better location for APs than a hallway.
- If an IEEE 802.11 network has been configured for mixed mode, the wireless clients may experience slower than normal speeds in order to support the older wireless standards.

When estimating the expected coverage area of an AP, realize that this value varies depending on the WLAN standard or mix of standards that are deployed, the nature of the facility, and the transmit power that the AP is configured for. Always consult the specifications for the AP when planning for coverage areas.

DoS Attacks

Wireless DoS attacks can be the result of:

- Improperly configured devices - Configuration errors can disable the WLAN. For instance, an administrator could accidently alter a configuration and disable the network, or an intruder with administrator privileges could intentionally disable a WLAN.

- A malicious user intentionally interfering with the wireless communication - Their goal is to disable the wireless network completely or to the point where no legitimate device can access the medium.
- Accidental interference - WLANs are prone to interference from other wireless devices including microwave ovens, cordless phones, baby monitors, and more, as shown in the figure. The 2.4 GHz band is more prone to interference than the 5 GHz band.

Rogue Access Points

A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy. Anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network resource.

Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.

A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP. Doing so circumvents the security measures and other unauthorized devices can now access network resources as a shared device.

To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies, as shown in the figure, and use monitoring software to actively monitor the radio spectrum for unauthorized APs.

Static or Dynamic?

The previous topic discussed the ways that a router creates its routing table. So, you now know that routing, like IP addressing, can be either static or dynamic. Should you use static or dynamic routing? The answer is both! Static and dynamic routing are not mutually exclusive. Rather, most networks use a combination of dynamic routing protocols and static routes.

Static Routes

Static routes are commonly used in the following scenarios:

- As a default route forwarding packets to a service provider
- For routes outside the routing domain and not learned by the dynamic routing protocol
- When the network administrator wants to explicitly define the path for a specific network

- For routing between stub networks

Static routes are useful for smaller networks with only one path to an outside network. They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.

Dynamic Routing Protocols

Dynamic routing protocols help the network administrator manage the time-consuming and exacting process of configuring and maintaining static routes. Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers. Dynamic routing protocols are scalable and automatically determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

- In networks consisting of more than just a few routers
- When a change in the network topology requires the network to automatically determine another path
- For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.