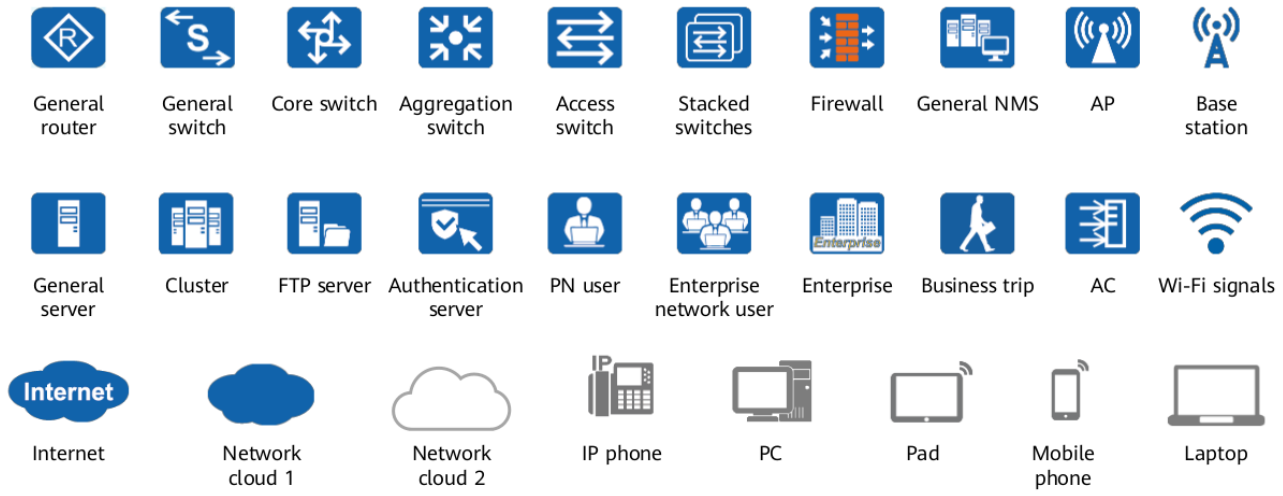
Data Communication Network Basis

1 Data Communication Network Basis

1.1 Huawei Device Icons



1.2 Communication and Networks

1.2.1 Concept of Network Communication

- **Communication:** Information exchange through various mediums and behaviors.

- **Network communication:** Occurs between terminal devices via a computer network.

> **Terminal devices** are the end-user devices such as computers, phones, or tablets that connect to a network for communication.

1.2.1.1 Examples of Network Communication:

---

1. Two computers sharing files through a network cable.
2. Multiple computers exchanging files via a router.
3. Downloading files from the Internet onto a computer.

1.2.2 Information Transfer Process

1.2.2.1 Analogy: Express Delivery vs Network Communication

Express Delivery	Network Communication
Objects packaged with delivery details	Data payload encapsulated with header/tail
Sorted at distribution centers	Routed through gateways based on destination address
Delivered to recipients, unpacked for confirmation	Data packets verified by destination computer

1.2.2.2 Common Terms

Term	Description
Data payload	Core information exchanged in communication.
Packet	Unit switched/transmitted on the network containing header, payload, tail.
Header	Information added before data for transmission facilitation.
Tail	Information added after data (not always present).
Encapsulation	Adding header/tail to form packet process.
Decapsulation	Removing header/tail to obtain original data process.
Gateway	Device for protocol conversion, route selection, exchange functions.
Router	Device that selects forwarding paths for packets based on destination address.
Terminal device	End devices in communication systems as senders or receivers (e.g., PC, VoIP).

1.2.3 Network Devices and Their Functions

1.2.3.1 Switches

> Switches connect end users to the network and facilitate Layer 2 switching inside broadcast domains.

1.2.3.2 Routers

> Routers determine paths for packet forwarding across different networks while isolating broadcast domains.

1.2.3.3 Firewalls

> Firewalls act as security barriers between trust zones—controlling access and monitoring traffic between networks.

1.2.3.4 Wireless Devices:

1.2.3.4.1 WLAN Overview:

WLAN uses radio waves or other wireless signals as transmission media instead of cables.

1.2.3.4.2 WLAN Devices:

- **Fat AP**: Independent operation suited for home use; simple functions; lower cost; requires individual configuration;mainly only one used for houses.
- **Fit AP**: Works with Access Controllers; used in medium/large enterprises; managed by AC; more complex features than Fat APs;mainly used more than one.
- **Access Controller (AC)**: Manages Fit APs; provides wireless control services like large capacity & high performance; deployed at aggregation layer.

1.3 Network Types and Topologies

1.3.1 Network Types

1.3.1.1 LAN (Local Area Network)

- **Coverage**: A few square kilometers (e.g., within a building or campus).
- **Use Cases**: Office networks, cyber bars, home networks.
- **Technologies**: Ethernet, Wi-Fi.

1.3.1.2 MAN (Metropolitan Area Network)

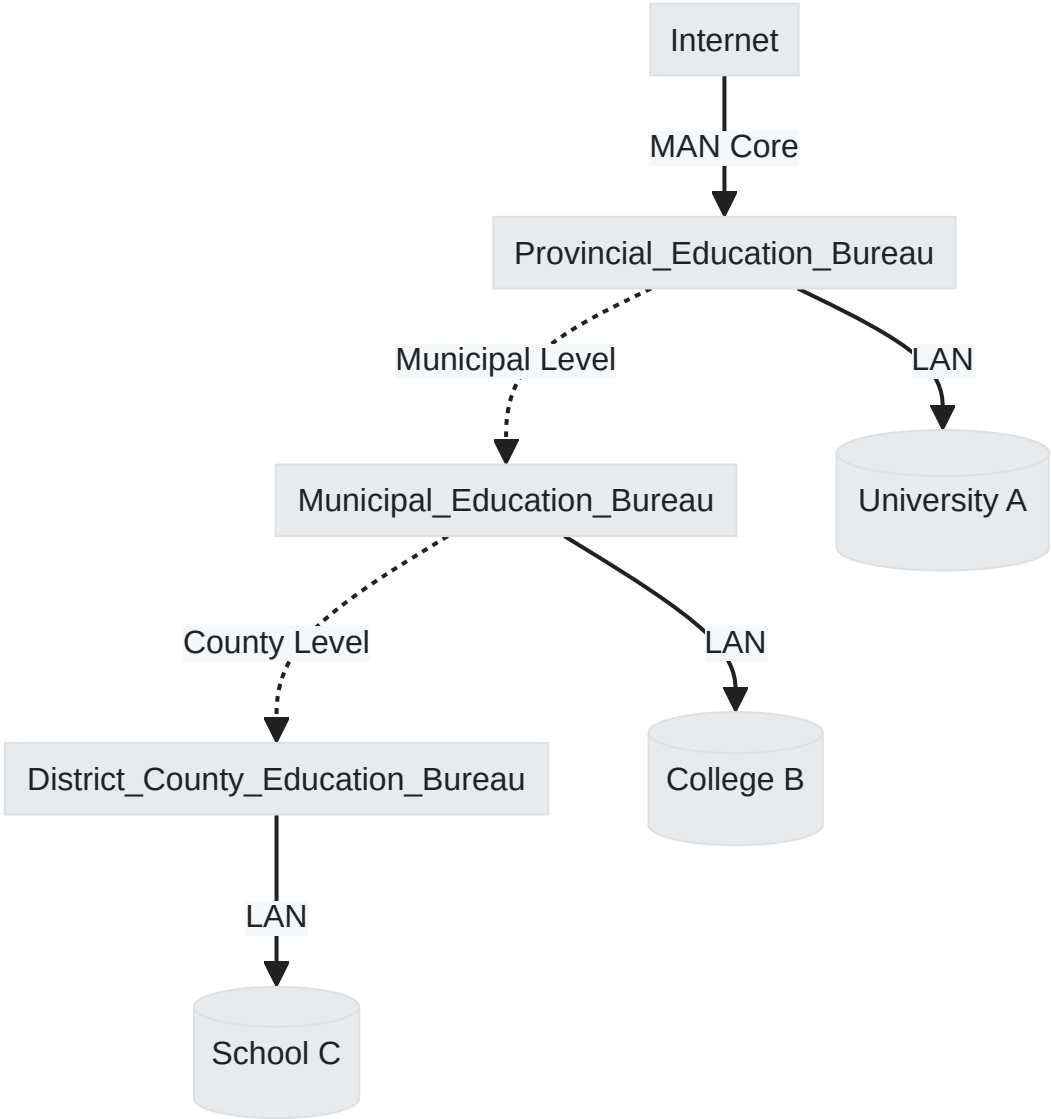
- **Coverage**: City-wide (expands the access scope of LANs).
- **Use Cases**: Broadband MANs, education MANs, e-government private lines.
- **Technologies**: Higher-speed Ethernet (10 Gbit/s or 100 Gbit/s), WiMAX.

1.3.1.3 WAN (Wide Area Network)

- **Coverage**: Large geographical areas; from tens to thousands of square kilometers.
- **Use Cases**: Connecting multiple LANs/MANs across cities or countries.
- **Technologies**: HDLC, PPP.

> **Info**
>
> The Internet is an example of a WAN.

1.3.2 Hierarchical Structure in Education Industry



Diagram

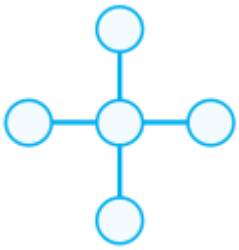
This diagram represents how LANs at educational institutions are connected through various levels of MAN cores up to the provincial level and eventually to the Internet.

1.3.3 Network Topology Types

Logical Structure:
Defines how data flows, is managed, and is controlled within the network, independent of physical connections.

> **Physical Structure:**
> Refers to the actual hardware and wiring through which data travels in a network.

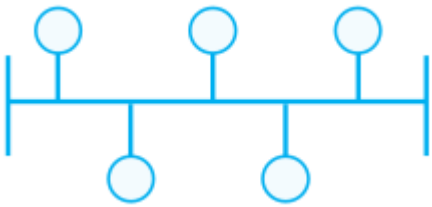
1.3.3.1 Star Topology



Advantages:

- Easy addition of new nodes.
- Centralized monitoring possible.
  Disadvantages:
- Central node failure impacts entire network.

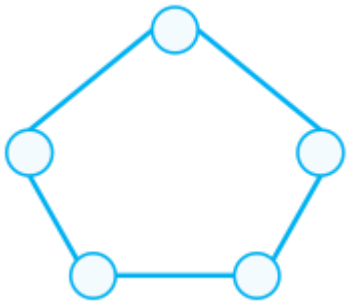
1.3.3.2 Bus Topology



Advantages:

- Simple installation; saves cable resources.
- Node failure usually doesn't affect entire network.
  Disadvantages:
- Bus fault affects all communications; low security due to shared medium.

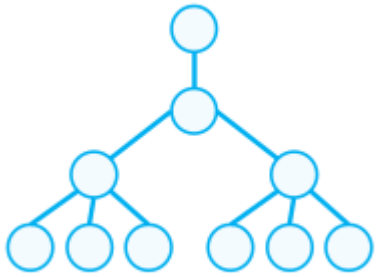
1.3.3.3 Ring Topology



Advantages:

- Saves cable resources.
  Disadvantages:
- Adding new nodes is complex; breaking the ring is required for expansion.

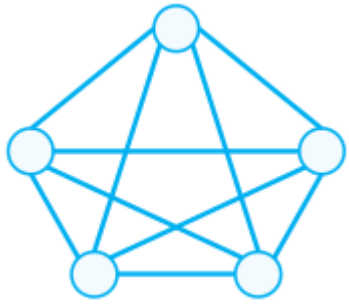
1.3.3.4 Tree Topology



Advantages:

- Easy to add more devices by connecting additional star networks together.
  Disadvantages:
- If a central node (like a root or branch) fails, it can disrupt communication for all devices connected to it.

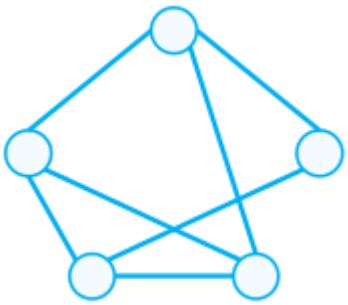
1.3.3.5 Full-Mesh Topology



Advantages:

- High reliability and communication efficiency.
  Disadvantages:
- High costs due to many ports and cables; difficult expansion.

1.3.3.6 Partial-Mesh Topology



Advantages:

- Lower cost than full-mesh topology.
  Disadvantages:
- Lower reliability compared to full-mesh topology.

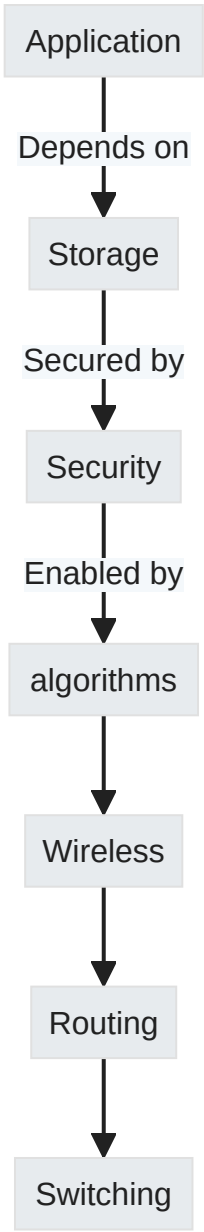
> **Tip**
>
> In practice, topologies are often combined based on specific needs for cost-efficiency and reliability.

1.4 Network Engineering and Network Engineers

1.4.1 Overview of Network Engineering

- Planning, design, implementation, Activation, and troubleshooting of network solutions.
- Integrates hardware devices, software, and technologies to create cost-effective systems.

1.4.1.1 Key Technical Modules



1.4.2 Role of a Network Engineer

- Master professional network technologies.
- Develop solutions based on customer requirements.
- Mobilize resources for project implementation.
- Provide training and documentation post-implementation.

1.4.3 Technology Development Path for Network Engineers

1.4.3.1 Overall Capabilities

> Solution design, network planning, implementation, troubleshooting, and optimization.

1.4.4 Huawei Certification for Talent Development

1.4.4.1 Career Paths Provided by Certification

Engineer —Evolution→ Senior_Engineer —Evolution→ Expert

1.4.5 Huawei Datacom Certification Portfolio

- **HCIA-Datacom:** A single course with an exam that covers fundamental data communication, internet traffic direction, network security, wireless tech, SDN/NFV, network automation, and network setup basics.
- **HCIP-Datacom:** One core course with an exam plus a choice of six specialized courses in advanced networking topics. You must complete the main course and can select from options like routing, network design, WAN planning, SD-WAN technologies, or network automation.
- **HCIE-Datacom:** An advanced-level course split into two parts with one comprehensive exam. It covers traditional networking and command-line skills as well as Huawei's SDN solutions for enterprise networks.

Network Reference Model

1 Network Reference Model

1.1 Applications and Data

1.1.1 Origin of Story - Applications

- Applications serve various user needs (web browsing, gaming, video playback).
- Information generated takes many forms: text, images, videos.

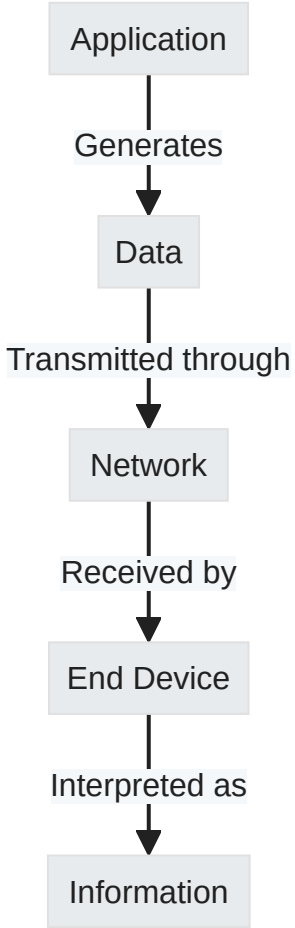
1.1.2 Application Implementation - Data

1.1.2.1 Data Generation

- Data is all kinds of information in digital form (`0s` and `1s`).

1.1.2.2 Data Transmission

- Applications transmit data between devices via networks.



1.2 Network Reference Model and Standard Protocols

1.2.1 OSI Reference Model Overview

The **OSI** (Open Systems Interconnection) model is a Theoretical framework used to understand and standardize the functions of a telecommunication or computing system. It consists of seven layers, each serving specific networking functions.

1.2.2 Layers Breakdown

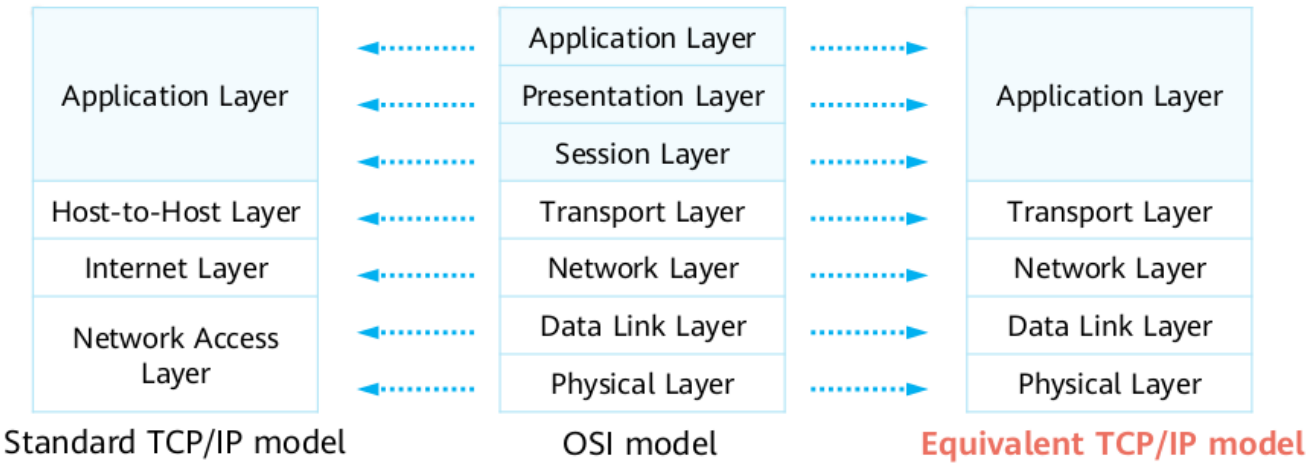
---

1. **Physical Layer**: Handles the transmission of raw bit streams over a physical medium.
2. **Data Link Layer**: Provides Host-to-Host data transfer and error correction uses Mac.
3. **Network Layer**: Manages device addressing and data routing.
4. **Transport Layer**: Ensures complete end-to-end data transfer with speed control and sequence management.
5. **Session Layer**: Manages sessions between applications.
6. **Presentation Layer**: Translates data formats for application compatibility.
7. **Application Layer**: Interfaces with applications to use network services.

1.2.3 TCP/IP Reference Model

TCP/IP is the foundation of modern Internet protocols, consisting of four layers in the standard model and mapping closely to the OSI model.

1.2.3.1 Standard TCP/IP vs OSI Model



- **Application (TCP/IP)** = Application + Presentation + Session (OSI)
- **Transport (TCP/IP)** = Transport (OSI)
- **Internet (TCP/IP)** = Network (OSI)
- **Network Access (TCP/IP)** = Data Link + Physical (OSI)

1.2.4 Common TCP/IP Protocols

1.2.4.1 Application Layer Protocols:

- **HTTP (Hypertext Transfer Protocol)**: Web page access
- **FTP (File Transfer Protocol)**: File transfers between hosts
- **DNS (Domain name service)**: Resolves domain names to IP addresses
- **TFTP (Trivial File Transfer Protocol)**: Simple file transfer protocol, which provides simple file transfer services.
- **Telnet**: Remote login protocol, which provides remote management services.
- **SMTP (Simple mail transfer protocol)**: which provides Internet email services.

1.2.4.2 Transport Layer Protocols:

- **TCP (Transmission Control Protocol)**: Reliable, connection-oriented communication
- **UDP (User Datagram Protocol)**: Connectionless communication, less overhead than TCP

1.2.4.3 Network Layer Protocols:

- **IP (Internet Protocol)**: Data packet routing between source and destination
- **IGMP (Internet Group Management Protocol)**: Multicast group management
- **ICMP (Internet Control Message Protocol)**: Control messages for network diagnostics

1.2.4.4 Data Link Layer Protocols:

- **PPP (Point-to-Point Protocol)**: Point-to-point protocol mainly used in WANs.
- **Ethernet**: Widely used LAN technology.
- **PPPoE (Point-to-Point Protocol over Ethernet)**: lets multiple users on a local network connect to the internet through a single connection point like a modem.

1.2.5 Protocol Standardization Organizations

---

1. **IETF** - Develops Internet protocols through RFCs.
2. **IEEE** - Creates standards including Ethernet and Wi-Fi.
3. **ISO** - International standardization organization; Created the OSI model.

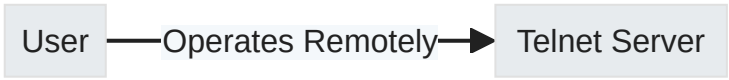
1.2.6 Application Layer Details

- At the application layer, the information (PDU) sent is known as data.
  - **PDU (Protocol Data Unit)**: is a chunk of information transferred over a network at different layers of the OSI model.

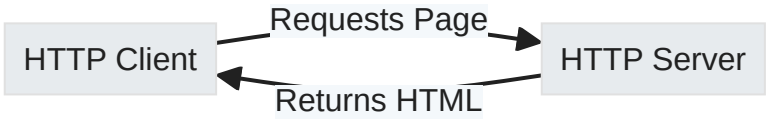
1.2.6.1 FTP Process:

FTP Client —Connects & Operates Files→ FTP Server

1.2.6.2 Telnet Process:



1.2.6.3 HTTP Process:



1.2.7 Transport Layer Details

A transport layer protocol adds its own header to the application's data, sets up a connection from one program to another, and sends out units called **segments**.

1.2.7.1 TCP/UDP Header Comparison:

Header Field	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Source Port	Identifies the sending application (16 bits).	Identifies the sending application (16 bits).
Destination Port	Identifies the receiving application (16 bits).	Identifies the receiving application (16 bits).
Sequence Number	Marks the order of bytes sent; only in TCP (32 bits).	Not applicable in UDP.
Acknowledgment Number	Next byte expected from receiver; valid if ACK flag is set; only in TCP (32 bits).	Not applicable in UDP.
Header Length	Length of TCP header in 32-bit words, usually 5 for	Not applicable in UDP, fixed 8-byte header.

Header Field	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
	no options (4 bytes per word).	
Reserved	Reserved for future use, set to 0; only in TCP (3 bits).	Not applicable in UDP.
Control Bits	Various flags like SYN, FIN, ACK used for connection state; only in TCP.	Not applicable in UDP.
Window	Flow control window size, receiver's buffer space; only in TCP (16 bits).	Not applicable in UDP.
Checksum	Ensures integrity of the header and data for both protocols (16 bits).	Ensures integrity of header and data for both protocols (16 bits).
Urgent Pointer	Points to urgent data if URG flag is set; only in TCP (16 bits).	Not applicable in UDP.
Options	Optional settings for advanced features; variable length up to 40 bytes; only in TCP.	Not applicable
Length	Not applicable in TCP.	*Specifies total length of header and data for UDP segment, minimum is 8 bytes due to header size*

> Note: TCP is more complex but reliable; UDP is simpler but less reliable.

1.2.7.2 TCP and UDP - Port Numbers

- source port used by a client is randomly allocated (greater than 1023 and is not being used)

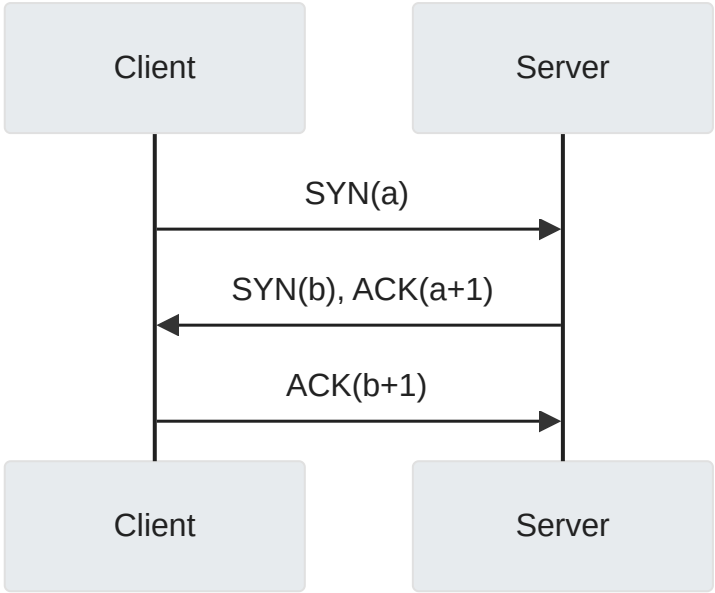
- destination port is specified by the application of a server.

Port

- **Souce port** : 1024
- **Destination port** : 80

1.2.7.3 Connection Management

1.2.7.3.1 Three-Way Handshake (TCP Connection Setup):

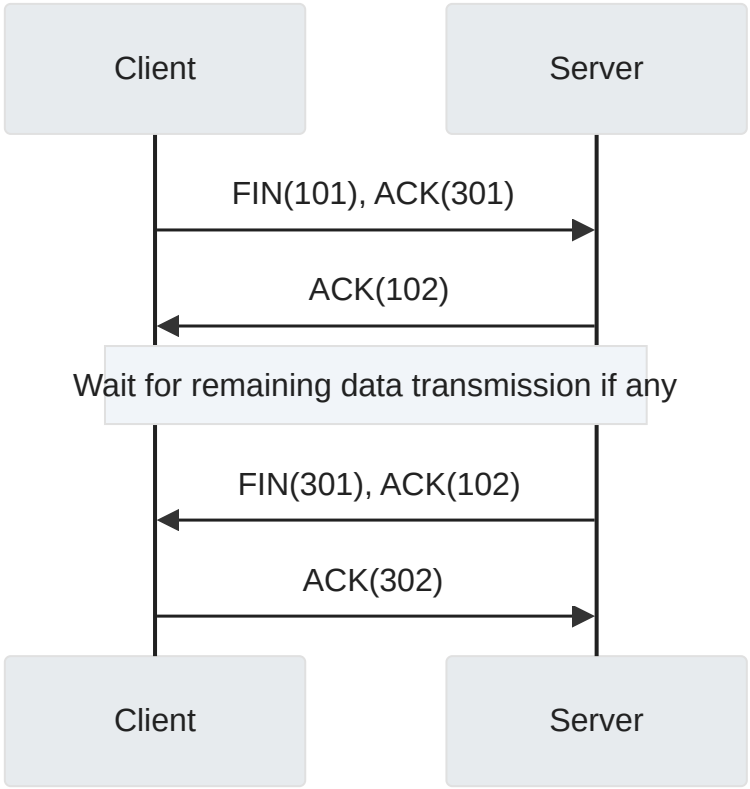


Explain Connection

- Client initiates the connection by sending a SYN packet with a random sequence number.
- Server responds with a SYN-ACK packet, acknowledging Client's SYN and providing its own random sequence number.
- Client sends an ACK packet acknowledging Server's SYN, which completes the connection establishment.

1.2.7.3.2 Four-Way Handshake (TCP Shutdown):

> PC1 initiates the closure of a TCP connection without sending data, PC2 acknowledges and may send remaining data before also initiating closure, and after PC1 acknowledges this final step, the connection is fully closed.

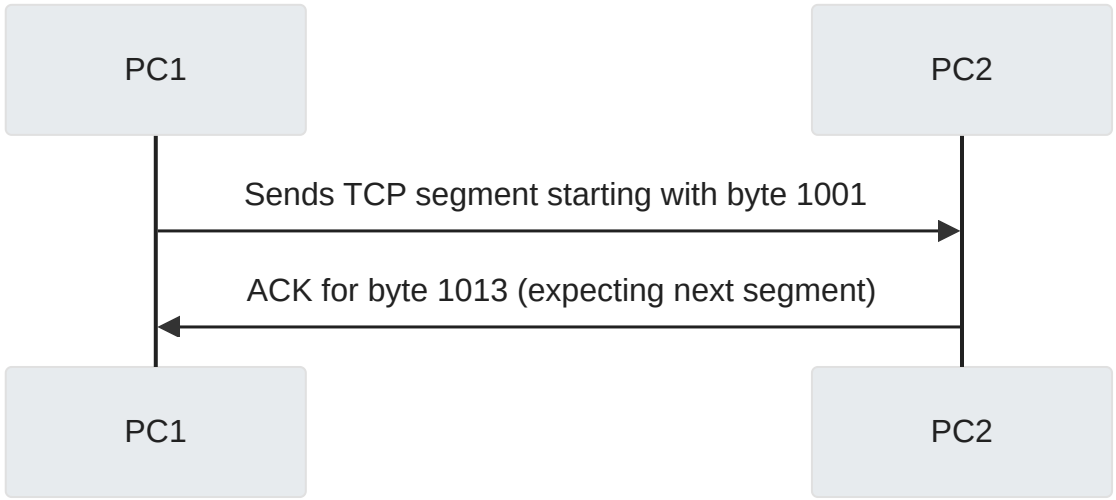


1.2.7.4 TCP Sequence Number and Acknowledgment Number

> PC1 (the sender) wants to send data to PC2 (the receiver). The numbering of bytes starts at `a+1`, and let's say `a` is 1000 for simplicity. So the first byte is numbered 1001.

1. **PC1 numbers bytes**: Bytes are numbered starting at 1001.
2. **PC1 sends TCP segments**: The first segment has a sequence number of 1001.

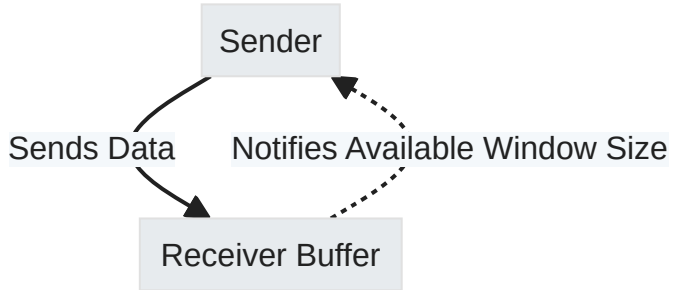
3. **PC2 acknowledges receipt**: After receiving, PC2 sends an acknowledgment for the next expected byte, which is 1013 if the segment payload was 12 bytes.
4. **PC1 prepares next segment**: PC1 receives the acknowledgment and prepares to send the next segment starting with byte number 1013.



1.2.7.5 Sliding Window Mechanism

Ensures proper flow control by adjusting the rate based on the receiver's buffer availability.

> During a TCP connection, both sides agree on how much data can be sent at once, then exchange data accordingly, and continually adjust this amount based on available space in the receiver's buffer.



1.2.8 Network Layer Details

- PDUs at the Network layer are called **packets**.
- Routing and **logical addressing** (IP) are core functions.

1.2.8.1 Transport vs. Network Layer Functions

> The transport layer establishes connections between processes on hosts, while the network layer transmits data from one host to another.

1.2.8.2 Packet Forwarding Process

---

1. Encapsulation of IP header by the source PC (includes source & destination IP).
2. Use of routing table by routers to forward packets based on destination IP.

1.2.9 Data Link Layer Details

- PDUs at this layer are called **frames**.

1.2.9.1 Ethernet MAC Addresses

> Each device has a unique MAC address identified by NIC (Network Interface Card) used within an IP network segment for locating devices.

> A MAC address is recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

> Example: **48-A4-72-1C-8F-4F**

1.2.9.2 Address Resolution Protocol (ARP)

ARP (Address Resolution Protocol): helps computers find each other's physical addresses on a network, remembers these addresses, and checks if an IP address is being used by more than one device.

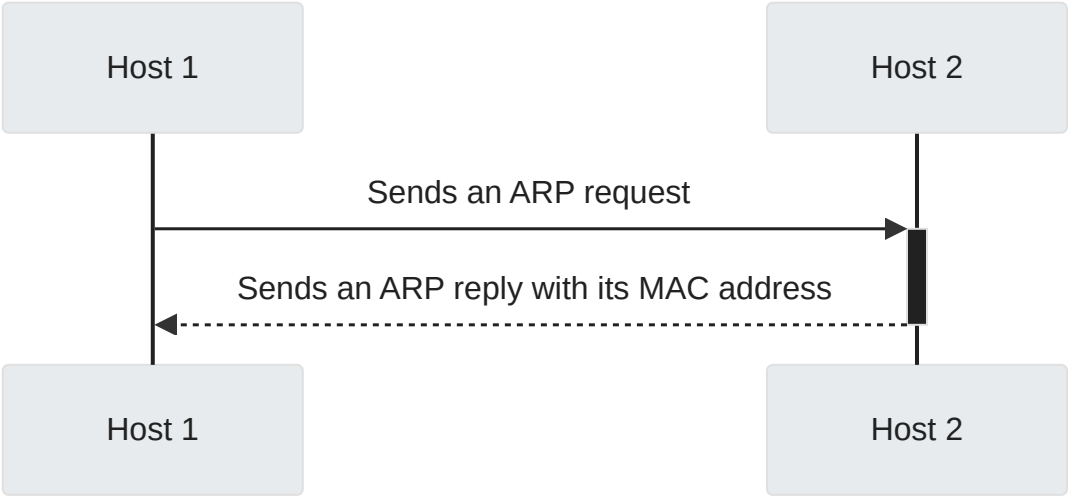
1.2.9.2.1 ARP Process

---

1. **Host 1 checks cached ARP entries**: Host 1 looks up its ARP cache to see if it already knows the MAC address associated with the IP address it wants to communicate with.
2. **Host 1 sends an ARP request**: If Host 1 does not find the MAC address in its cache, it broadcasts an ARP request on the network to ask for the MAC address corresponding to a specific IP address.

> **Broadcast address**: FF-FF-FF-FF-FF-FF
> **Destination MAC address**: all 0s

3. **Host 2 adds an ARP entry**: When Host 2 receives the ARP request and recognizes its own IP address, it updates its own ARP cache with the MAC and IP address of Host 1.
4. **Host 2 sends an ARP reply**: Host 2 responds directly to Host 1 with an ARP reply packet containing Host 2's MAC address.
5. **Host 1 adds an ARP entry**: Upon receiving the ARP reply from Host 2, Host 1 updates its ARP cache with the new information so that it can now send data frames directly to Host 2 using its MAC address.



1.2.10 Physical Layer Overview

PDUs transmitted at the physical layer are called **bitstreams**.

1.2.10.1 Transmission Media Types

1.2.10.1.1 Twisted Pairs (Ethernet)

- **STP**: Shielded Twisted Pairs
- **UTP**: Unshielded Twisted Pairs

1.2.10.1.2 Optical Fibers

Components include fibers themselves and optical modules for signal conversion.

- **Fibers**: are thin strands of glass or plastic that transmit light signals over long distances
- **optical modules**: are devices that convert electrical signals into light for transmission through fibers and then back into electrical signals at the

receiving end.

1.2.10.1.3 Serial Cables

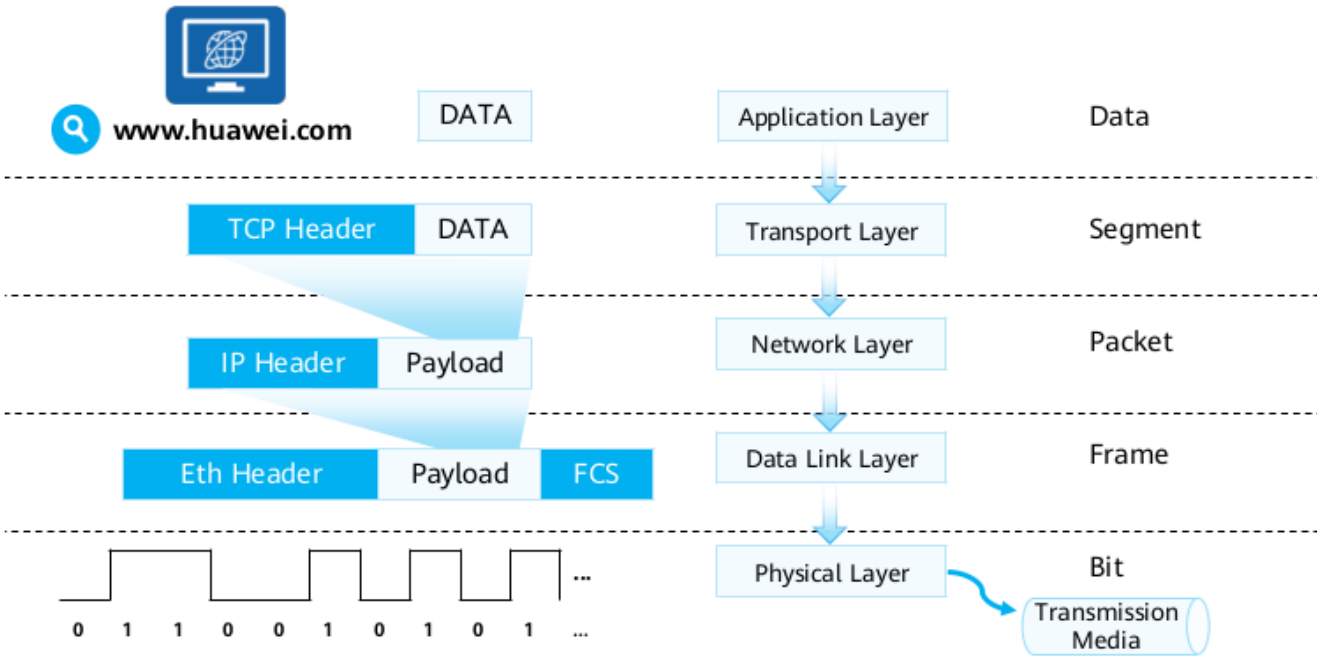
Used in WANs with various interfaces like V.24/V.35.

1.2.10.1.4 Wireless Signals

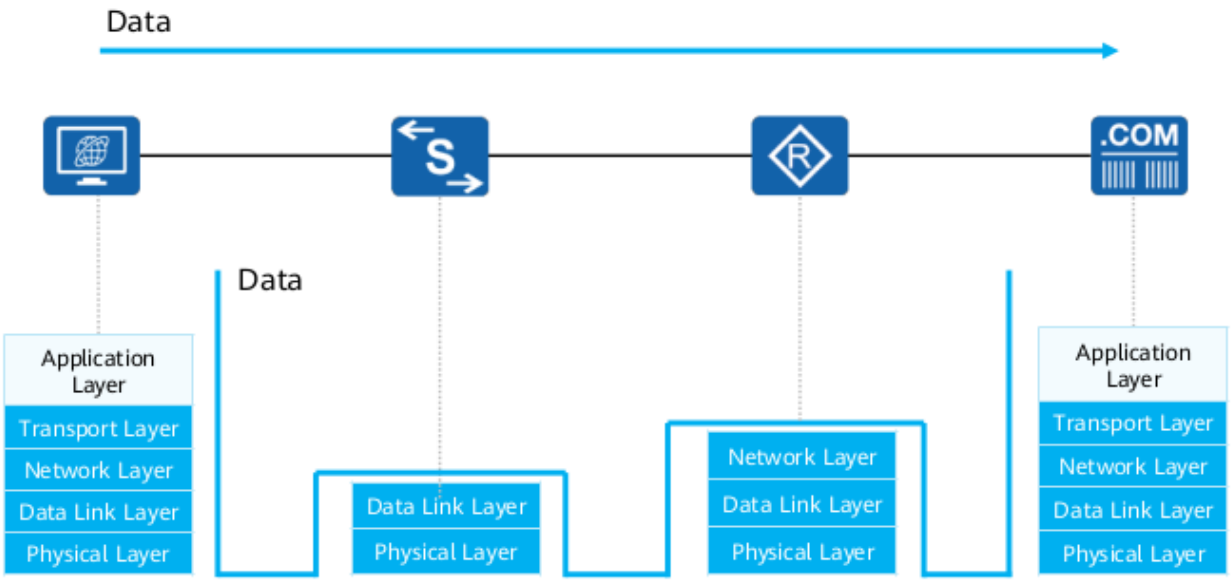
Electromagnetic waves used by devices like wireless routers and mobile phones for data transmission.

1.3 Data Communication Process

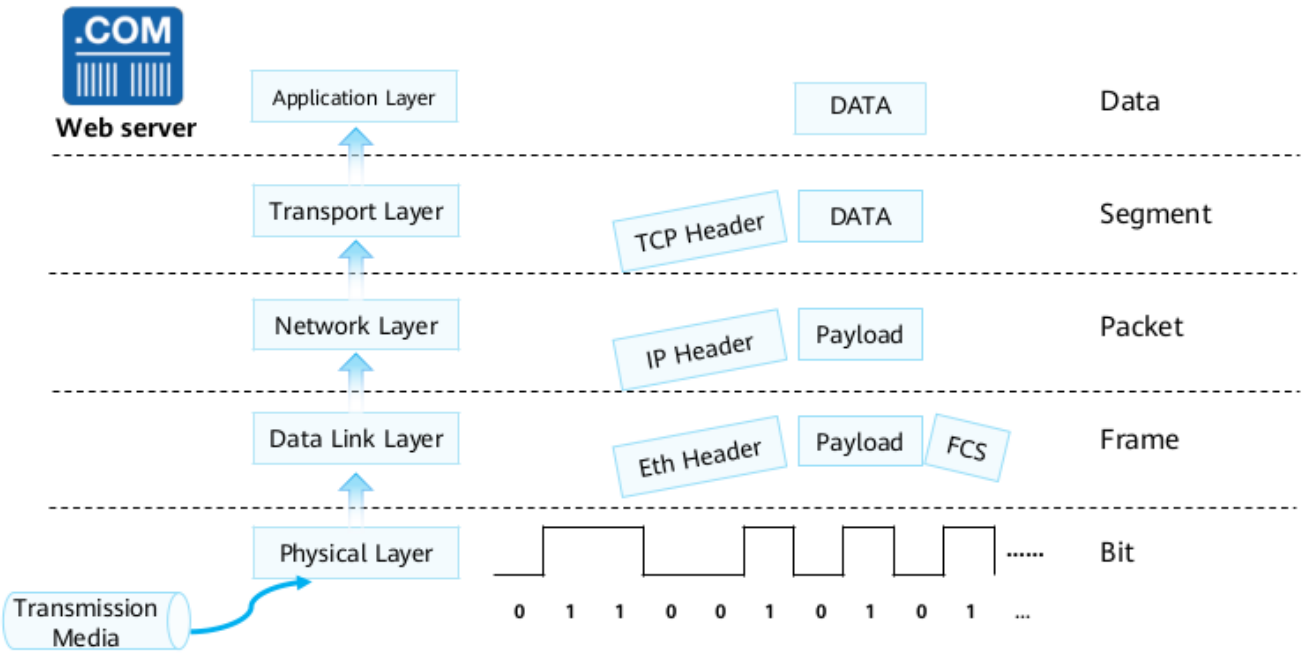
1.3.1 Data Encapsulation on the Sender



1.3.2 Data Transmission on the Intermediate Network



1.3.3 Data Decapsulation on the Receiver



1.3.4 Layered Model Benefits

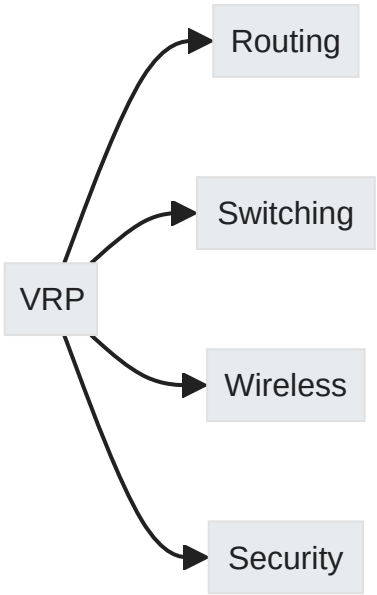
- **Modularity**: Makes it easier to handle and fix parts of the system since they're split into separate chunks.

- **Standardization**: Sets common rules for each part so they work well together.
- **Compatibility**: different tech pieces talk to each other because they share a common language.

Huawei VRP Basics

1 Huawei VRP Basics

1.1 VRP Overview



- The **Versatile Routing Platform (VRP)**: is Huawei's universal OS for datacom products.
- It adopts a component-based architecture and supports IP-based functions.

> designed with modular components that can be combined like building blocks, and it allows for the use of internet protocols to manage network traffic and functions.

- **VRP provides the following functions:**

- Provides a unified user interface and a unified management interface.
- VRP handles network decision-making and sets rules for data routing. (control plane & forwarding plane)
- VRP manages the interaction between the network device's data-handling component and its decision-making component.(control plane & forwarding plane)

1.1.1 Development Stages

Period	Version	Description
1998-2001	VRP1	Centralized design for low to mid-range devices. Low performance.
1999-2000	VRP2	Distributed design used in AR series routers.
2000-2004	VRP3	Distributed platform supporting core routers' features.
2004-Now	VRP5	Component-based design with high performance for various Huawei products. (AR router ,S Switches)
2009-Now	VRP8	Multi-process, component-based architecture optimized for multi-CPU and multi-chassis systems (NE router , CE switches)

1.1.2 File System & Storage Media

1.1.2.1 Common File Types

- **System Software (.cc)**: Essential for device operation.
- **Patch File (.pat)**: Fixes system software bugs.
- **Configuration File (.cfg/zip/dat)**: Contains command configurations.
- **PAF File (.bin)**: Controls product features and resources.

1.1.2.2 Storage Media Types

SDRAM: Stores system running info (like computer memory).
NVRAM: Nonvolatile; stores log buffer files (moved to flash after timer/buffer full).
Flash Memory: Nonvolatile; stores system software/config files.
SD Card: Nonvolatile; large storage capacity used for system files/logs.
USB: Interface for connecting large-capacity storage mediums.

1.1.3 Device Initialization Process

🔌 **After power-on:**

1. BootROM initializes hardware.
2. System software loads from default storage path.
3. Reads configuration file for initialization procedures.

1.1.4 Device management

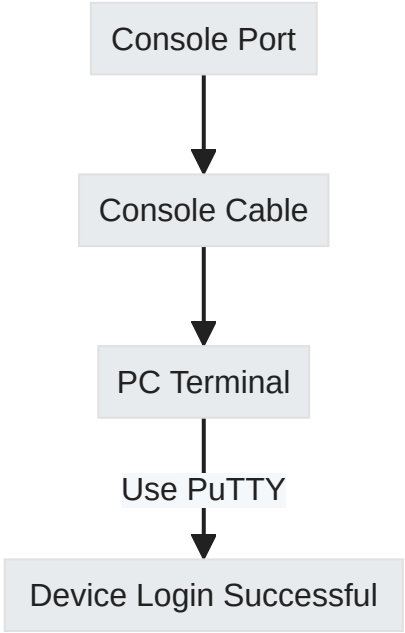
Device management can be done through a user-friendly graphical interface on the web (Web System) or by typing specific commands into a text-based interface (CLI).

1.1.5 Command Line Basics

1.1.5.1 Command Line Overview

1.1.5.1.1 Login Methods

1.1.5.1.1.1 Local Login (Console Port)



> **Tip**
>
> Use console port when configuring a device for the first time.
> set Connection type to **Serial**.
> Set Speed to **9600**.

1.1.5.1.1.2 Remote Login (Telnet/SSH)

SSH default port: `22`
Telnet default port: `23`

> Use PuTTY or similar terminal emulator to initiate connection.

1.1.6 User Levels & Commands Accessible

User Level	Accessible Commands
0	Visit level (e.g., ping)
1 - 2	Monitoring level commands
3	Configuration level
>3	Management level

1.2 Command Line Basics

1.2.1 Command Line Overview

1.2.1.1 Basic Command Structure

- CLI commands follow a unified structure: `Command Word` ➜ `Keyword` ➜ `Parameter List`
  - **Command Word**: Specifies the operation to be executed (e.g., `display`, `reboot`, `ip`).
  - **Keyword**: Further restricts a command, used to express command logic.
  - **Parameter List**: Composed of names and values to further restrict command function.

Command Word → Keyword → Parameter List

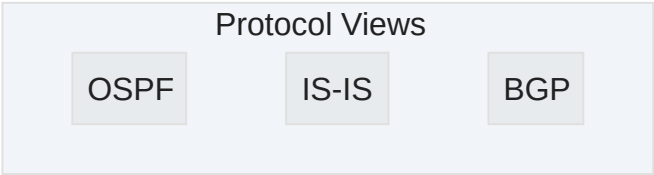
Example

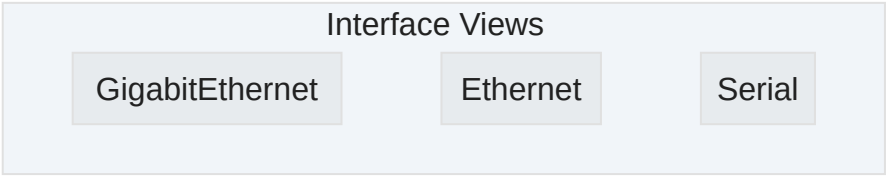
- **Command**: `display ip interface GE0/0/0`
- **Word**: `display`
- **Keyword**: `ip`
- **Parameter Name**: `interface`

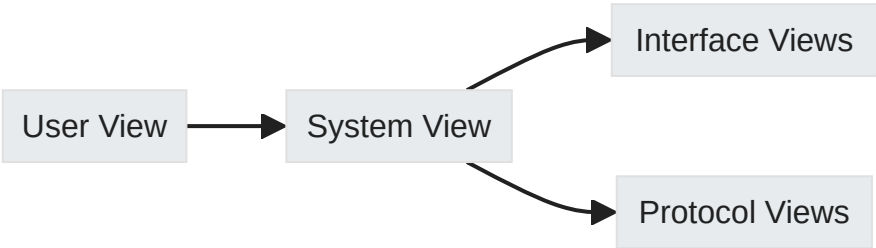
- **Value**: `GE0/0/0`

1.2.1.2 Command Views

Views help categorize commands by function. Common views include:







- **User View** (`<Huawei>`): Check running status; only query and tool commands.
- **System View** (`[Huawei]`): Set system parameters; access other configuration views.
- **Interface/Protocol Views** (e.g., `[Huawei-GigabitEthernet0/0/1]` , `[Huawei-ospf-1]`): Set specific interface or protocol parameters.

> Example:

Markdown

```
<Huawei>system-view     # Enter system view from user view.\
```

```
[Huawei]interface GigabitEthernet 0/0/1  # Enter interface view from system view.
```

1.2.1.3 Editing Commands

Function Key	Description
Backspace	Deletes character before cursor.
← or Ctrl+B	Moves cursor left.
→ or Ctrl+F	Moves cursor right.

1.2.1.3.1 Incomplete Keyword Input

- The CLI allows entering partial keywords if they're unique enough for recognition.

```
<Huawei>d cu                # Correct for 'display current-configuration'
<Huawei>d c                 # Error: Ambiguous command found at '^' position.
```

1.2.1.3.2 Using Tab Key

- Auto-complete keywords with Tab.

1.2.1.4 Command Line Online Help

Use '?' for help:

```markdown
<Huawei> ?                # Full help: Shows all commands in the view.
<Huawei> d?               # Partial help: Shows commands starting with 'd'.
```

1.2.1.5 Undoing Commands

Undo actions with the keyword 'undo':

```markdown
[Huawei]interface g0/0/1                  # Set IP address on interface g0/0/1.
[Huawei-GigabitEthernet0/0/1]undo ip address       # Undo set IP address.
```

1.2.1.6 Shortcut Keys

You can use system shortcut keys for faster operations:

- CTRL+A/Z/X/C/V: Navigation & editing shortcuts within the CLI environment.

1.2.2 Basic Configuration Commands

1.2.2.1 Navigating Directories

- `pwd` - Print Working Directory (Current Directory).
- `cd directory` - Change Directory.

- `mkdir directory` - Make Directory.
- `rmdir directory` - Remove Directory (must be empty).

1.2.2.2 Managing Files

- `dir` - Display files/directories info.
- `more filename` - Display information text about file content.
- `copy source destination` - Copy files.
- `move source destination` - Move files.
- `rename old-name new-name` - Rename file/directory.
- `delete filename` - Delete a file.

1.2.2.3 Recycle Bin Operations

- `undelete` - Restore a deleted file.
- `reset recycle-bin` - Empty recycle bin.

> **Note**
>
> Use `/force` to bypass confirmation prompts when deleting, and `/unreserved` to permanently delete without sending to recycle bin.

1.2.3 Basic Configuration Commands

1.2.3.1 Device Identification and Time Management

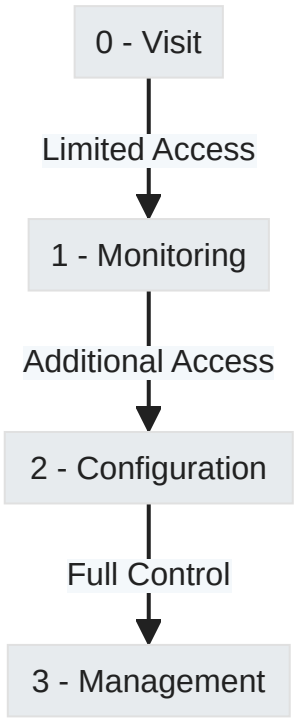
- **System Name**: `[Huawei] sysname name`

> Set unique device identifier.

Command	Description
`clock timezone name {add|minus} offset`	Set local time zone.
`clock datetime [utc] HH:MM:SS YYYY-MM-DD`	Set system or UTC time.(current time)
`clock daylight-saving-time`	Configure DST(daylight saving time) settings.

1.2.3.2 Command Level Configuration

- Configure a command level to restrict access to certain commands based on user privilege levels.



- `command-privilege level <level> view <view-name> <command-key>`

1.2.3.3 Password-based Login Mode

- Set up password authentication for remote logins via VTY (Virtual Terminal Line).
- a maximum of 15 users can log in to a device through VTY at the same time.
- Enter VTY interface: `user-interface vty 0 4`
- Set password: `set authentication password cipher <password>`

1.2.3.4 User Connection Timeout

- Configure the timeout period for inactive user connections.
- Command: `idle-timeout <minutes> [seconds]`
- Default: 10 minutes

1.2.3.5 Interface IP Address Configuration

- Assign an IP address to a device's physical or logical interface.
- Enter interface configuration mode: `interface <interface-number>`
- Set IP address: `ip address <ip-address> {<subnet-mask>|<mask-length>}`

1.2.3.6 Viewing and Saving Configurations

1.2.3.6.1 Display Current Configurations

- View the currently active configuration settings on the device.
- `display current-configuration`

1.2.3.6.2 Save Configurations

- Persist the current configurations to memory.
- `save`

1.2.3.6.3 Check Saved Configurations

- Review the saved configuration file in memory.
- `display saved-configuration`

1.2.4 Clear Saved Configurations

- Remove all saved configurations from memory.
- `reset saved-configuration`

1.2.5 System Startup Parameters

- Check parameters that determine system behavior on startup.
- `display startup`

1.2.6 Configure Startup File

- Set which configuration file to use on next system startup.
- `startup saved-configuration <configuration-file>`

1.2.7 Restart Device

- Restart the device with or without saving changes first.
- `reboot`

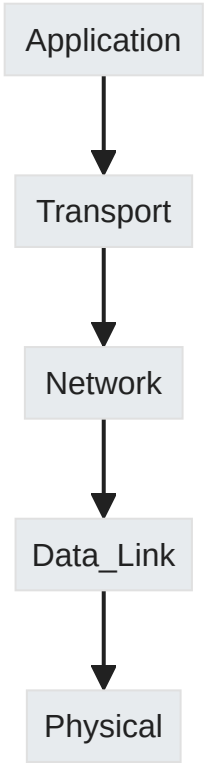
Network Layer Protocols and IP Addressing

1 Network Layer Protocols and IP Addressing

1.1 Network Layer Protocols

- Referred to as the IP layer, includes protocols like ICMP and IPX in addition to IP.
  - **ICMP (Internet Control Message Protocol):** A protocol for sending alerts about network issues like unavailable services or unreachable devices.
  - **IPX (Internetwork Packet Exchange):** An old protocol for sending data across Novell NetWare(Software) networks, now largely Outdated.
  - **IP (Internet Protocol):** The main protocol for sending data packets across the internet using unique addresses.

1.1.1 TCP/IP Model Layers



1.1.2 Protocols Overview

- **IP (Internet Protocol)**: know as logical address since its changed due to multiple reasons
  - **IPv4:** Standard internet protocol with 32-bit addresses.
  - **IPv6:** Newer version with 128-bit addresses for increased address space.

1.1.3 Data Encapsulation

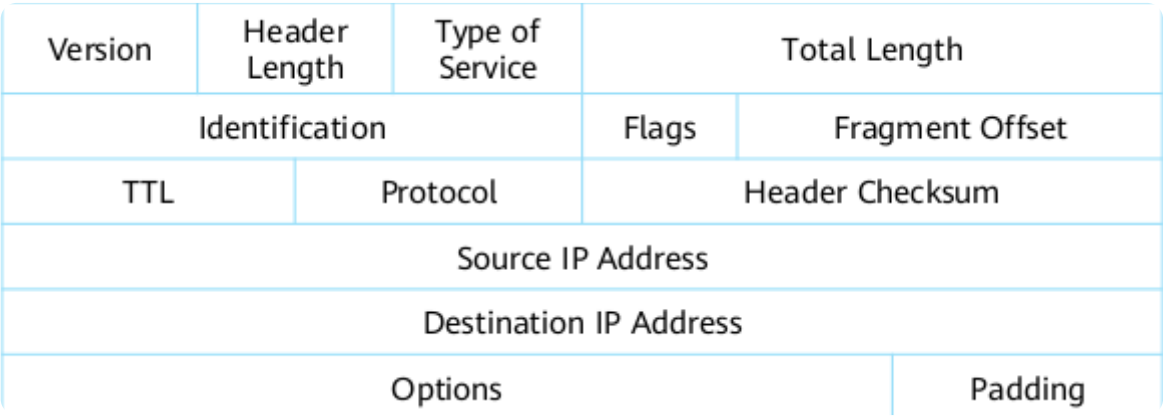
Data transfer involves encapsulating data at each layer with specific headers.

Layer	PDU Name	Header Added
Application	Data	None
Transport	Segment	TCP/UDP
Network	Packet	IP

Layer	PDU Name	Header Added
Data Link	Frame	Ethernet

> 💡 Encapsulation wraps data with necessary protocol information before transmission across a network.

1.1.4 IPv4 Packet Format



Component	Size (Bits)	Description
Version	4	Indicates the IP version (IPv4) or (IPv6).
Header Length	4	Specifies the header size in 32-bit words. Minimum value is 5 (indicating 20 bytes) without options.
Type of Service	8	Used for Quality of Service (QoS); directs routers to handle the packet with a certain level of precedence.
Total Length	16	The entire packet size, including header and data, in bytes. Maximum size is 65,535 bytes.
Identification	16	A unique identifier for fragmented packets to aid in reassembly at the destination.
Flags	3	Control flags related to fragmentation (e.g., whether a packet can be fragmented).
Fragment Offset	13	Indicates where in the original data this fragment belongs; used during reassembly of

Component	Size (Bits)	Description
		fragmented packets ; to help the receiver assemble the fragments.
Time to Live (TTL)	8	Limits the packet's lifespan; decrements on each router hop and discards if it reaches zero to prevent looping.
Protocol	8	Identifies the protocol of the encapsulated data (e.g., TCP, UDP). 1 : ICMP 2 : IGMP 6 : TCP 17 : UDP
Header Checksum	16	A checksum used for error-checking the header only; recalculated at each hop.
Source IP Address	32	The IP address of the originating host sending the packet.
Destination IP Address	32	The intended recipient's IP address for this packet.
Options	Variable	Optional parameters for additional features; rarely used and not included in minimum header length calculation.
Padding	*Variable*	*Used to ensure that the header's length is a multiple of 32 bits; filled with zeros.*

- **Flags** & **Fragment Offset**: Used during packet fragmentation and reassembly to ensure packets are properly reconstructed.
- The Flags field is 3 bits long
  1. **Reserved Fragment (bit):** Always set to 0; not used.
  2. **Don't Fragment (DF) bit:** If 1, the packet can't be split; if 0, it can be.
  3. **More Fragments (MF) bit:** If 1, more packet pieces are coming; if 0, this is the last or only piece.

🔑 TTL prevents infinite loops by discarding packets after they pass through a certain number of routers.

> Default is **255**

1.2 Introduction to IPv4 Addresses

IP Address —Identifies→ Node on Network —Used For→ Data Forwarding

> An IP address uniquely identifies a node on a network and is used to forward data packets.

1.2.1 Address Notation & Range

- **IPv4:** 32 bits long in dotted decimal notation (e.g., `192.168.10.14`).
- **Range:** `0.0.0.0` to `255.255.255.255`.
- Conversion between decimal and binary systems
- 192

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	0	0

1.2.2 IP Address Structure

- **Network part:** Identifies the network.
- **Host part:** Identifies hosts within that network.

> 💡 Network **mask/subnet mask**: distinguishes between these two parts.

1.2.2.1 Example of Structure and Notation

Example

IP address: 192.168.10.1
Network mask: 255.255.255.0 or /24 notation.
Network part is: 192.168.10.0
Host part is: 0.0.0.255

1.2.3 Classification of Addresses (IPv4)

Class	Leading Bits	Address Range	Default Mask	Purpose
A	0xxx...	`0.0.0.0–127.255.255.255`	`/8`	Large networks
B	10xx...	`128.0.0.0–191.255.255.255`	`/16`	Medium networks
C	110x...	`192.0.0.0–223.255.255.`	/24	Small networks

Calculation
A :

1	**0**	**0**	**0**	**0**	**0**	**0**	**0**
128	0	0	0	0	0	0	0

$$0 - 128 - > 127$$

Calculation

Same idea for B , C same as A but with more leading 1's

🌐 Classes D (`224.x.x.x–239.x.x.x`) for multicast and E (`240.x.x.x–254.x.x.x`) for research are not typically assigned to hosts.
Multicast address: is used to implement one-to-multiple message transmission.

1.2.4 IP Address Types

- **Network address/network ID:** identifies a network.
- **Broadcast address:** a special address used to send data to all hosts on a network ; last address of the network ID.
- **Available addresses:** IP addresses that can be allocated to device interfaces on a network ; address after network ID till Broadcast address.

Number of available addresses: $2^n–2$ (n is the number of bits in the host part).
-2 for broadcast and network id.

1.2.4.1 IP Address Calculation

What are the network address, broadcast address, and number of available addresses of class B address 172.16.10.1/16?

Example

Network ID: 172.16.0.0
Broadcast address: 172.16.255.255
Number of available addresses: $2^{16} - 2 = 65534$
Range of available addresses:

$$172.16.0.1 - 172.16.255.254$$

1.2.5 Private vs Public IPs

Private IP Addresses

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0–192.168.255.255

Public IP Addresses

Allocated by IANA, unique across the Internet.

> Private IPs require **NAT** to communicate with public networks.

1.2.5.1 Special IPv4 Addresses

Use Case	Address	Function
Broadcast	255.255.255.255	Used to send a message to all devices on the local network.
Any Network	0.0.0.0	Represents an unspecified host or the default network; used as a source address for devices seeking to obtain an IP assignment.
Loopback	127.0.0.0/8	Used by a host to send traffic to itself for testing or inter-process communication.
Link-local	169.254.0.0/24	Automatically assigned to a device for local communications when no external DHCP server is available.

1.2.6 IPv4 vs IPv6 Comparison

Feature	IPv4	IPv6
Length	32 bits	128 bits
Address Types	Unicast, Broadcast, Multicast	Unicast, Multicast, Anycast
Characteristics		
Address Availability	Limited number of addresses	Virtually unlimited number of addresses
Packet Header Design	Not as efficiently designed	Simplified packet header for more efficient routing
Network Dependency	ARP dependency can cause flooding	Automatic address allocation reduces dependencies

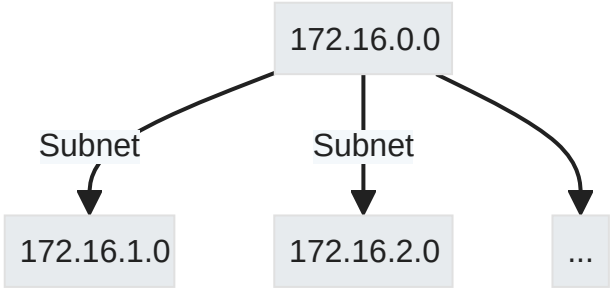
1.3 Subnetting

> **Why Subnetting?**
> Reduces broadcast domains, increases network efficiency, and improves IP address usage.

- **technique:**
  - **VLSM (Variable Length Subnet Masking):** A technique that allows network administrators to divide an IP address space into subnets of different sizes, optimizing the use of IP addresses based on the varying needs of each subnet.
  - **FLSM (Fixed Length Subnet Masking):** A subnetting approach where all subnets are created equal in size, using a consistent subnet mask, which can lead to inefficient use of IP addresses if subnets have widely differing numbers of hosts.

1.3.1 Class B Address Example

> Example 172.16.0.0 to subnets each subnet support 200 user



Subnet	Network ID	Network Broadcast	Available Address
Subnet 1	172.16.1.0	172.16.1.255	$2^8 - 2 = 254$
Subnet 2	172.16.2.0	172.16.2.255	$2^8 - 2 = 254$
Subnet X	172.16.X.0	172.16.X.255	$2^8 - 2 = 254$

Tip

- Take bits from the host part to create a subnet.
- Use Variable Length Subnet Mask (VLSM) for efficiency.

1.4 ICMP (Internet Control Message Protocol)

Role & Uses:

- Helper protocol used alongside IP.
- Handles error messages and Functioning info.
  ICMP Types:

Type	Code	Description
0	0	Echo Reply
3	0-3	Destination Unreachable
5	0	Redirect
8	0	Echo Request

> ⚠ **Warning**
>
> ICMP can be exploited for network attacks; thus, it should be properly secured.

> ICMP Redirect messages are sent by routers to tell a computer to use a more direct route for sending data to its destination, improving network efficiency.

> Ping uses ICMP **(Echo Request and Echo Reply)** to test if a computer can communicate with another on the network, measuring how long it takes for messages to go back and forth.

> ICMP is a protocol (**Tracert**) that helps identify network issues by sending error messages, like "Destination Unreachable," when data can't reach its intended target. The Tracert tool uses ICMP to map the route data takes to its destination by sending packets with increasing TTL values until the packets reach their endpoint, returning timing information at each hop.

1.5 IPv4 Address Configuration & Basic Application

Configuration Steps:

1. **Enter Interface View:**

Markdown

```
[Huawei] interface <interface-type> <interface-number>
```

2. **Assign IP Address:**

Markdown

```
[Huawei-GigabitEthernet0/0/1] ip address <ip-address> {
<mask> | <mask-length> }
```

> **mask:** specifies a subnet mask. The value is in dotted decimal notation.
> **mask-length:** specifies a mask length. The value is an integer ranging from 0 to 32.

1.5.1 Logical vs Physical Interfaces:

Physical interfaces are Physical ports on devices whereas logical interfaces like VLANIF or Loopback are virtual and always up.

> A device deletes data not meant for its IP if it's routed through Loopback interface.

1.5.2 Network IP Address Planning

Objectives:

- **Uniqueness:** Each device on the network must have a distinct IP address to avoid conflicts.
- **Continuity:** The range of IP addresses should be contiguous to simplify routing and network management.
- **Scalability:** The plan should accommodate future growth without major changes to the existing structure.
- **Easy Management:** The address scheme should be logical and structured to make administration tasks straightforward.
- **High Utilization:** Efficient use of assigned IP spaces to minimize waste and maximize the available address pool.

IP Routing Basics

1 IP Routing Basics

1.1 Overview of IP Routing

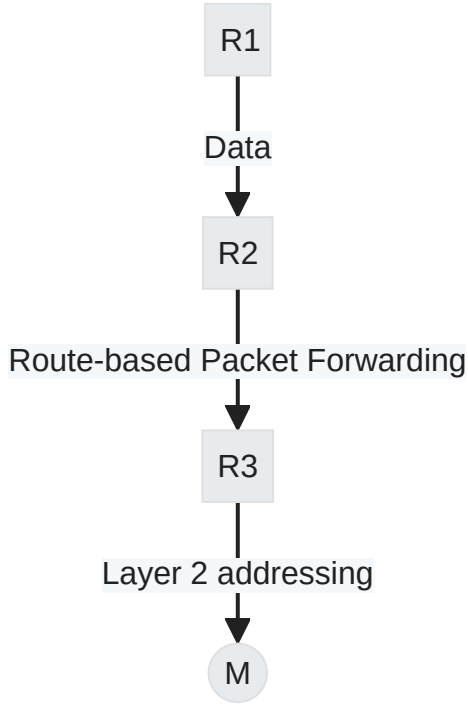
1.1.1 Basic Concepts of Routing

- **Subnet**: A segment of a network with its own unique IP address range.
- **Inter-Subnet Communication**: Necessary for different subnets to communicate.
- **Routes:** are the path information used to guide packet forwarding.
- **Routing Devices:** are crucial for directing traffic through the network based on predefined routes.

> In Huawei networking devices, physical interfaces with IP addresses also have MAC addresses for Layer 2 communication, except for logical or virtual interfaces like loopbacks or tunnels that don't handle Ethernet frames.

1.1.1.1 Routing Devices and Tables

- **Router**: determine the path for an IP packet using the destination address and forward it accordingly.
- The **last-hop router** performs Layer 2 addressing before passing the packet to its final destination.
    - translate the IP address into a format that can be understood at the local network level



1.1.1.2 Routes and Routing Information

A routing entry contains several key components:

- **Destination**: Identifies which subnet the packet is intended for.
- **Mask**: Works with the destination IP to specify the subnet.
- **Outbound Interface**: The interface from which a packet leaves the router.
- **Next Hop**: The address of the next device in line towards the packet's final destination.

> **Example of an IP routing table:**

- Routers discover routes using multiple methods.
- A router selects the optimal route and installs it in its IP routing table.
- The router forwards IP packets based on routes in the IP routing table.

Destination/Mask	Outbound Interface	Next Hop
`10.1.1.0/24`	`GE0/0/0`	`1.1.1.2`

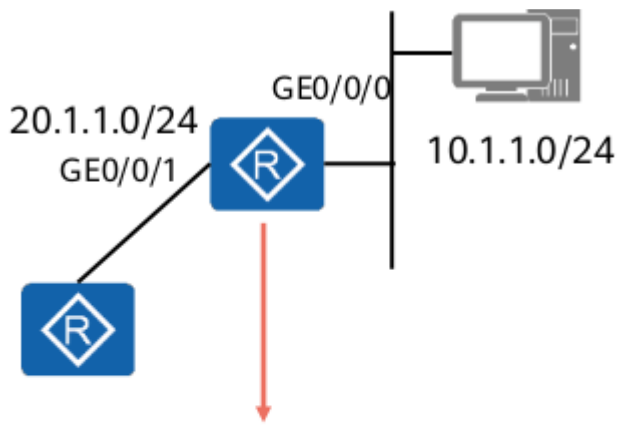
1.1.2 Generation of Routing Entries

1.1.2.1 Direct Routes

- Generated automatically for directly connected networks.

> Generated for interfaces with both physical and protocol status 'up'.

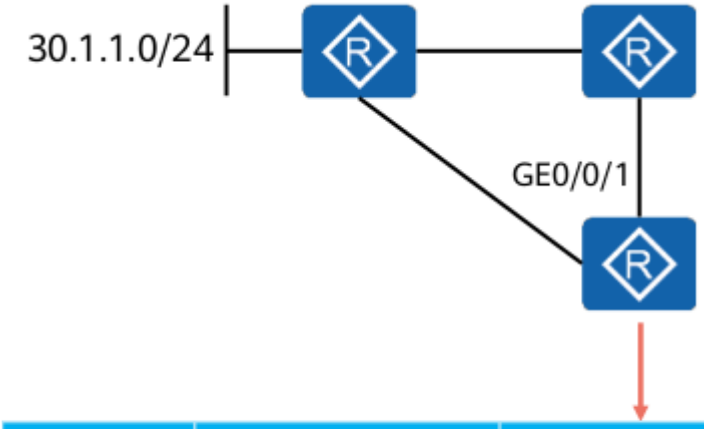
- Utilized by last-hop routers to deliver packets directly to hosts.
  - ARP entries are used to forward packets directly without a next hop since Local use **Mac**.



Protocol	Destination/Mask	Outbound Interface
Direct	10.1.1.0/24	GE0/0/0
Direct	20.1.1.0/24	GE0/0/1

1.1.2.2 Static Routes

- Manually configured by network administrators.
- Deterministic routes to specific destinations.

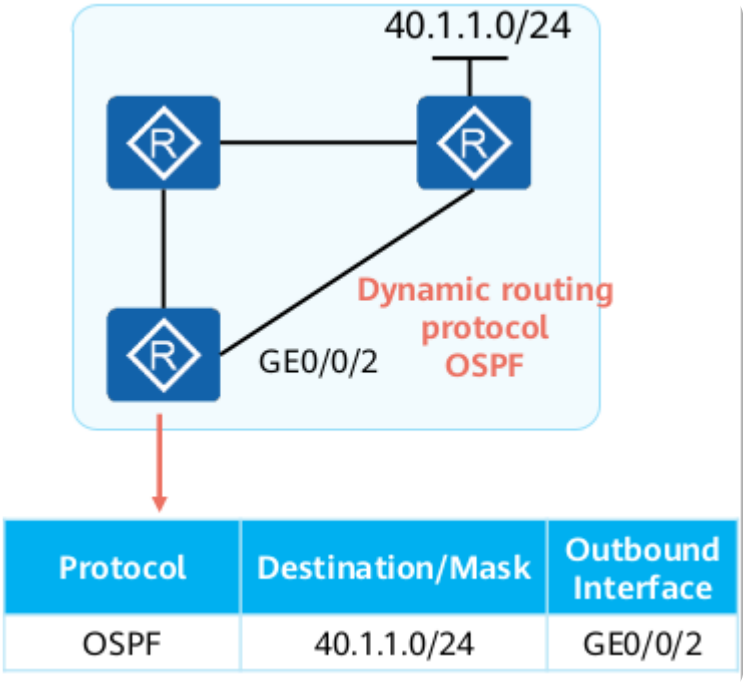


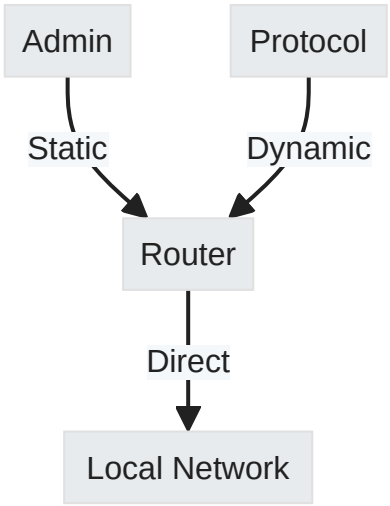
Protocol	Destination/Mask	Outbound Interface
Static	30.1.1.0/24	GE0/0/1

1.1.2.3 Dynamic Routes

- Learned through dynamic routing protocols such as OSPF or BGP.

> automatically adapts to network changes.





1.1.3 Optimal Route Selection

1.1.3.1 Key Terms

Destination/Mask	Protocol	Pre	Cost	Flag	NextHop	Interface
1.1.1.1/32	Static	60	0	D	0.0.0.0	NULL0
2.2.2.2/32	Static	60	0	D	100.0.0.2	Vlanif100
100.0.0.0/24	Direct	0	0	D	100.0.0.1	Vlanif100
100.0.0.1/32	Direct	0	0	D	127.0.0.1	Vlanif100

Destination/Mask	Protocol	Pre	Cost	Flag	NextHop	Interface
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack(
127 .00 .01 /32	Direct	0	0	D	127.0.0.1	InLoopBack(

- **Routing Table**: A database used by routers to determine the best path for forwarding packets.
- **Route Preference (Pre)**: Used to select routes from different protocols; lower values indicate higher priority.

Destination/Mask	Protocol	Preference	Next Hop
10.0.0.0/30	Static	**60**	30.1.1.2
10.0.0.0/30	OSPF	**10**	20.1.1.2

Installed in the IP routing table

- **Flag**: indicates special statuses or attributes of a particular route

Flags

- **R** - Relay
- **D** - Downloaded to Forwarding Information Base (FIB)

> **Forwarding Information Base (FIB):** table used by network routers and switches to determine where to forward packets; it contains the necessary information to make routing decisions for outgoing network traffic.

Forwarding Information Base (FIB) vs ip table

> The Forwarding Information Base (FIB) is primarily used in routers to make quick forwarding decisions based on pre-computed routes, whereas an IP table, often associated with firewalls or servers, holds rules for packet filtering and network address translation rather than routing.

- **Cost (Metric)**: Used when comparing routes from the same protocol; lower values indicate preferred routes.

- **Metrics** can include **hop count**, **bandwidth**, **delay**, **cost**, **load**, and **reliability**.

Destination/Mask	Protocol	Cost	Next Hop
10.0.0.0/30	OSPF	**20**	20.1.1.2
10.0.0.0/30	OSPF	**10**	30.1.1.2

Installed in the IP routing table

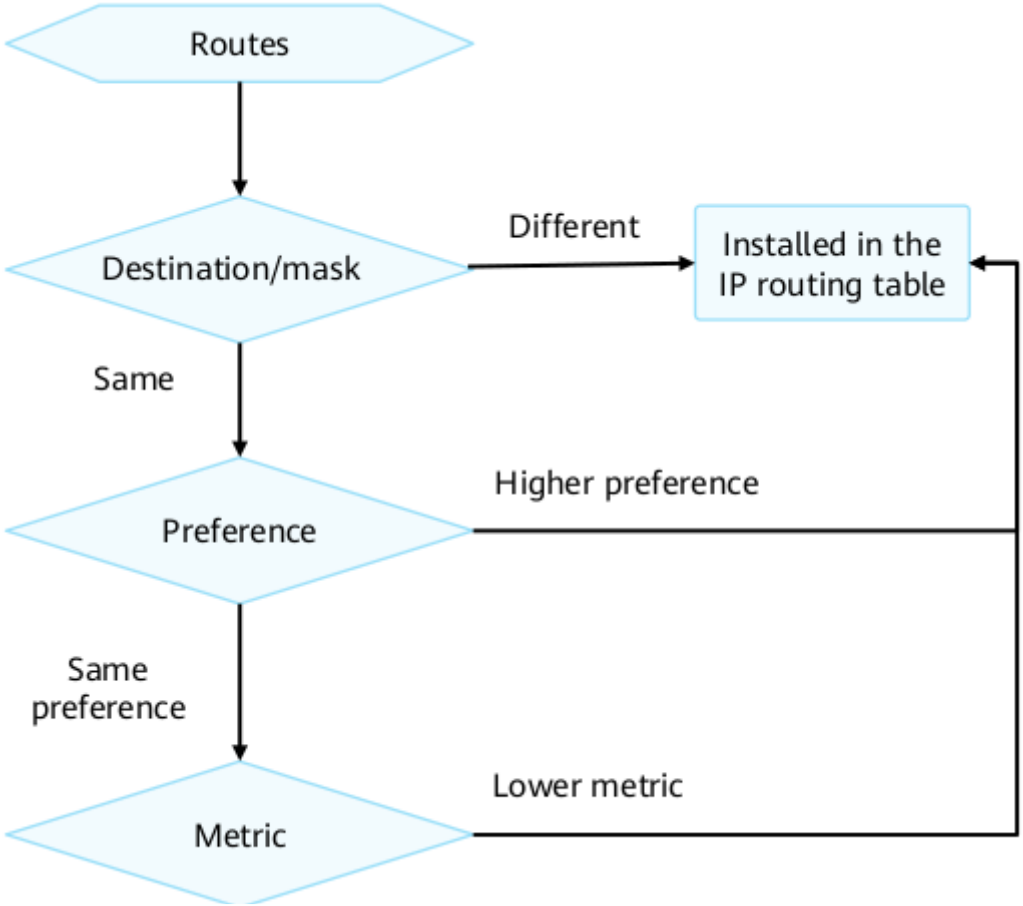
- **Next Hop**: The address of the next device packets are forwarded to en route to their final destination.
- **Interface**: The local interface through which packets are sent from the router.

1.1.3.2 Route Types and Preferences

Protocol	Route Type	Default Preference
Direct	Direct route	0
Static	Static route	60
OSPF	Internal route	10
OSPF	External route	150

1.1.3.3 Route Installed procedure

> Routes –> Destination/mask –> Preference –> Metric



1.1.4 Route-based Forwarding

1.1.4.1 Key Concepts

- **Longest Match Forwarding**: Routers compare the destination IP address bit by bit with routing table entries to find the longest matching prefix.

Longest Matching Mechanism

- Given Destination IP: `172.16.2.1`
  - **Routing Entries:**
  - 172.16.0.0/16 (255.255.0.0)
  - 172.16.2.0/24 (255.255.255.0)

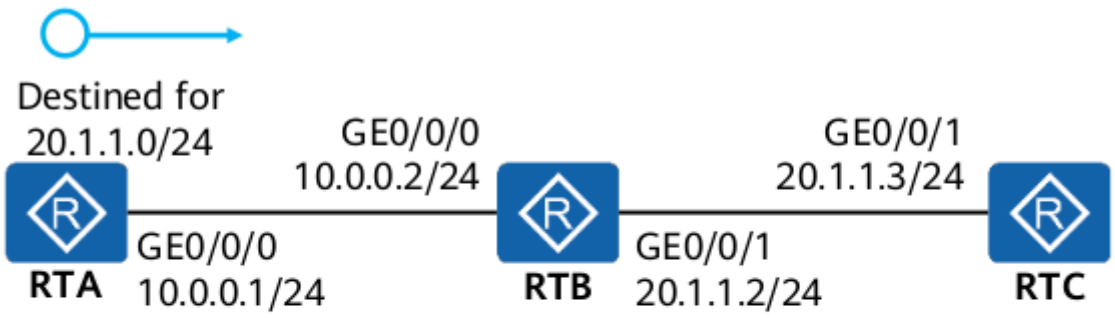
> The router will select `172.16.2.0/24` as it has a longer match (more specific network).

1.2 Static Routing

1.2.1 Key Points

- **Manually Configured**: Network administrators need to manually set up static routes.
- **System Requirements**: Static routes have lower system requirements compared to dynamic routing protocols.
- **Network Size**: Ideal for simple, stable, and small networks.
- **Lack of Adaptability**: One disadvantage is that static routes cannot automatically adapt to network changes.

1.2.1.1 Scenario Example



Destination	Protocol	Next Hop
20.1.1.0	Static	10.0.0.2
10.0.0.0	Direct	10.0.0.1

> In the example above, `RTA` needs to route traffic destined for `20.1.1.0/24` via `RTB` at `10.0.0.2`.

1.2.2 Configuration Commands

1.2.2.1 Static Route

Markdown

```
[Huawei] ip route-static ip-address { mask | mask-length } <nexthop-address>
```

> Used in Broadcast interface (for example, an Ethernet interface) or a virtual template (VT) interface, you must specify the next hop. since in Broadcast their usually switch and switch connected to multiple port but in router side it connected with one port only

1.2.2.2 Outbound Interface Specification

Markdown

```
[Huawei] ip route-static ip-address { mask | mask-length } <interface-type> <interface-number> [nexthop-address]
```

> Used in point-to-point interface (such as a serial interface), you must specify the outbound interface. since in point-to-point interface their is just two port.

1.2.2.3 Configuration Example

```
[RTA] ip route-static 20.1.1.0 255.255.255.0 10.0.0.2
[RTC] ip route-static 10.0.0.0 255.255.255.0 S1/0/0
```

1.2.3 Default Routes

- Default routes (`ip route-static 0.0.0.0 0.0.0.0`) are special static routes that match any destination address not found in the routing table.

1.2.3.1 Application Scenarios

> Default routes are typically used at the egress of an enterprise network or on edge devices connecting to larger networks like the Internet.

1.2.3.1.1 Configuration Example

```
[RTA] ip route-static 0.0.0.0 0 10.0.0.2
```

1.3 Dynamic Routing

1.3.1 Dynamic Routing Overview

Dynamic routing protocols automatically manage the routing process, adapting to topology changes and reducing administrative workload.

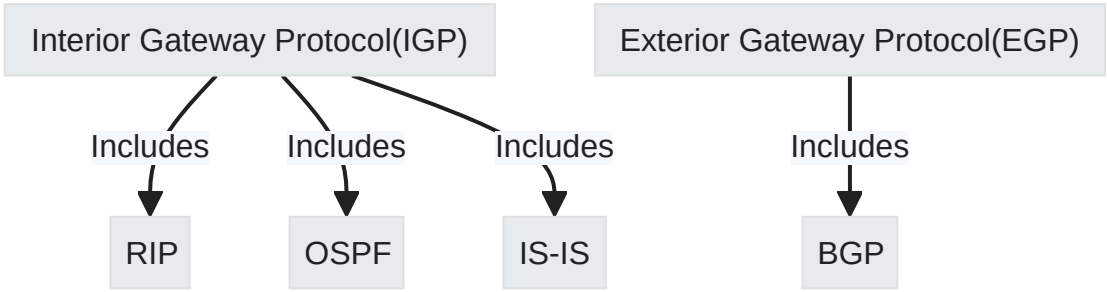
> **Administrative workload:** tasks and activities that network administrators must perform to keep a network running smoothly. This includes configuring routers, updating routing tables, fixing network issues, and adjusting settings when the network changes.

1.3.1.1 Advantages of Dynamic Routing

- **Automatic Discovery**: Routes are learned without manual configuration.
- **Adaptability**: Can adjust to network topology changes dynamically.

1.3.1.2 Classification of Dynamic Routing Protocols

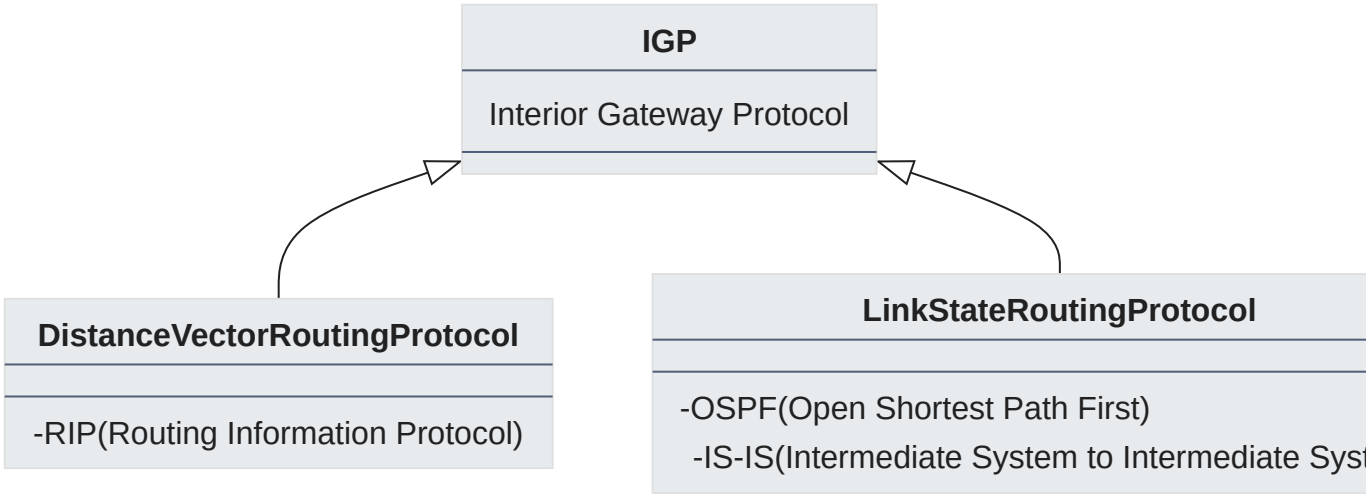
1.3.1.2.1 By Application Scope



- **IGPs:** run within an autonomous system (AS)
- **EGP:** runs between different (ASs)

> **Autonomous System (AS):** is a collection of IP networks and routers under the control of one or more network operators that presents a common routing policy to the internet.

1.3.1.2.2 By Working Mechanism (Classification under IGP)



> **BGP (Border Gateway Protocol):** is sometimes classified as a path-vector protocol due to its enhancement over distance-vector algorithms.

> **A path-vector protocol:** is a network routing protocol that keeps track of the full paths (or sequences of autonomous systems) that data packets travel through to reach their destination, rather than just the distance or metric to the next hop.

1.4 Advanced Routing Features

1.4.1 Route Recursion

- **Definition**: Recursive lookup in IP routing table when next-hop is not directly connected.

Example

- Static route to `30.1.2.0/24` via `20.1.1.3` on RTA.
- If no directly connected route to `20.1.1.3` , route is not usable and cannot be installed in the IP routing table.

- **Solution**:
  - Configure static route to next-hop's network (e.g., RTA's route to `20.1.1.0/24` via `10.0.0.2`).
  - like configure another static route to learn about the next hop of static route in the example `20.1.1.3`

```
[RTA] ip route-static 30.1.2.0 24 20.1.1.3
                                  Recursion
[RTA] ip route-static 20.1.1.0 24 10.0.0.2
```

> **Main Benefit:** Minimized Routing Information**: It keeps the routing information concise on RTA without the need to know all the individual subnets behind other routers.

1.4.2 Equal-Cost Route

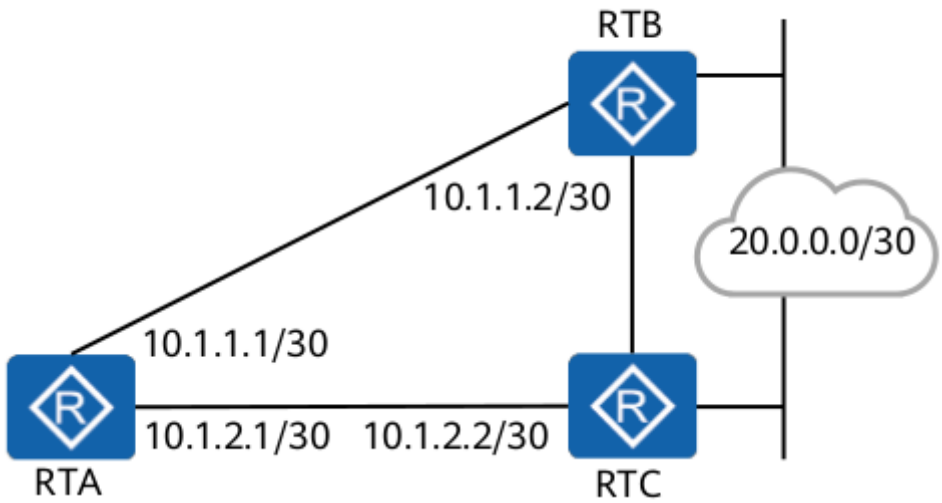
- Routes with identical costs used for load balancing.

RTA's IP routing table

Destination/Mask	Next Hop
10.0.0.0/30	20.1.1.2
	30.1.1.2

1.4.3 Floating Route

- Backup routes with higher preference values than primary routes.
- Used when the primary route is down.



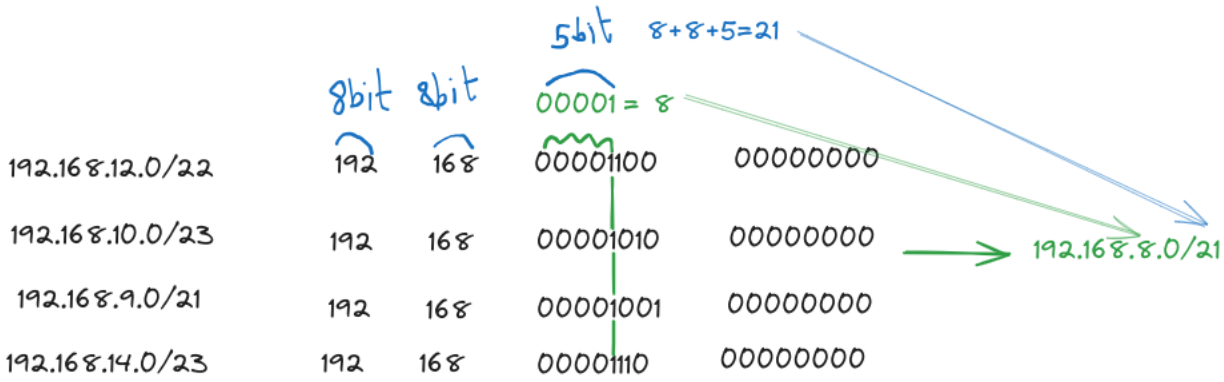
- Configure a floating route on RTA.

```
[RTA] ip route-static 20.0.0.0 30 10.1.1.2
[RTA] ip route-static 20.0.0.0 30 10.1.2.2  preference 70
```

-

1.4.4 CIDR (Classless Inter-Domain Routing)

- Replaces classful addressing with variable subnet masks (VLSM).
- Allows for more efficient use of IP space through aggregation.



-

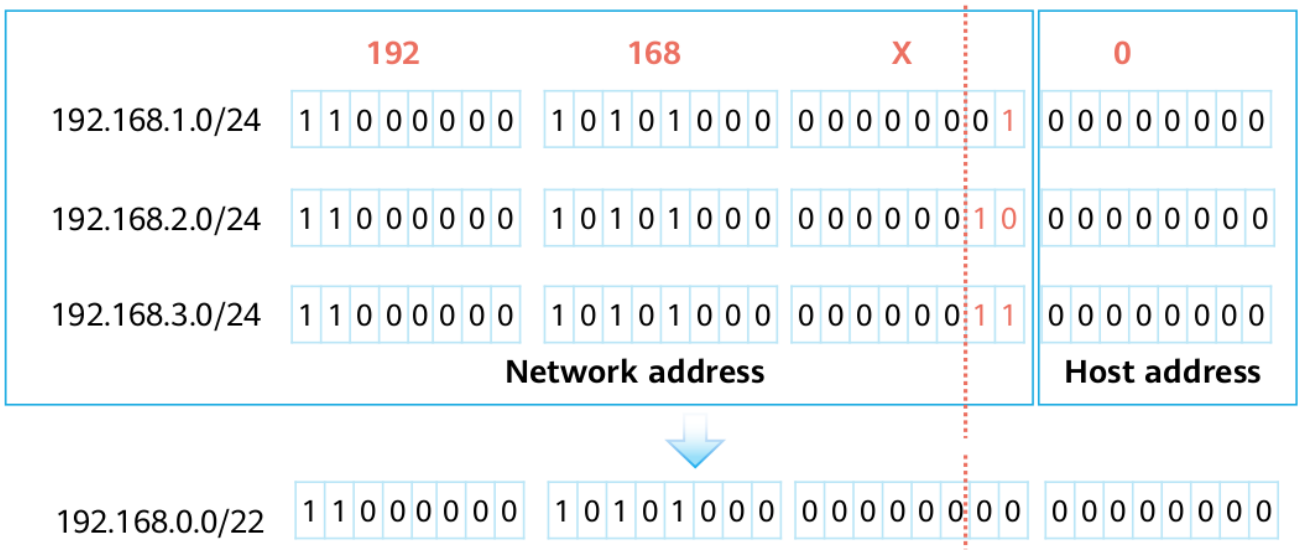
> take the all bit similar until reaching different bit

1.4.5 Route Summarization (Aggregation)

- Combines multiple routes into one summary route to reduce routing table size and conserve resources.

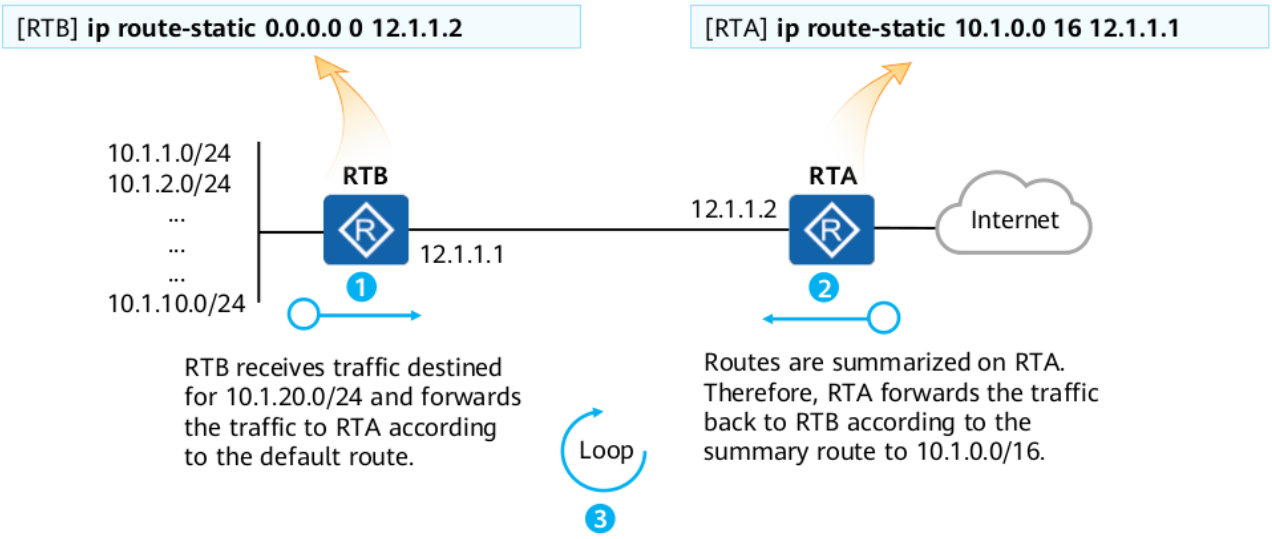
Example

- Before Summarization:
  - $10.1.1.0/24, 10.1.2.0/24, \ldots\ldots, 10.1.10.0/24$
- After Summarization:
  - $10.1.0.0/16$ (covers all above subnets)



1.4.6 Problems with Summarization

1.4.6.1 Routing Loops



> Route summarization on RTA for the 10.1.0.0/16 network can cause a routing loop. When RTB receives traffic for a non-existent subnet like 10.1.20.0/24, it sends it to RTA based on its default route. However, due to the summary route, RTA sends the traffic back to RTB, creating a loop.

> **Solving Routing Loops:**
> Configure routes pointing to Null interface (e.g., Null0) as a safety measure since the interface is always up and its do discard for every packet Therefore, such a route is called a black-hole route.

1.4.6.2 Accurate Summarization

- Ensure that summarized routes are accurate and do not include unintended networks.
- Use Exact mask lengths to avoid over-summarizing.

OSPF Basics

1 OSPF Basics

1.1 OSPF Overview

1.1.1 Static vs Dynamic Routing Protocols

Static Routes

- Manually configured.
- Must be manually adjusted if topology changes.
- Suitable for small or stable networks.

Dynamic Routing Protocols

- Highly flexible, reliable, and scalable.
- OSPF is a common dynamic protocol used in live networks.

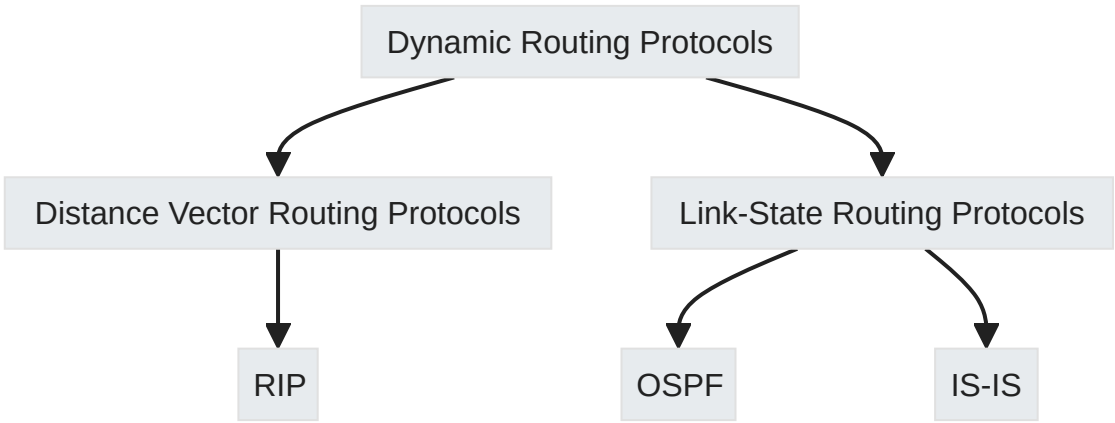
- Must be manually adjusted if topology changes.

  - Suitable for small or stable networks.

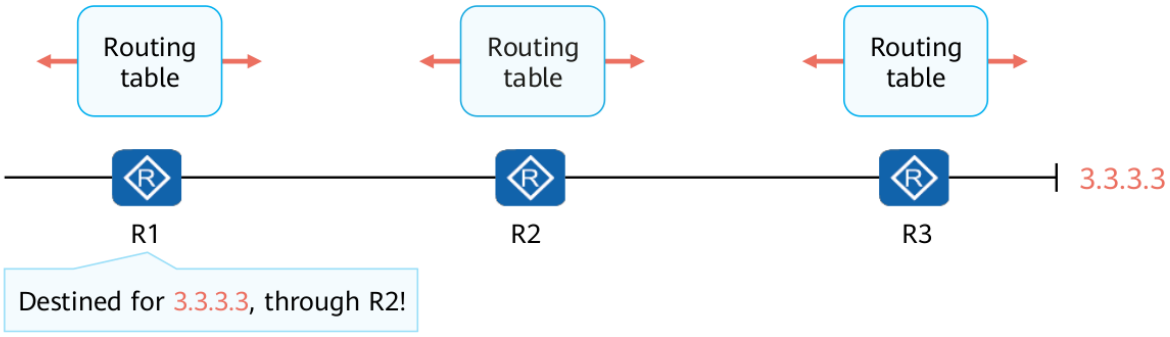
Dynamic Routing Protocols

- Highly flexible, reliable, and scalable.
- OSPF is a common dynamic protocol used in live networks.

1.1.2 Classification of Dynamic Routing Protocols



1.1.3 Distance-Vector Routing Protocol

- Distance-vector routing protocols allow routers to determine the best path to a destination based on distance.
- Routers periodically share their routing tables with immediate neighbors.
- Each router has limited knowledge of the overall network topology.
- 

1.1.4 Routed Protocols:

- IPv4
- IPv6

1.1.4.1 Routing Protocol vs Routed Protocol:

- A **routing protocol**, like OSPF or BGP, defines how routers communicate with each other to distribute information that enables them to select routes between any two nodes on a computer network.
- A **routed protocol**, such as IPv4 or IPv6, is used to send user data (payload) through the established network path determined by the routing protocol.

1.1.5 Benefits of OSPF

- **Minimal Routing Traffic:** OSPF reduces control traffic overhead by sending updates only when there's a change in the topology, rather than at regular intervals.
    - OSPF uses multicast addresses 224.0.0.6 to communicate with DRs and BDRs, and 224.0.0.5 for all other OSPF routers (DROthers).

> - **Control traffic** is the signaling information exchanged between network devices to manage and maintain the network, such as routing protocols and handshakes.
> - **Data traffic** is the actual user or application information being transmitted over the network, such as emails, videos, or website content.

- **Rapid Convergence:** OSPF quickly recalculates routes when network changes occur, ensuring minimal disruption in data forwarding.

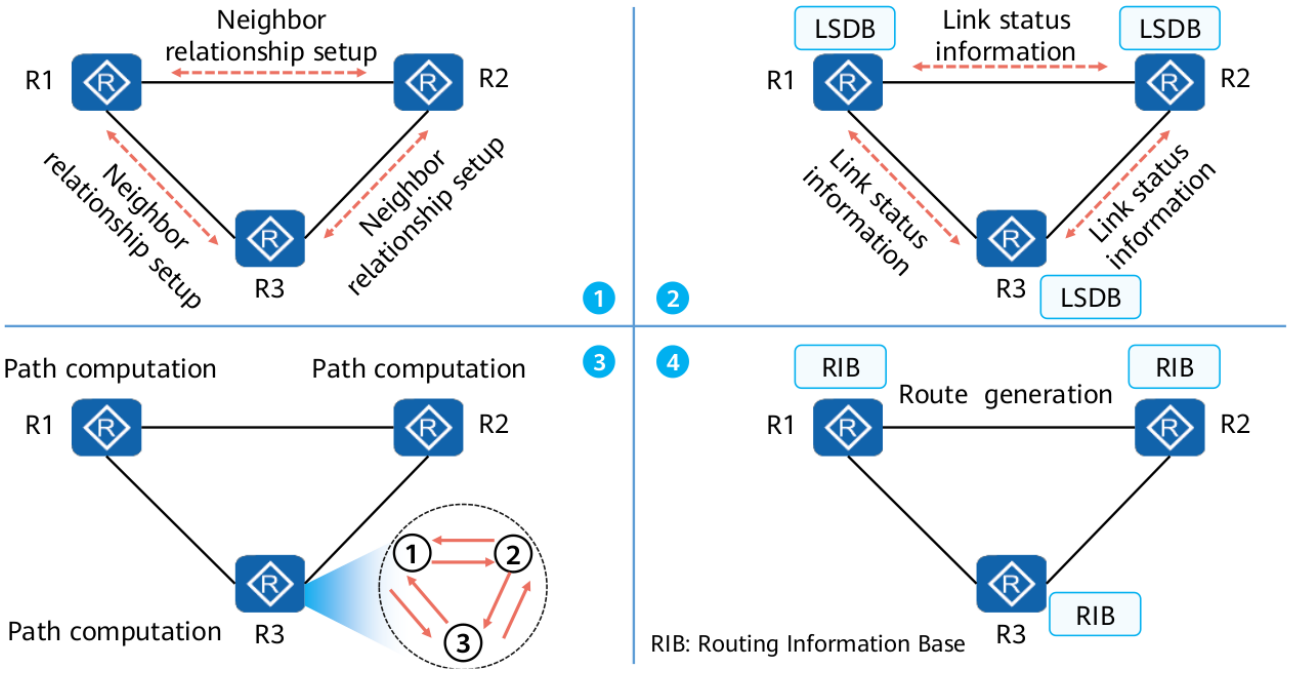
- **Scalable:** OSPF can support large networks with no limitations on hop count.
- **Accurate Route Metrics:** OSPF calculates the cost of routing paths based on various factors for efficient route selection.

1.1.6 How OSPF Works

---

1. **LSA Flooding**: Routers share link status with LSAs (Link State Advertisements).
    - **LSAs (Link State Advertisements):** LSAs are messages that OSPF routers share to inform each other about the status and connections of their network links. contains the interface cost and the relationship between the router and its neighboring routers.
2. **LSDB**: Routers store Link-State Advertisements (LSAs) in their Link State Database (LSDB) to represent the entire network topology.
3. **SPF Algorithm**: Calculates the shortest path to each network segment forming a loop-free tree.

> Based on SPF calculation results,each router installs routes into the routing table.



> **The Routing Information Base (RIB):** is a data table stored in a router or a network switch that lists routes to particular network destinations, and in some cases, metrics associated with those routes.

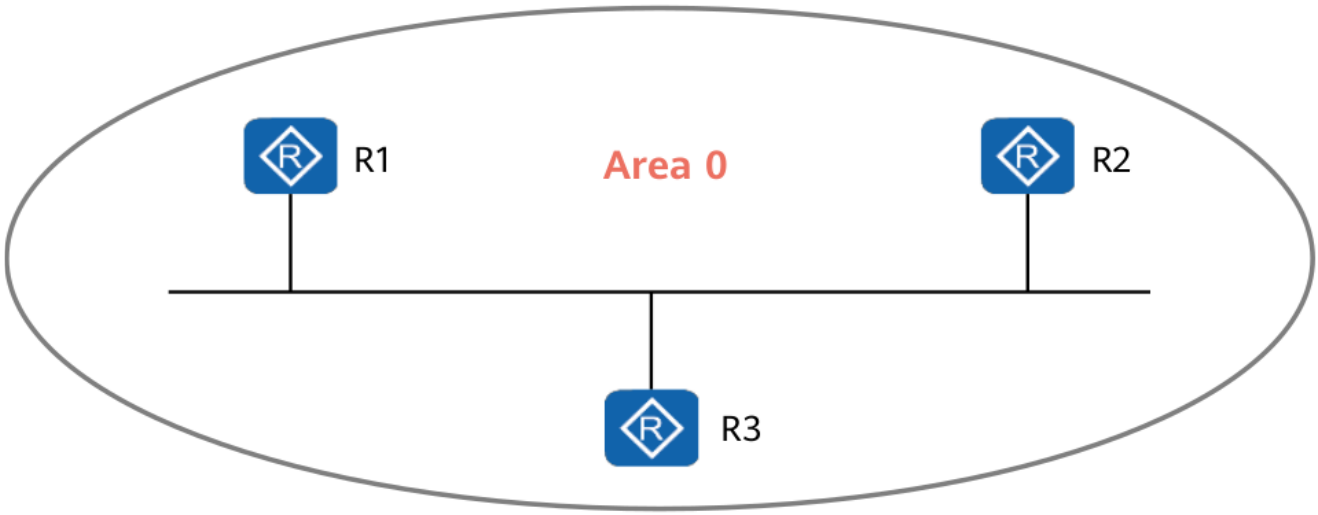
1.1.7 Introduction to OSPF

> **There are two versions:** OSPFv2 for older internet addresses (IPv4) and OSPFv3 for newer addresses (IPv6).

> Instead of sharing entire routes, OSPF routers share information about the status of connections between them.

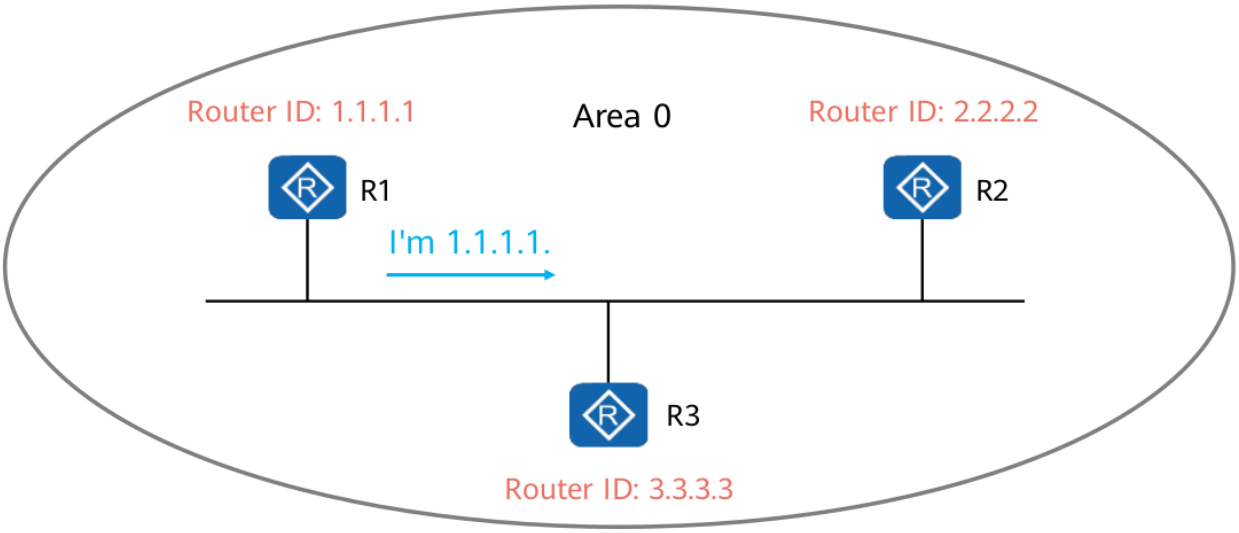
1.1.8 Key Terminology in OSPF

`Area` : Logical grouping identified by an Area ID.



`Router ID` : Unique identifier within an area;Represented same as ipv4 ex 1.1.1.1 ; The router ID can be manually specified or automatically assigned by the system.

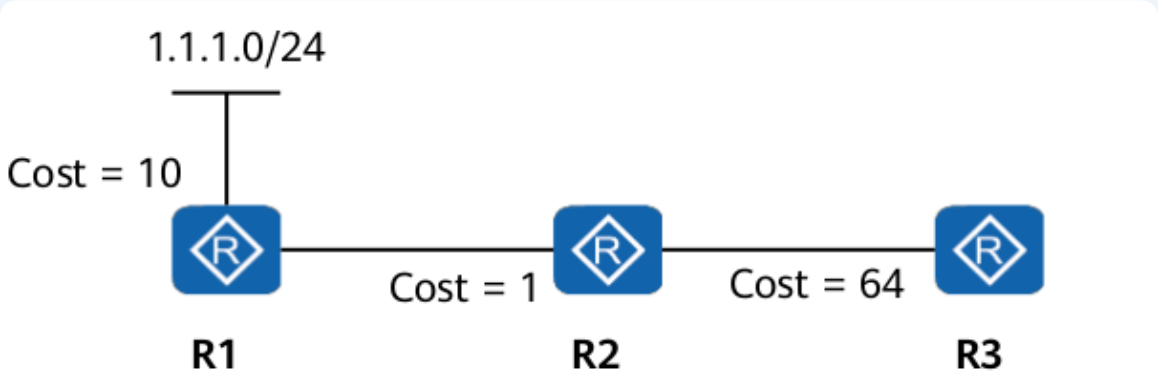
> The system assigns a `Router ID` based on the highest loopback address; if a loopback address is not present, then it selects the highest IPv4 address from the active interfaces.



`Cost Value` : Metric used to determine path selection; lower cost preferred.

Note

- Default cost value = 100 Mbit/s
- formula = $\text{Default cost value} / \text{costs of interfaces}$
- ex.Cost Value of an OSPF Interface
  - Serial interface costs of interfaces= $(1.544 Mbit/s)$
  - $100 / 1.544$=64 (approximately)
- ex.Accumulated Costs on an OSPF Path



- In the routing table of R3, the cost of the OSPF route to 1.1.1.0/24 is 75 (10 + 1 + 64).

1.1.9 Types of Packets in OSPF

Packet Name	Function
Hello	Is periodically sent to discover and maintain OSPF neighbor relationships.
Database Description	Describes the summary of the local LSDB, which is used to synchronize the LSDBs of two devices.
Link State Request	Requests a needed LSA from a neighbor. LSRs are sent only after DD packets have been successfully exchanged.
Link State Update	Is sent to advertise a requested LSA to a neighbor.
Link State ACK	Is used to acknowledge the receipt of an LSA.

> The Hello interval in OSPF is set to 10 seconds for point-to-point (P2P) or broadcast networks, and 30 seconds for non-broadcast networks, indicating how often Hello packets are sent to maintain adjacency.

1.1.10 Three Types of OSPF Entries

OSPF Neighbor Table Entry:

- This table tracks the OSPF neighbors a router has discovered by exchanging Hello packets, detailing their relationship status and key information like router IDs and interface addresses.
- `display ospf peer` Use the command to view this table, which helps routers determine whom they can share routing information with.

```
<R1> display ospf peer
    OSPF Process 1 with Router ID 1.1.1.1
                    Neighbors
Area 0.0.0.0 interface 10.1.1.1(GigabitEthernet1/0/0)'s neighbors
Router ID:  2.2.2.2    Address:  10.1.1.2    GR State: Normal
    State: Full  Mode:Nbr is  Master  Priority: 1
    DR:  10.1.1.1  BDR: 10.1.1.2   MTU: 0
    Dead timer due in 35  sec
    Retrans timer interval: 5
    Neighbor is up for 00:00:05
    Authentication Sequence: [ 0 ]
```

> The Router Dead Interval is typically four times the Hello interval, after which a non-responsive neighbor is considered down and its adjacency with the local router is terminated.

OSPF LSDB (Link State Database) Entry:

- The LSDB holds all the Link State Advertisements (LSAs) that a router has created or received, forming a complete map of the network topology.
- Use the `display ospf lsdb` command to access this database, which includes details such as LSA type(type) and the advertising router's identity(advRouter) which indicates the router that sends the LSA..

```
<R1> display ospf lsdb
                OSPF Process 1 with Router ID 1.1.1.1
                        Link State Database
                            Router ID: 0.0.0.0
Type      LinkState ID    AdvRouter    Age  Len   Sequence    Metric
Router     2.2.2.2        2.2.2.2       98  36    8000000B      1
Router     1.1.1.1        1.1.1.1       92  36    80000005      1
Network   10.1.1.2        2.2.2.2       98  32    80000004      0
```

OSPF Routing Table Entry:

- This table is distinct from the main router routing table and contains OSPF-specific paths with details like destination IP address, route cost, and next-hop IP address for packet forwarding decisions.

- To view this information, use the `display ospf routing` command. It shows how OSPF has calculated routes to different networks based on the LSDB.

```
<R1> display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing tables
Routing for Network
Destination        Cost  Type      NextHop        AdvRouter       Area
1.1.1.1/32          0     stub      1.1.1.1        1.1.1.1         0.0.0.0
10.1.1.0/20         1    Transit    10.1.1.1       1.1.1.1         0.0.0.0
2.2.2.2/32          1     stub      10.1.1.2       2.2.2.2         0.0.0.0

Total Nets: 3
Intra Area: 3  Inter Area: 0  ASE: 0  NSSA: 0
```

1.2 OSPF Working Mechanism

1.2.1 Neighbor Relationship and Adjacency

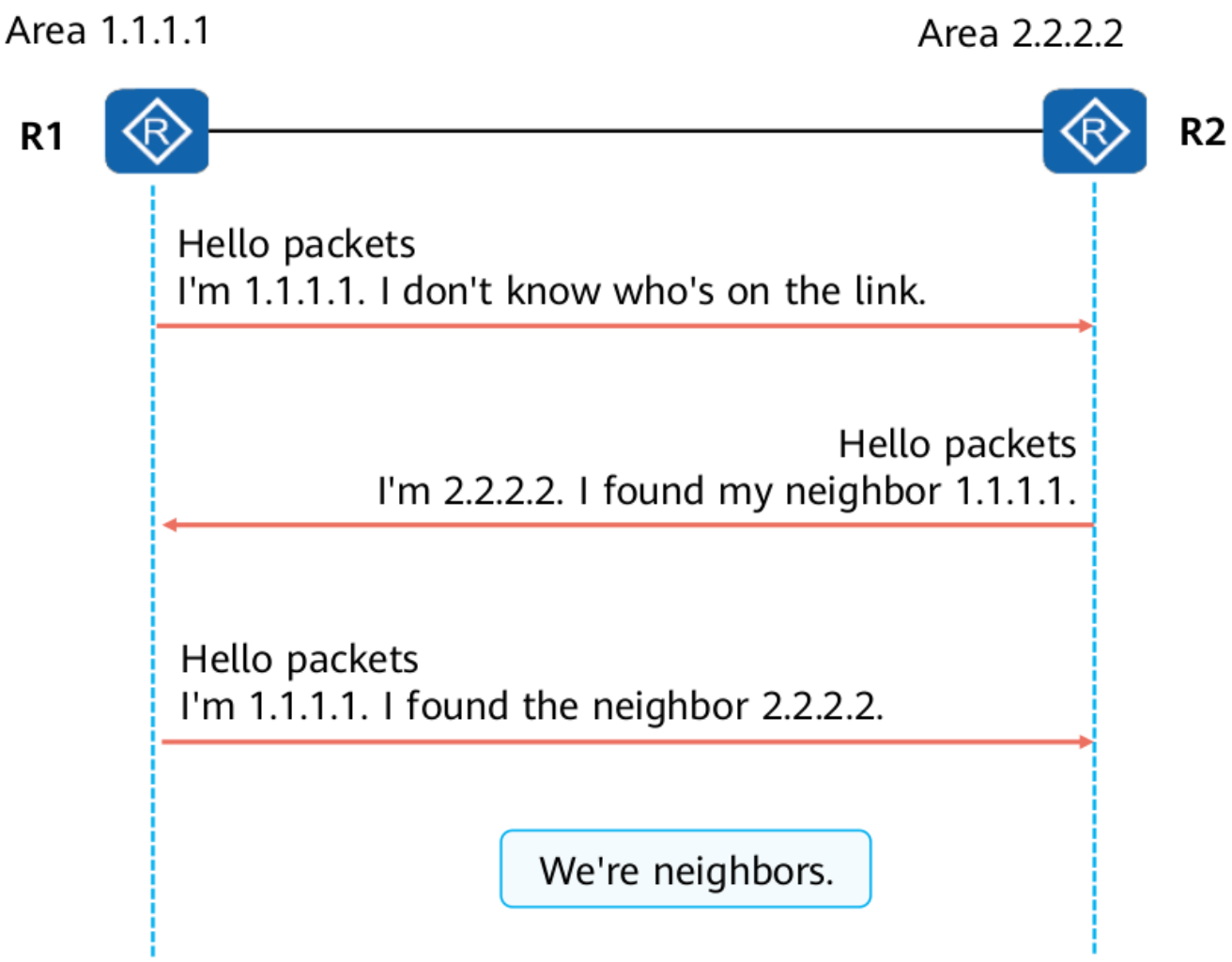
- **Neighbor Relationship**: Two routers running OSPF become aware of each other by exchanging Hello packets.
- **Adjacency**: After LSDB sync, routers calculate routes independently.

1.2.2 Establishing OSPF Adjacency - Steps Overview

1.2.2.1 Step 1: Neighbor Discovery

- Bidirectional communication is established using Hello packets.
- The `Init` phase moves to the `2-way` phase once both sides find each other.

- **Init:** phase is when one device starts communication.
- **2-way:** phase is when both devices acknowledge each other and start a two-sided conversation.



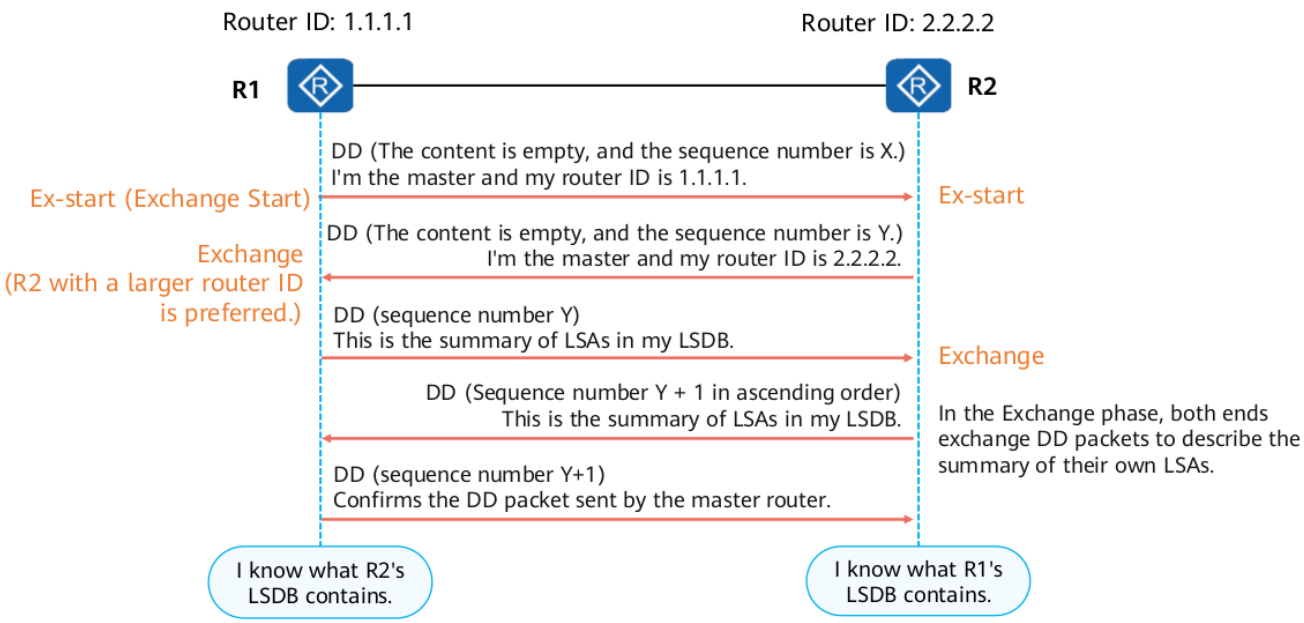
1.2.2.2 Step 2: Master/Slave Negotiation

- Exchange starts (`Exstart`) with empty DD (Database Description) packets.
  - **Exstart state:** is the initial phase where routers establish adjacency by exchanging empty Database Description packets to prepare for synchronization of their link-state databases.
- Router with the higher Router ID becomes the master during negotiation.

> A router with a priority of 0 will not participate in the DR/BDR election process in OSPF, effectively opting out of the role.

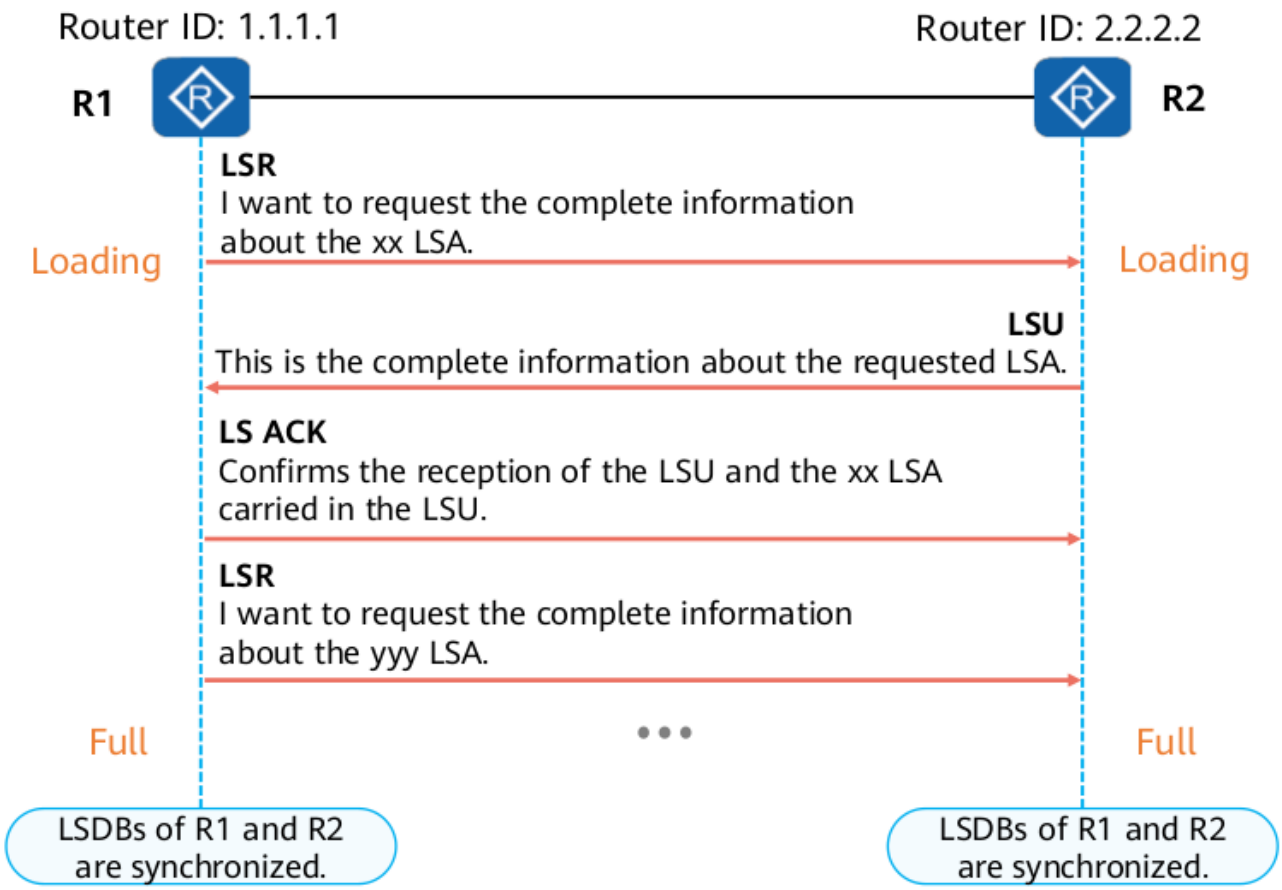
1.2.2.3 Step 3: LSDB Information Exchange

- Exchange of DD packets containing summaries of LSAs (Link-State Advertisements).
- The neighbor status changes from `Exstart` to `Exchange`.
  - **Exchange state:** is when neighboring routers send each other their respective link-state advertisements (LSAs) to construct a complete and accurate map of the network topology.
- After sending the last DD packet, R1 changes the neighbor status to `Loading`.
  - **Loading state:** indicates that a router is receiving and processing database description packets (DD) from a neighbor to synchronize its link-state database with that of the neighbor's.



1.2.2.4 Step 4: LSDB Synchronization

- LSR (Link-State Request), LSU (Link-State Update), and LSAck exchanged for detailed LSA information.



> The Link State Database (LSDB) must be consistent across all routers within the same OSPF area to ensure accurate network topology representation and routing.

1.2.2.5 Step 5: Route Calculation

- Performed independently on each router after synchronization.

1.2.3 OSPF Neighbor Table

Field	Explanation	
OSPF Process	Identifier for the local OSPF process and router ID.	
Area ID	Unique identifier for the area to which the neighbor belongs.	
Address	IP address of the neighbor's interface.	
GR State	Graceful Restart status, showing if it is normal or in a GR state.	
State	Current state of the OSPF neighbor relationship.ex(Init, 2-Way, ExStart, Exchange, Loading, or Full)	
Mode	Indicates if the local device is master or backup during exchanges.	
Priority	Neighbor's priority for Designated Router (DR) election.	
DR	IP address of the Designated Router on the link.	
BDR	IP address of the Backup Designated Router on the link.	
MTU	Maximum Transmission Unit size on the neighbor's interface.	
Retrans timer interval	Time interval for retransmitting Link State Advertisements (LSAs).	
Authentication Sequence	Number used to identify authentication sequence with neighbor.	

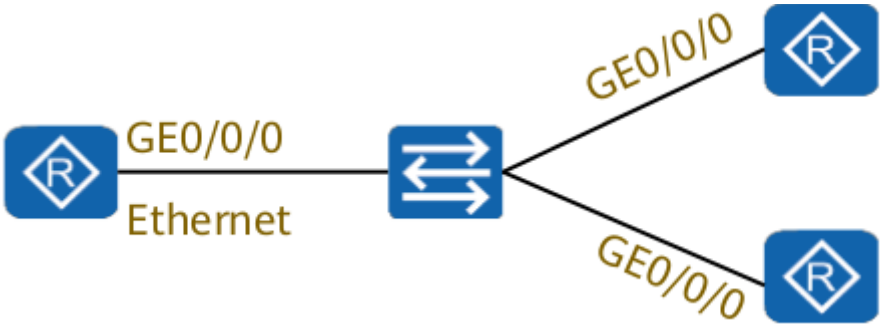
Field	Explanation	
	adcast Network Type `(NBMA)`	

1.2.4 OSPF Network Types

> To establish a neighbor relationship, the OSPF interface network types on both sides of a link must match.

1.2.4.1 Broadcast Network Type `(BMA)`

- Typical on Ethernet networks. Supports broadcast.



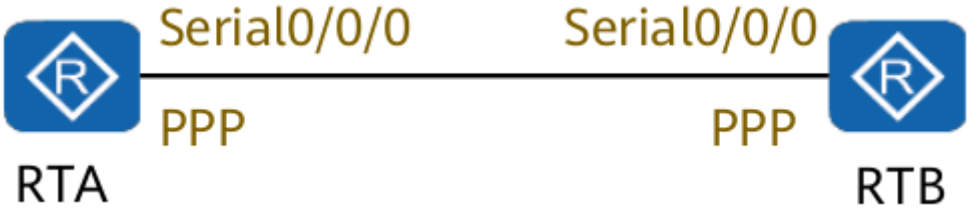
1.2.4.2 Non-Broadcast Network Type `(NBMA)`

- environment that allows multiple network devices to access but does not support broadcast.

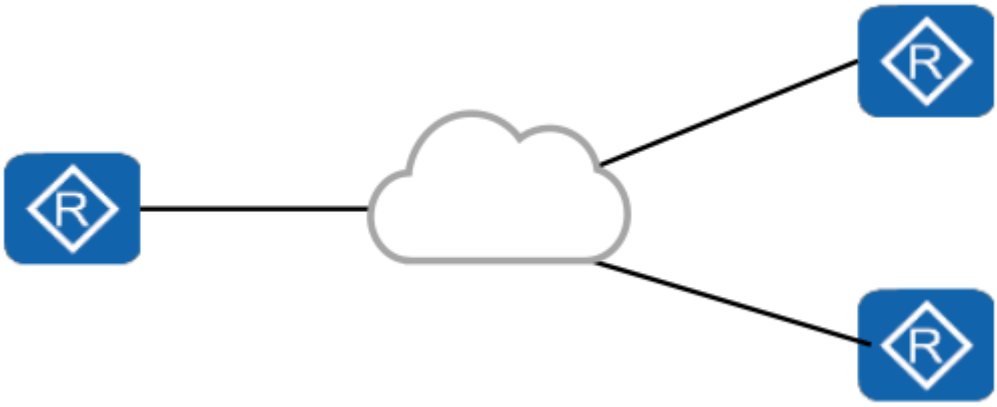
> an NBMA network connects multiple devices so they can communicate but restricts them from sending data to all devices at once through broadcasting. Instead, communication must be directed specifically from one device to another using pre-established paths or addressing methods.

- **Example:** Frame Relay networks. Does not support broadcast.

1.2.4.3 Point-to-point `(P2P)`

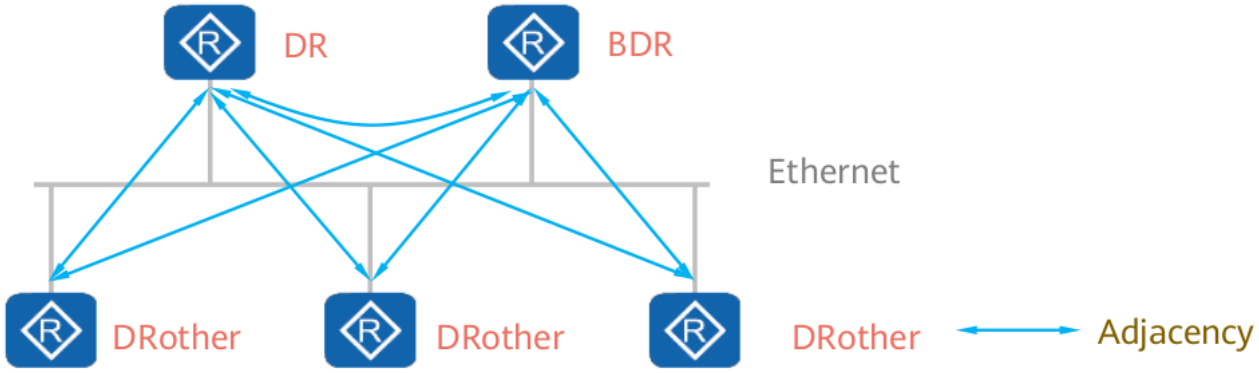
- A link that connects exactly two routers. Common with PPP.
- Default network type of the OSPF interface is P2P.
- 

1.2.4.4 Point-to-Multipoint `(P2MP)`

- single source transmits data to multiple destinations or users.
- Bundles multiple P2P links. Not a default type; set manually when needed.
- 

1.2.5 DR and BDR Concept

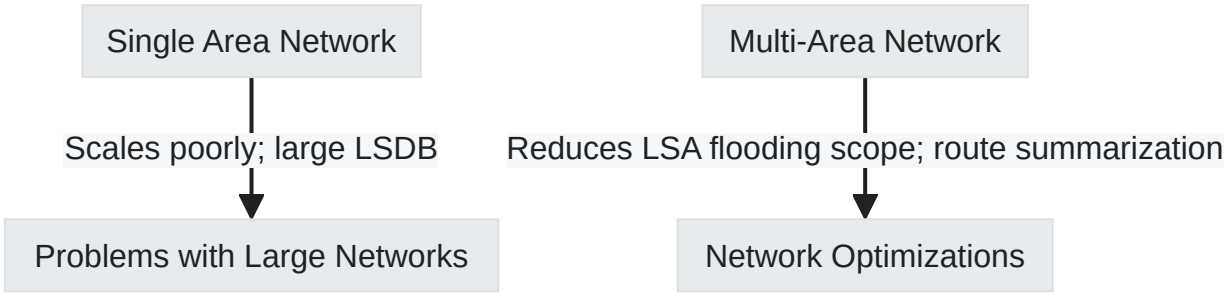
> Designated Router (DR) and Backup Designated Router (BDR) reduce the number of adjacencies needed on MA networks like Ethernet.



> The interface with the highest priority becomes the Designated Router (DR); if priorities equal, the highest router ID wins, and once elected, DR does not change unless there's a restart or topology change.

1.2.6 OSPF Area Concepts

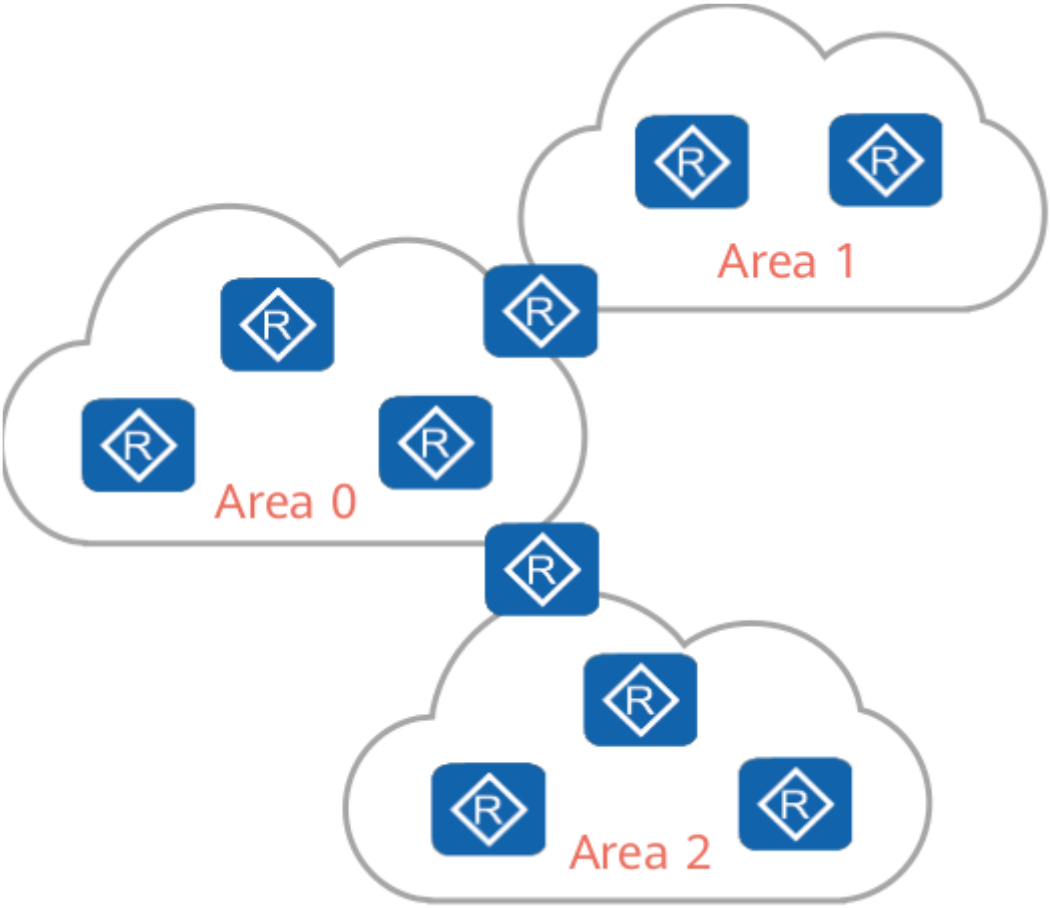
1.2.6.1 Single Area vs Multi-Area Networking



> Routers within the same area share and keep their map of the network's layout Uniform

> Domain is a group of connected devices using the same rules to exchange routing information.

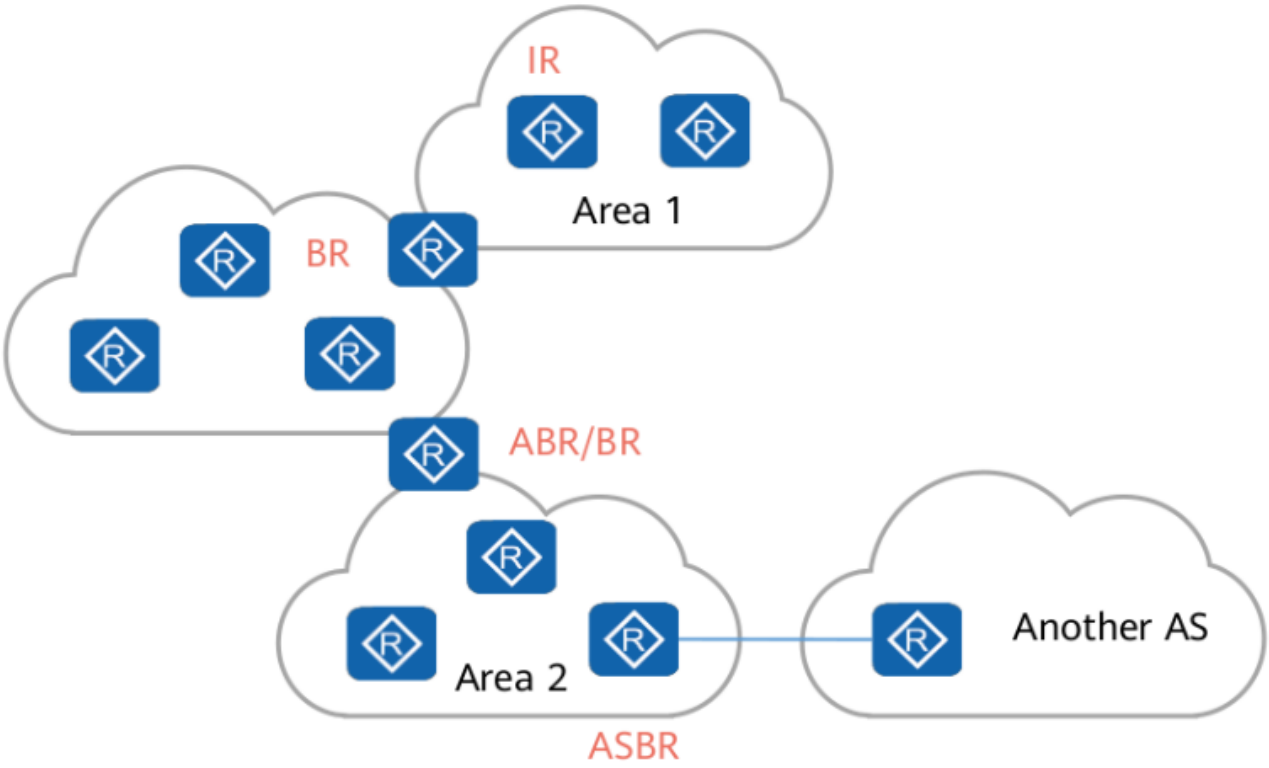
1.2.6.2 Types of Areas in OSPF



Area Type	Description	Notes
Backbone Area (Area 0)	Core area through which all other areas communicate	Mandatory for multi-area networks
Non-backbone Area	Any area that isn't the backbone	Must connect to backbone area

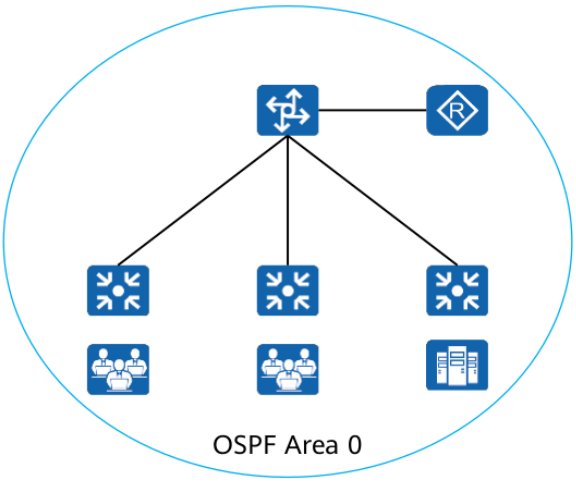
> The backbone area (Area 0) acts as a central hub that connects all other areas to prevent routing loops. Non-backbone areas only know how to reach the backbone and trust it to route to other areas. Direct connections between non-backbone areas are avoided to prevent routing inconsistencies and looping paths.

1.2.6.3 Types of OSPF Routers Based on Function

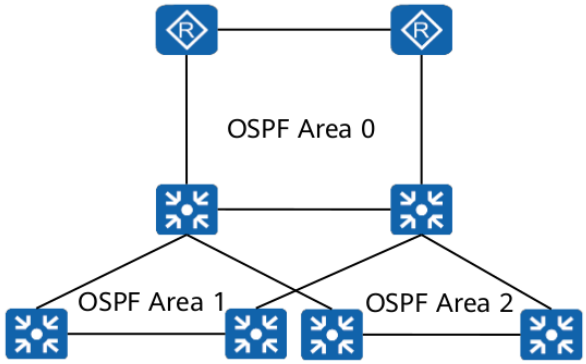


Router Type	Description
Internal Router (IR)	All interfaces within one area
Area Border Router (ABR)	Connects multiple areas; has an interface in Area 0
Backbone Router (BR)	At least one interface in the backbone area
Autonomous System Boundary Router (ASBR)	Exchanges routes with external AS; imports external routes

1.2.6.4 Typical Networking Scenarios



Small- and medium-sized enterprise network (single area)



Large enterprise network (multiple areas)

- For small-scale enterprises:

> Use a single-area network due to limited scale and simplicity.

- For large-scale enterprises:

> Adopt a multi-area approach to enhance scalability and performance.

1.2.7 OSPF authentication

> OSPF supports multiple levels of authentication; when configured on an interface, routers must share the same password to establish a neighbor relationship.

> An OSPF silent interface is configured to prevent forming neighbor relationships over that interface, useful for security or topology reasons.

1.3 Typical OSPF Configuration

1.3.1 Creating and Running an OSPF Process

- Syntax: `ospf [<process-id> | router-id <router-id>]`
  - Default process ID is `1`.

> The process-id is a unique identifier for a single instance of the OSPF routing protocol running on a router, allowing for multiple separate OSPF processes on the same device, its benefit to separating and managing different networks or traffic classes.

- Multiple processes can run on the same device.
- The `router-id` specifies the ID of a device.

Note

Always ensure that each OSPF router has a unique `router-id`.

Example

```
[Huawei] ospf 1 router-id 1.1.1.1
```

1.3.2 Configuring OSPF Area

1.3.2.1 Creating OSPF Area and Entering View

- **Syntax:** `area <area-id>`
  - Area IDs can be decimal or dotted decimal notation.

Example

```
[Huawei-ospf-1] area 0
```

1.3.3 Interface Configuration for OSPF

1.3.3.1 Specifying Interface for OSPF

- **Syntax:** `network <network-address> <wildcard-mask>`
- Used for interfaces on a router will participate in OSPF.
- `<network-address>` : is the IP address that represents the network you want to include in OSPF.
- `<wildcard-mask>` : Reverse of Mask

Example

```
[Huawei-ospf-1-area-0.0.0.0] network 10.1.12.0 0.0.0.3
```

1.3.4 Setting Interface Cost and Priority

1.3.4.1 Setting an Interface Cost

Markdown

```
[Huawei-GE1/0/1] ospf cost <cost-value>
```

- Cost for an OSPF interface.
- By default, OSPF automatically calculates the cost of an interface based on the interface bandwidth.

- The cost value is an integer ranging from 1 to 65535.

1.3.4.2 Setting Bandwidth Reference Value for Cost Calculation

---

Markdown

```
[Huawei-ospf-1] bandwidth-reference <value>
```

- Bandwidth reference value that is used to calculate interface costs.
- The value ranges from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

1.3.4.3 Setting DR Priority of an Interface

Markdown

```
[Huawei-GigabitEthernet0/0/0] ospf dr-priority <priority-value>
```

- Priority for an interface that participates in DR election.
- The value ranges from 0 to 255.

1.3.5 Verification Commands

Tip

After configuring OSPF, always verify that neighbors are established and routes are learned properly.

1.3.5.1 Check Neighbor Table

Markdown

```
<R2> display ospf peer brief
```

```
<R2> display ospf peer brief
         OSPF Process 1 with Router ID 2.2.2.2
                  Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                     Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/0            1.1.1.1        Full
 0.0.0.1          GigabitEthernet0/0/1            3.3.3.3        Full
 ----------------------------------------------------------------------------
```

1.3.5.2 Check Routing Table

Markdown

```
<R1> display ip routing-table
```

```
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing tables: Public
         Destinations : 10       Routes : 10
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        3.3.3.3/32  OSPF    10   2           D   10.1.12.2       GigabitEthernet 0/0/0
       10.1.12.0/30 Direct  0    0           D   10.1.12.1       GigabitEthernet 0/0/0
...
<R1>ping -a 1.1.1.1 3.3.3.3
  PING 3.3.3.3: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes = 56 Sequence = 1 ttl = 254 time = 50 ms
...
```

Ethernet Switching Basics

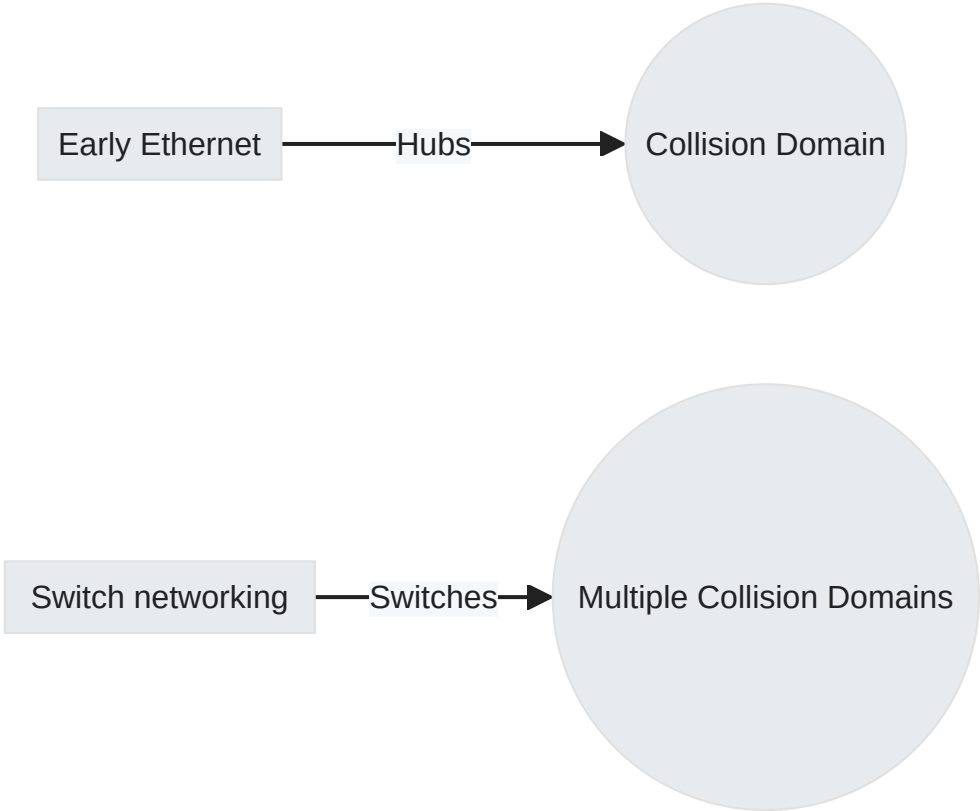
1 Ethernet Switching Basics

1.1 Overview of Ethernet Protocols

Ethernet is the foundational standard for most Local Area Networks (LANs). It specifies the types of cables and signal processing methods used in a LAN environment.

- Ethernet networks are built on the CSMA/CD mechanism.
- Switches have largely replaced hubs in modern networks due to their ability to improve performance by isolating collision domains.

> A collision domain is a segment of a network where packet collisions can occur, typically confined to a single broadcast domain when using a hub.



1.1.1 CSMA/CD Mechanism

- Devices listen for network silence before transmitting.
- If two devices transmit simultaneously, a collision occurs.
- Devices stop sending data and send jam signals upon detecting collisions.
- After waiting for a random delay period, devices attempt to resend data.

1.1.2 Broadcast Domains

> A broadcast domain is the area where a broadcast message can reach all devices in a network at Layer 2 of the OSI model.

- All hosts within the same broadcast domain receive any broadcasted packets.

- Switches send broadcast messages to all devices connected to them, making those devices part of a single communication group.

1.1.3 Ethernet NIC (Network Interface Card)

> **NIC Definition**: Essential hardware component enabling network device connection to an external network. Each port on a networking device corresponds to one NIC. Commonly referred to as network interface or port.

> **Physical ports:** actual interface on your computer where you can connect a cable—like an Ethernet port connected to its respective NIC.

> **Software/network port:** This is a virtual construct used by your computer's operating system to organize and manage network traffic. For example, when you access a website using your web browser, it typically uses port 80 (for HTTP) or port 443 (for HTTPS).

> **Ethernet NICs**: In the context of this document, all NICs referenced are Ethernet compatible. The switches discussed use Ethernet NICs at each port.

> **Data Handling**: Computers or switches send and receive data frames through NICs which process these frames into bitstreams suitable for transmission across physical media.

1.2 Overview of Ethernet Frames

1.2.1 Ethernet Frame Format

- Ethernet frames are the data units used in Ethernet networks.
- Two primary formats: **Ethernet II** and **IEEE 802.3**.
- Frame length: `64–1518 bytes`, where the MTU (Maximum Transmission Unit) is `1500 bytes`.

1.2.1.1 Ethernet II vs IEEE 802.3

Ethernet II Frame Structure	Size (bytes)	Description
Destination MAC (DMAC)	6	Destination Media Access Control address
Source MAC (SMAC)	6	Source Media Access Control address
Type / Ethertype	2	field in an Ethernet frame specifies the protocol of the data contained in the frame's payload (like IPv4, IPv6, ARP, etc.).
User Data	46-1500	Payload containing the encapsulated data from a higher layer protocol
Frame Check Sequence (FCS)	4	Error-checking field used to detect corruption

> - Type
> - **0x0800:** Internet Protocol Version 4 (IPv4)
> - **0x0806:** Address Resolution Protocol (ARP)

IEEE 802.3 Frame Structure	Size (bytes)	Description
Destination MAC (DMAC)	6	Destination Media Access Control address
Source MAC (SMAC)	6	Source Media Access Control address

IEEE 802.3 Frame Structure	Size (bytes)	Description
Length field	2	Specifies the length of the payload data
Logical Link Control (LLC)	Variable	Provides additional control information for managing data communication links.
Destination Service Access Point (DSAP)	1 byte	Identifies which application or service on the destination device should handle data.
Source Service Access Point (SSAP)	1 byte	Identifies the application or service on the source device that generated data.
Control	1 byte	Ensures proper sequencing and error checking for frames being transmitted.
SNAP	-	- Extends LLC to allow use of EtherType values for protocol identification.
- Org Code	3 bytes	Specifies an organization that defines the format of following fields in SNAP.
- Type	2 bytes	Indicates which protocol is encapsulated within this Ethernet frame (like IP, ARP).
User data	38-1492B	Contains actual information being transmitted (application data, etc.).
FCS	4 bytes	Error-checking field that helps ensure data integrity during transmission.

1.2.2 MAC Address

- **A media access control (MAC):** address uniquely identifies a NIC on a network. Each NIC must have a globally unique MAC address, defined and standardized in IEEE 802.
  - **Length**: `48 bits` or `6 bytes`.
  - **Format**: Six groups of two hexadecimal digits (`00-AA-BB-CC-DD-EE`).

Criteria	IP Addresses	MAC Addresses
Uniqueness	Unique within a network segment	Globally unique
Changeability	Can be changed	Cannot be changed
Assignment Basis	Based on network topology	Based on the manufacturer
Network Relevance	Used for route selection and networking	Used primarily for local network traffic
Flexibility & Maintenance	Devices can be reassigned IP addresses; helpful for reconfiguration and mobility	MAC addresses are static, but devices can be replaced without affecting IP addressing

1.2.3 OUI and CID

> **Organizationally unique identifier (OUI):** First 3 bytes assigned by IEEE to manufacturers(globally unique).
> **Company ID (CID):** Last 3 bytes assigned by manufacturers to individual devices.

1.2.4 Frame Types

1.2.4.1 Unicast Frame

- Destination MAC = Unicast MAC address
- Sent from one source to one destination only.

> **Format:** XX-XX-XX-XX-XX-X0 | Individual device identification.

1.2.4.2 Broadcast Frame

- Destination MAC = FF:FF:FF:FF:FF:FF
- Sent from one source to all hosts on LAN.

> **Format:** FF-FF-FF-FF-FF-FF | All devices on the LAN.

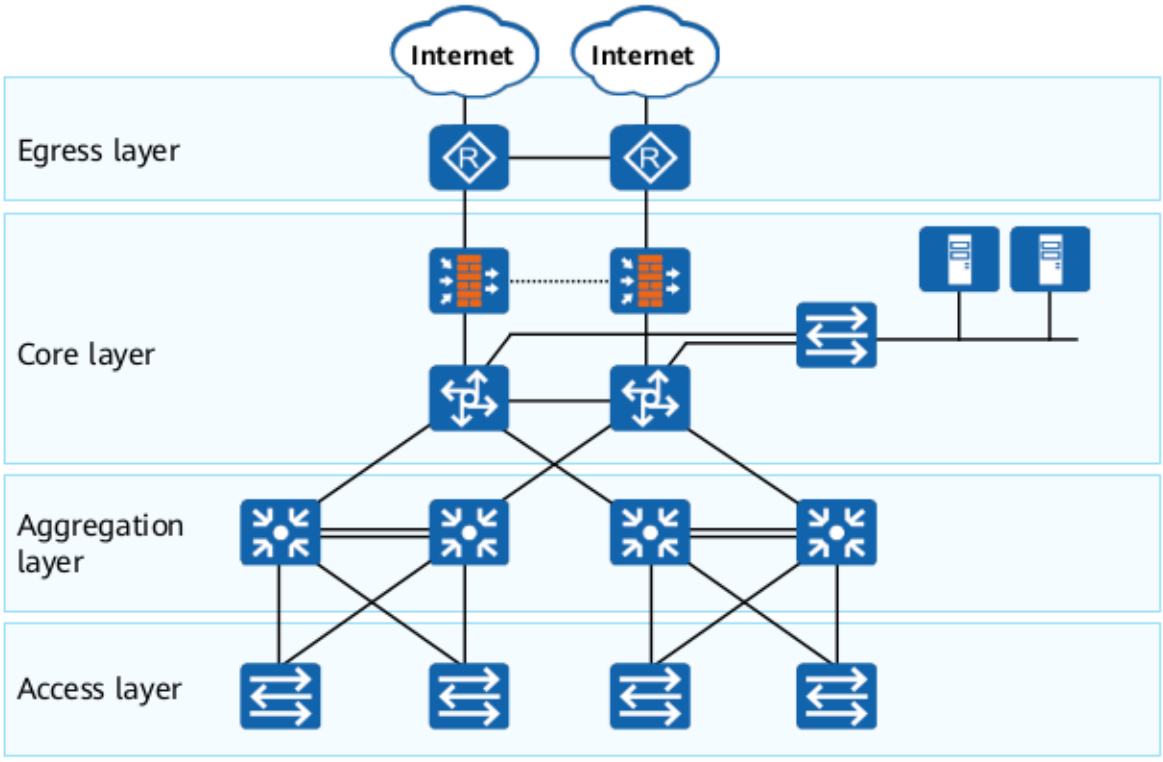
1.2.4.3 Multicast Frame

- Destination MAC = Starts with '01' e.g., 01:80:C2...
- Sent from one source to multiple hosts subscribed to multicast group.

> **Format:** XX-XX-XX-XX-XX-X1 | Group of devices on the LAN.

1.3 Overview of Ethernet Switches

- A campus network typically includes an **access layer**, **aggregation layer**, **core layer**, and **egress layer**.
- Devices involved include routers, switches (Layer 2 & Layer 3), and firewalls.



1.3.1 Switches

1.3.1.1 Layer 2 Ethernet Switch

- Operates at the Data Link Layer (Layer 2 of the TCP/IP model).
- Forwards packets based on MAC addresses.

1.3.1.2 Layer 3 Ethernet Switch

- Capable of high-speed Layer 3 forwarding.
- Used when routers are insufficient due to high costs or low performance.

1.3.2 Frame Processing Behaviors

- **Flooding**: If the destination MAC address is unknown or a broadcast address, the frame is sent to all ports except the originating port.
- **Forwarding**: The switch sends the frame to a specific port based on the MAC address table.
- **Discarding**: Frames coming from the same place they arrived are discarded to prevent loops.

1.3.3 MAC Address Table Learning Process

> **Note**
>
> Switches dynamically learn MAC addresses and associate them with interfaces. Entries have an aging time (e.g., Huawei default is 300s).

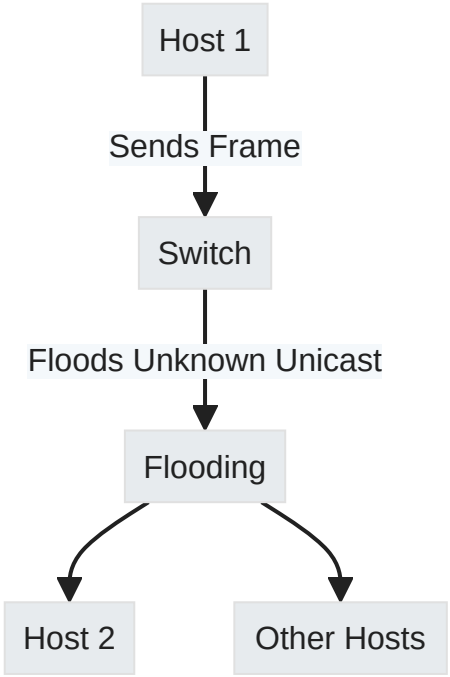
MAC Address	Interface
MAC1	GE0/0/1
MAC2	FE0/1

1.3.3.1 Initial State

Host 1 —Sends Frame→ Switch —Table Empty→ MAC Address Learning

> `Host1` sends a frame with its own source IP/MAC to `Host2` .

1.3.3.2 Frame Reception & Flooding

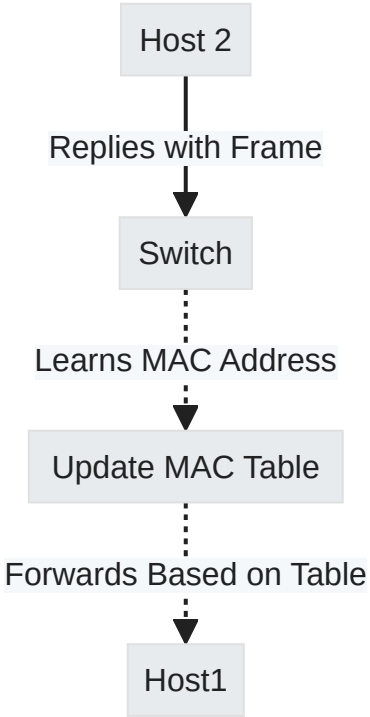


MAC Address	Interface
MAC1	GE0/0/1

> The switch learns `Host1` 's MAC and updates its table linking it to interface GE 0/0/1.

> If no entry for `Host2` 's MAC exists, the switch floods the frame.

1.3.3.3 Update Table & Forwarding



> `Host2` receives and processes the frame since it matches its own MAC address.

> When `Host2` replies, the switch finds an entry in its table and forwards accordingly while learning `Host2` 's interface (GE 0/0/2).

MAC Address	Interface
MAC1	GE0/0/1
MAC2	GE0/0/2

1.4 Process of Data communication Within a Network Segment

1.4.1 Overview

- **Objective**: Host 1 wants to access Host 2 within a network.
- **Hosts**:

    - Both hosts know their own IP and MAC addresses.
    - Assumption: Host 1 has obtained the IP address of Host 2.

- **Switch**: The switch is initially in a powered-on state with an empty MAC address table.

1.4.2 Initialization Process

> **Note**
>
> Initially, both the ARP cache table on Host 1 and the MAC address table on the switch are empty.

1.4.3 ARP Request and Flooding Frames

- Host 1 sends an **ARP Request** to find MAC2 (Host 2's MAC address).
- The switch floods the frame to all ports except the one it received from because its MAC address table is empty.

1.4.4 MAC Address Learning

- The switch learns MAC1 (Host 1's MAC) when it receives the ARP Request and updates its MAC address table:

MAC Address	Port	Type
`0050-5600-0001`	GE0/0/1	dynamic

> **Tip**
>
> Switches learn source MAC addresses from incoming frames and store them in their tables along with associated ports.

1.4.5 Reply of the Target Host (ARP Reply)

- Host 2 processes the ARP Request and sends an **ARP Reply** back to Host 1 containing its own MAC and IP addresses.
- The switch forwards this reply directly to Host 1 since it now knows where to send packets destined for `0050-5600-0001`.

1.4.5.1 Updated Switch Table after ARP Reply

MAC Address	Port	Type
`0050-5600-0001`	GE0/0/1	dynamic
`0050-5600-0002`	GE0/0/2	dynamic

> **Host 1** updates its ARP cache with the IP-MAC mapping for Host 2.

VLAN Principles and Configuration

1 VLAN Principles and Configuration

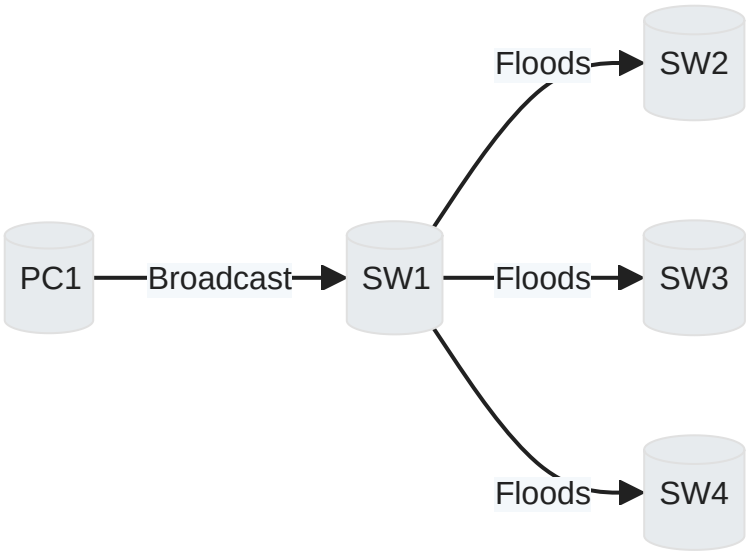
1.1 What Is VLAN

1.1.1 Broadcast Domains

> In a typical switching network, all devices receive broadcasts sent by any single device.

1.1.1.1 Issues with Large Broadcast Domains

- Increased **junk traffic** (unnecessary data packets that consume bandwidth).
- Higher potential for **network security** breaches.
- Reduced network efficiency due to too much broadcasts.



1.1.2 VLANs (Virtual Local Area Networks)

1.1.2.1 Purpose of VLANs

- To segment large broadcast domains into smaller ones.
- To improve **security**, reduce **junk traffic**, and Save network resources.

1.1.2.2 Characteristics of VLANs

- Each VLAN creates its own broadcast domain.
- Devices in the same VLAN can communicate at Layer 2; different VLANs require Layer 3 communication.
- VLAN assignments are geographically independent, allowing flexible network design.

1.1.2.3 Advantages of Using VLAN Technology

Advantage	Description
Flexible groups	Allows terminals in different locations to be part of the same network.
Bandwidth conservation	Limits broadcast traffic to within a single VLAN.
Enhanced security	Segregates traffic so that devices across VLANs cannot directly communicate at Layer 2.
Network robustness	Isolates faults within a single VLAN, preventing them from affecting other segments.

1.2 VLAN Principles

1.2.1 VLAN Identification

- **How VLANs are identified:** Through a 4-byte IEEE 802.1Q tag inserted into Ethernet frames.

> IEEE 802.1Q, often referred to as Dot1q, defines a system of VLAN tagging for Ethernet frames by inserting an 802.1Q tag into the frame header to carry VLAN information.

- **VLAN Tag Components:**

Field	Description	Values
TPID	Identifies frame type	0x8100 for IEEE 802.1Q
PRI	Priority of frame (QoS)	0-7
CFI	Canonical format indicator	0 for Ethernet frames
VLAN ID	Identifies the VLAN	1 to 4094

> **Canonical format :** used for transmitting a MAC address in an Ethernet

> frame sends the least significant bit (rightmost bit) of each byte first.

> PCs cannot identify tagged frames and therefore can send or process only untagged frames. By contrast, all frames processed by switches are tagged ones

1.2.2 VLAN Assignment Methods

- **Interface-based:** Assigns based on switch interfaces.
- **MAC address-based:** Assigns based on source MAC addresses.
- **IP subnet-based:** Assigns based on source IP addresses/subnets.
- **Protocol-based:** Assigns based on frame protocol types.
- **Policy-based:** Uses a combination of methods.

1.2.2.1 Interface-Based VLAN Assignment

> - PVID (Port Default VLAN ID) is configured per switch interface.
> - Untagged frames received are assigned to the corresponding PVID.

Info

Default PVID is usually set to `1`. It must be reconfigured if PCs move to different ports.

1.2.2.2 MAC Address-Based VLAN Assignment

> A mapping table is maintained to assign VLANs based on source MAC addresses. This method allows port flexibility without needing reconfiguration.

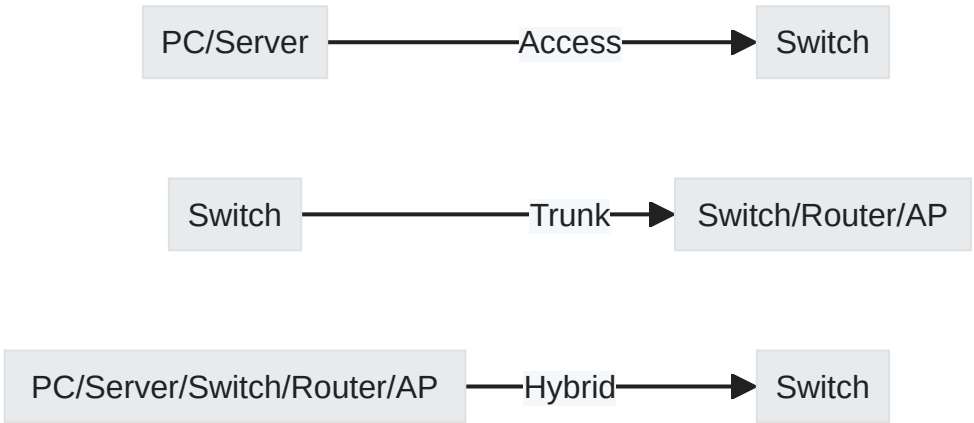
> ⚠ **Warning**
>
> Possible security risks due to potential MAC address spoofing.

1.2.3 Layer 2 Ethernet Interface Types

1.2.3.1 Overview

- Ethernet interfaces on switches can be categorized into three main types:
  - Access
  - Trunk
  - Hybrid

> Each type is designed to handle VLAN tagging and forwarding in different scenarios.



1.2.3.2 Access Interface

- Connects endpoints like PCs or servers to a switch.
- Carries untagged frames.
- Belongs to one VLAN only.

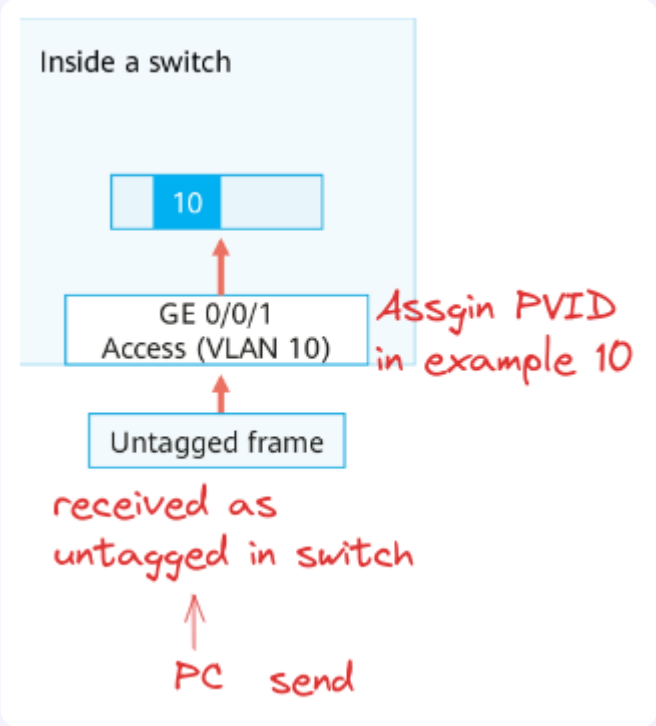
> Access interfaces are suitable for devices that do not recognize VLAN tags.

1.2.3.2.1 Frame Processing (Access)

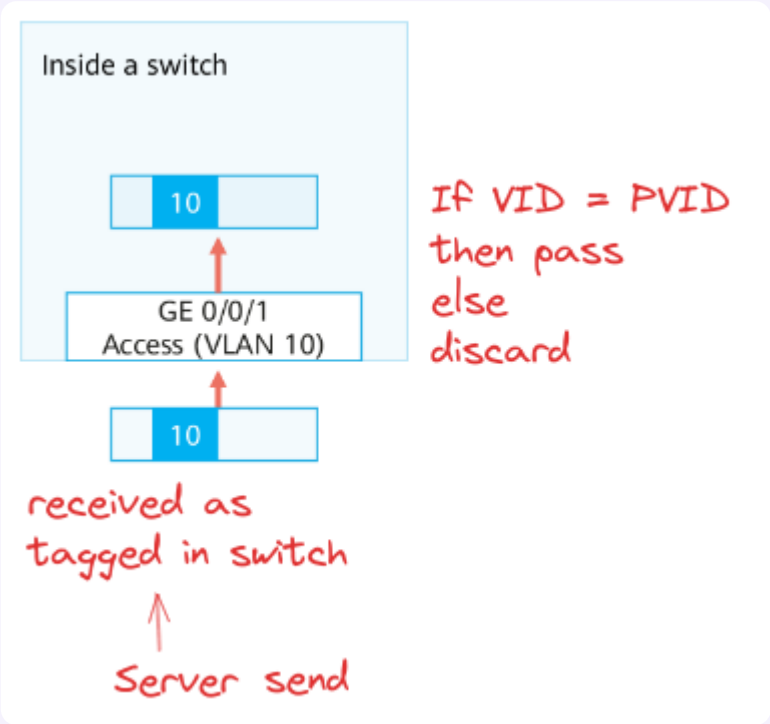
Action	Description
Receive (Untagged In)	If the incoming frame has no VLAN tag, the switch will assign it a default VLAN ID known as the Port VLAN ID (PVID).
Receive (Tagged In)	If the incoming frame has a VLAN tag, the switch will check if the tag's VLAN ID (VID) matches the PVID of that port. If they match, the frame is allowed; if not, it is discarded.
Send (Untagged Out)	When sending a frame out of an untagged port, it simply forwards the frame without any VLAN tag.
Send (Tagged Out)	When sending a frame out of a tagged port, if its VID matches the PVID of that port, the switch removes the tag before sending it out. If they don't match, then it discards the frame.

Example

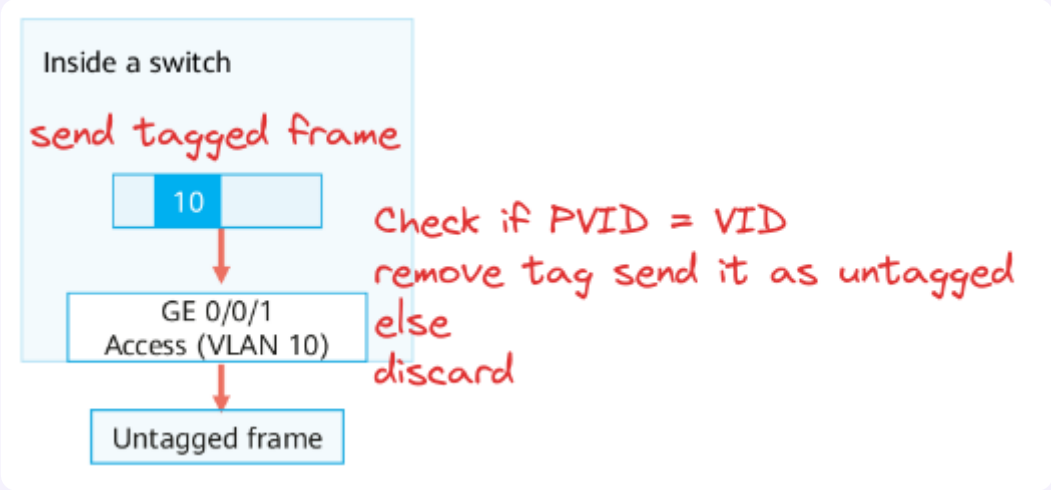
- **Receive (Untagged In):** A computer without VLAN configuration sends data to the switch, which assigns it to the default VLAN (PVID).



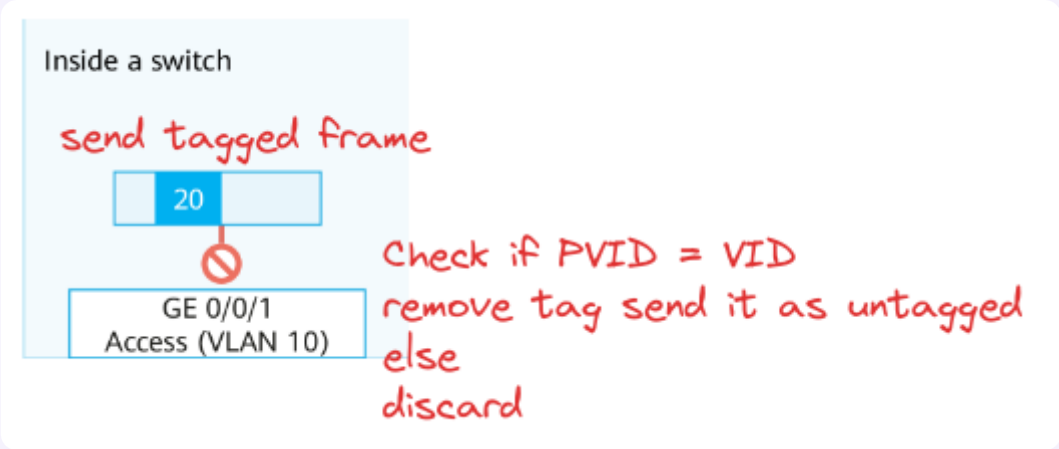
- **Receive (Tagged In):** A server sends data with a VLAN tag, and the switch checks if the tag matches the port's settings before accepting it.



- **Send (Untagged Out):** The switch sends data to a device like a printer that doesn't understand VLAN tags, so it removes any tag.(if the VID match the PVID)



- **Send (Tagged Out):** The switch forwards data with a VLAN tag to another switch, but removes the tag if that port is set to send untagged traffic only.



> **PVID** stands for Port VLAN ID: The default VLAN ID assigned to untagged frames that arrive on a port.
> **VID** stands for VLAN ID: The identifier for each Virtual Local Area Network.

1.2.3.3 Trunk Interface

- Connects switches or supports devices like routers that handle tagged frames.
- Carries multiple tagged VLANs using 802.1Q.

- Configured with a permitted VLAN list.

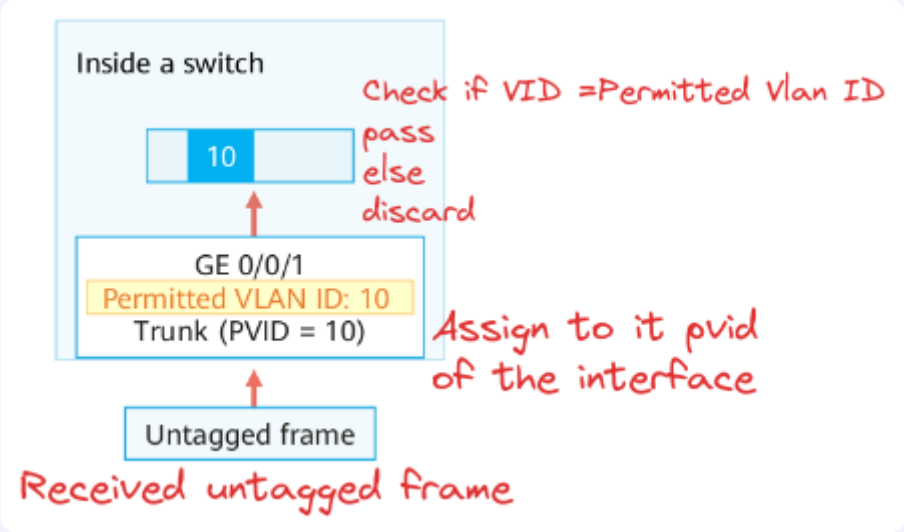
> Only allows frames if their VLAN ID is within the permitted list.

1.2.3.3.1 Frame Processing (Trunk)

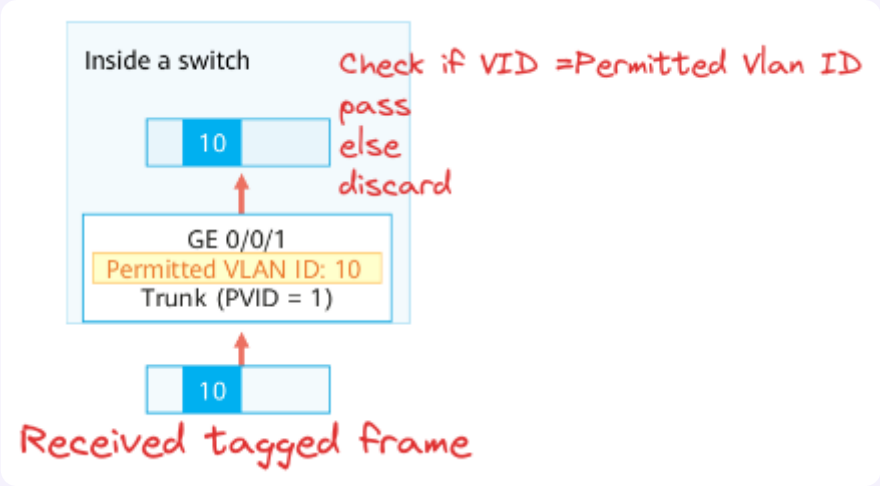
Action	Description
Receive (Untagged In)	Add a VLAN tag using the port's default VLAN ID (PVID) to untagged incoming frames. Decide to allow or block when the VID is in the list of VLAN IDs
Receive (Tagged In)	Check if incoming tagged frames are allowed on that port when the VID is in the list of VLAN IDs
Send (Untagged Out)	If the frame's VLAN ID matches the port's PVID, remove the VLAN tag before sending; otherwise, send as is (still tagged).
Send (Tagged Out)	Send tagged frames out of the port if their VLAN ID is permitted on that port. Frames with disallowed VLAN IDs are discarded.

Example

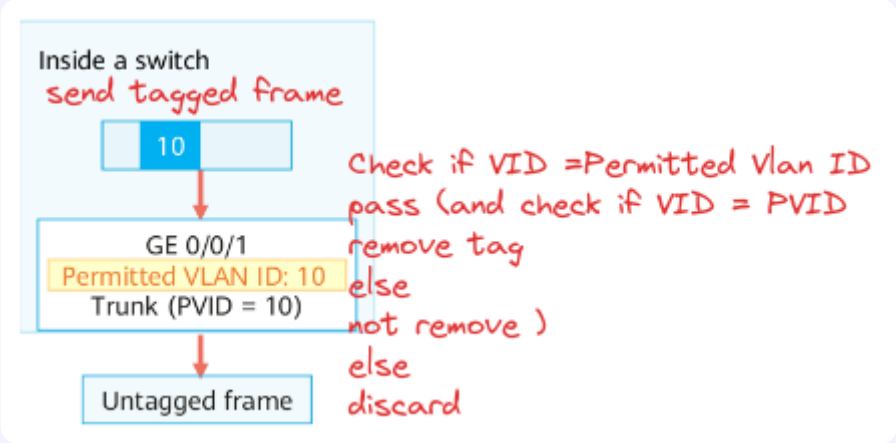
- **Receive (Untagged In):** A computer without VLAN configuration sends data to the switch, which adds the appropriate VLAN tag based on the switch port's (PVID).



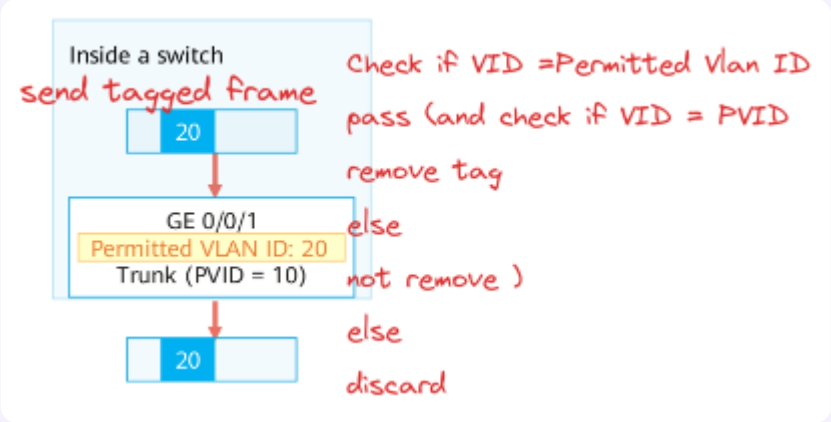
- **Receive (Tagged In):** A server sends data with a VLAN tag, and the switch checks if it should accept frames on that VLAN.



- **Send (Untagged Out):** The switch forwards data to a printer without a VLAN tag because the printer doesn't understand VLANs.



- **Send (Tagged Out):** The switch sends data with a VLAN tag to another switch that manages traffic for multiple VLANs.



1.2.3.4 Hybrid Interface

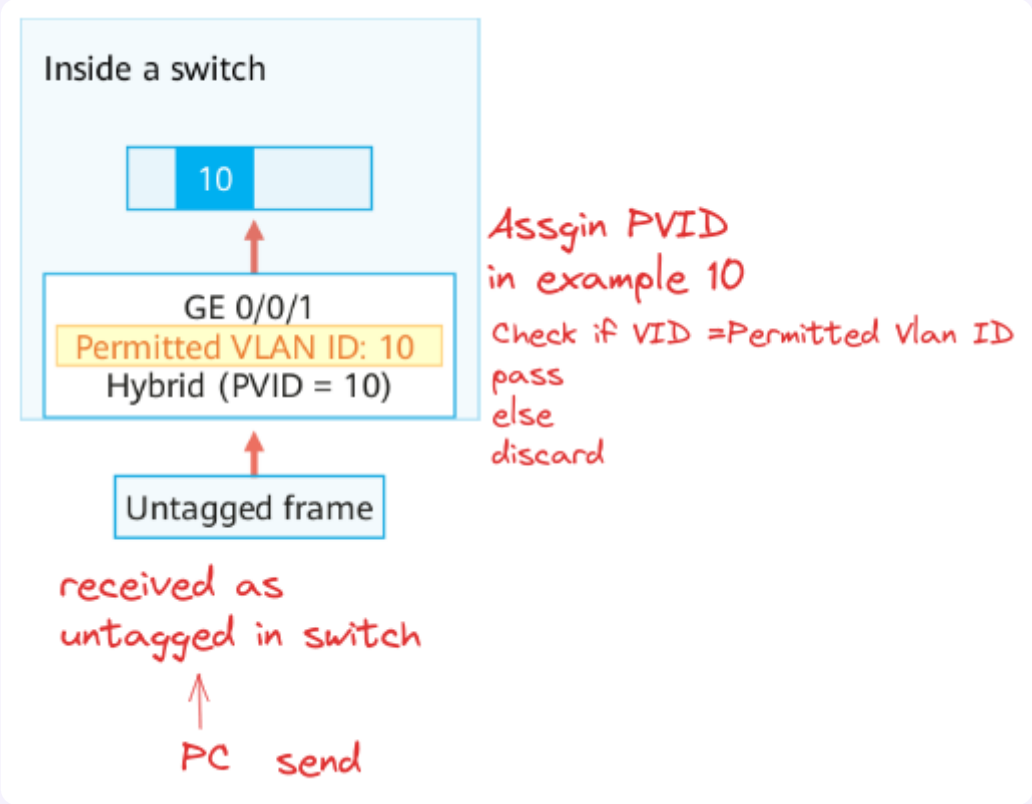
- Combines features of both access and trunk interfaces.
- Supports both tagged and untagged traffic across multiple VLANs.
- Configured with separate lists for tagged and untagged VLAN IDs.

1.2.3.4.1 Frame Processing (Hybrid)

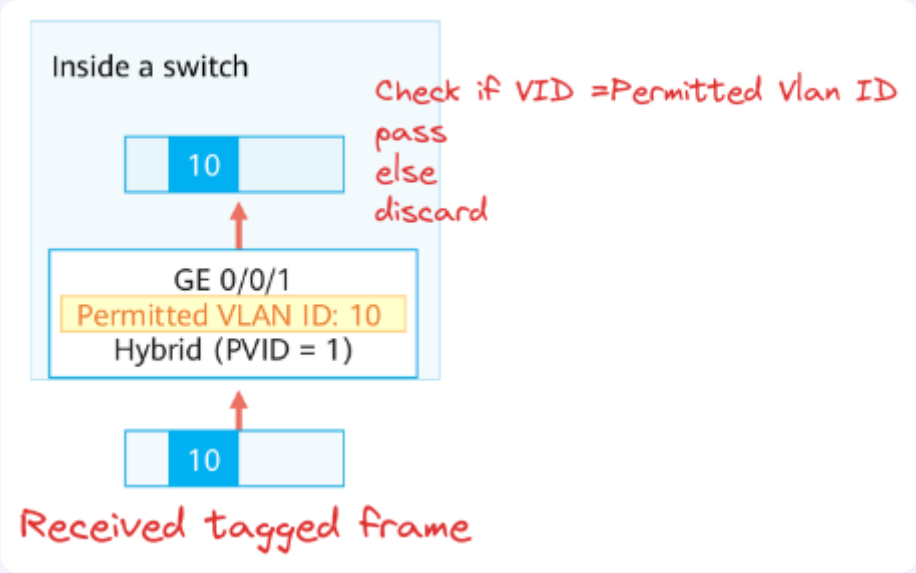
Action	Description
Receive (Untagged In)	When a frame without a VLAN tag arrives, the switch adds the default VLAN ID (PVID) to it. The frame's Acceptance is then determined when the VID is in the list of VLAN IDs otherwise discard
Receive (Tagged In)	If the VLAN ID of the frame is in the list of VLAN IDs permitted by the interface, the interface permits the frame. Otherwise, the interface discards the frame.
Send (Untagged Out)	If an interface allows a frame's VLAN ID and is set to not use VLAN tags, it will remove the tag before sending the frame.
Send (Tagged Out)	If the frame's VLAN ID is allowed by the interface and the interface is set to keep VLAN tags, then it sends the frame with its tag Whole.

Example

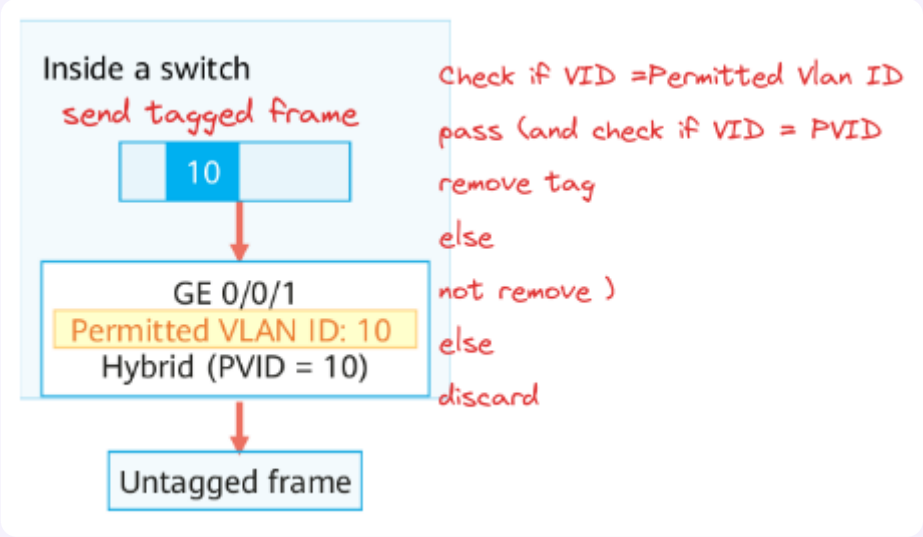
- **Receive (Untagged In):** A computer sends data without a VLAN tag, and the switch assigns its default VLAN to the data before processing.



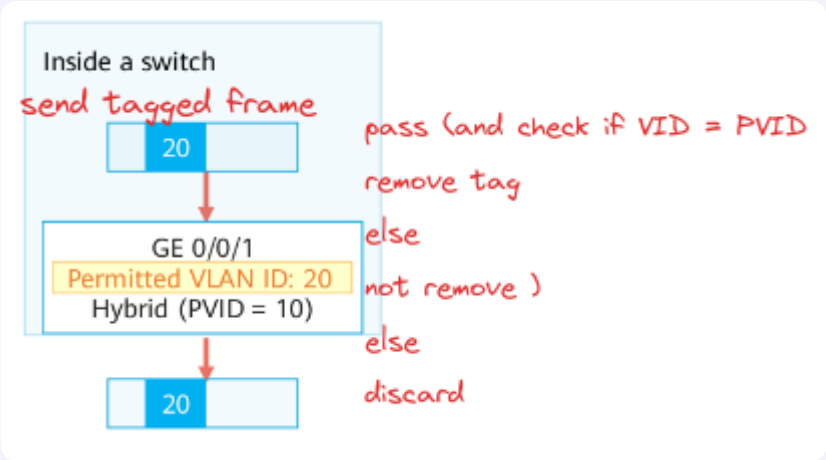
- **Receive (Tagged In):** A printer sends data with a VLAN tag, and the switch checks if it's allowed on that network; if not, the data is discarded.

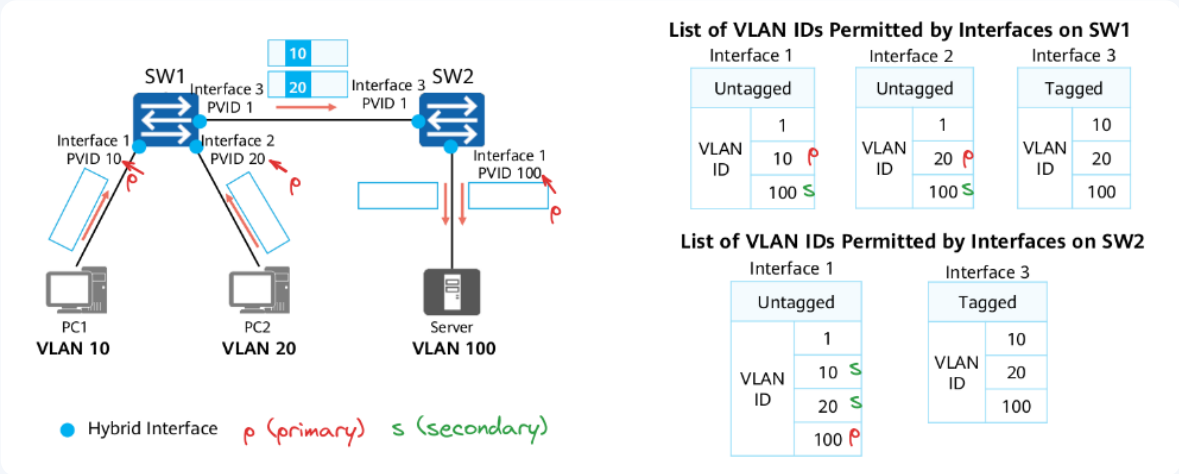


- **Send (Untagged Out):** A switch sends data to an older printer that doesn't understand VLAN tags, so it removes the tag before sending.



- **Send (Tagged Out):** A switch forwards data with its VLAN tag intact to another switch that also manages VLANs.





1.3 VLAN Applications

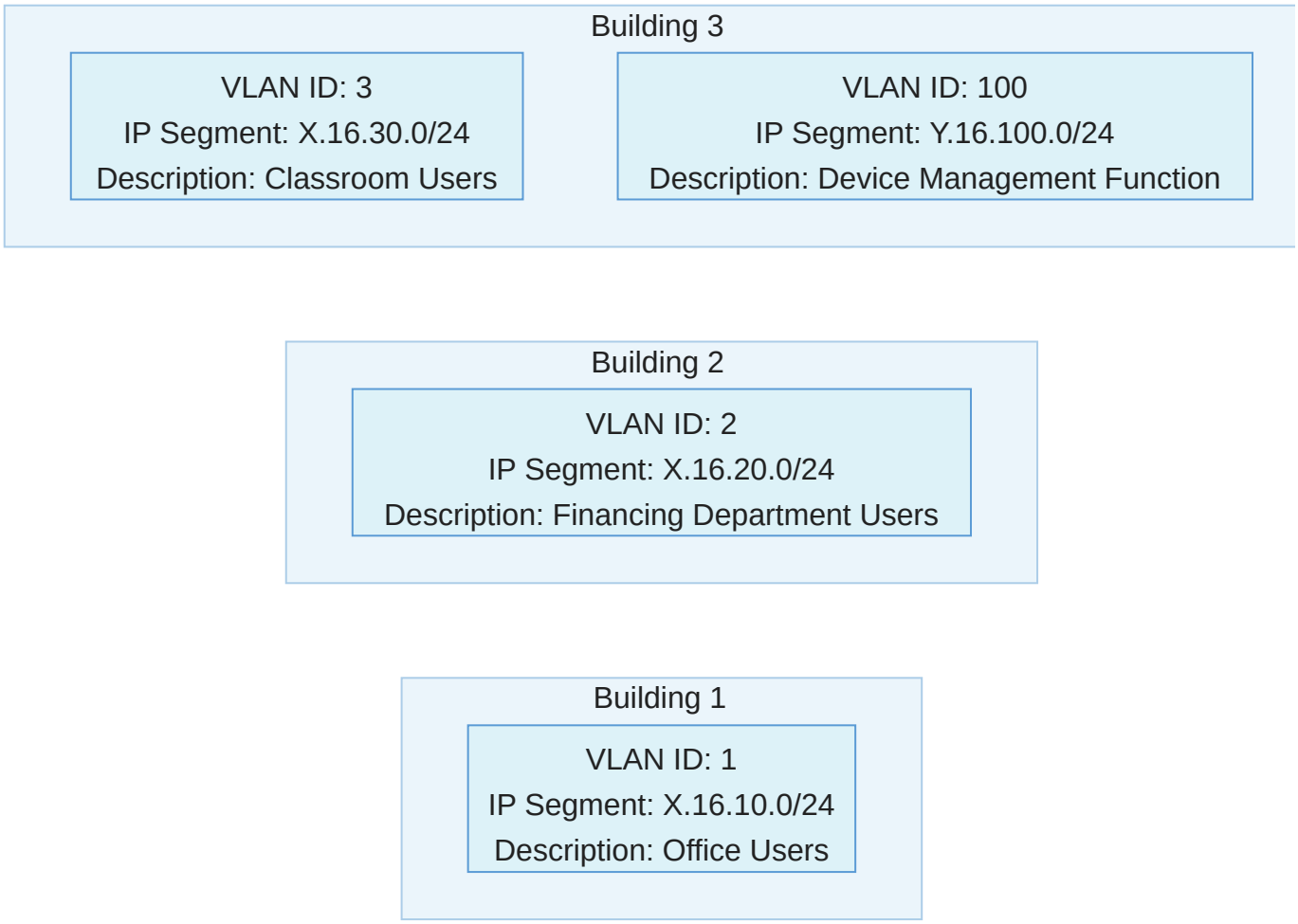
Tip

- **By Service**
  - `Voice`, `Video`, and `Data` services should have separate VLANs to enhance performance and security.
- **By Department**
  - Departments such as `Engineering`, `Marketing`, and `Financing` should have distinct VLANs for data segmentation.
- **By Application**
  - Applications or areas such as `Servers`, `Offices`, and `Classrooms` can be grouped into dedicated VLANs.

1.3.1 Example of VLAN Planning

VLAN ID	IP Address Segment	Description
1	X.16.10.0/24	Office Users
2	X.16.20.0/24	Financing Department Users
3	X.16.30.0/24	Classroom Users
100	Y.16.100.0/24	Device Management Function

> **Scenario:** Three buildings with different sections assigned to specific VLANs based on purpose and location.



> In this scenario, each building is connected through its respective access switch to the core switch located in the administrative building.

1.4 VLAN Configuration Examples

1.4.1 Basic Commands

1.4.1.1 Creating VLANs

- `[Huawei] vlan <vlan-id>` : Create a single VLAN.
- `[Huawei] vlan batch <vlan-id1> [to <vlan-id2>]` : Create multiple VLANs in a batch.

> VLAN IDs range from 1 to 4094.

> By default, all interfaces are added to the default VLAN with the ID of 1.

1.4.1.2 Deleting VLANs

- `[Huawei] undo vlan <vlan-id>` : Delete a specific VLAN.

1.4.1.3 Display VLANS

- Display current VLANS: `[Huawei] display vlan`

```
[SW1]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;        D: Down;                TG: Tagged;  UT: Untagged;
MP: Vlan-mapping;                     ST: Vlan-stacking;
#: ProtocolTransparent-vlan;          *: Management-vlan;
--------------------------------------------------------------------------------
VID           Type        Ports
--------------------------------------------------------------------------------
1             common      UT:GE0/0/1(U)     GE0/0/2(U)     GE0/0/3(U) ......
10            common      UT:GE0/0/1(U)
                          TG:GE0/0/3(U)
20            common      UT:GE0/0/2(U)
                          TG:GE0/0/3(U)
100           common      UT:GE0/0/1(U)     GE0/0/2(U)
                          TG:GE0/0/3(U)
......
```

1.4.2 Interface-based VLAN Assignment

1.4.2.1 Access Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type access` : set the link type of the interface to access.
- `[Huawei-GigabitEthernet0/0/1] port default vlan <vlan-id>` : configure a default VLAN for the interface

1.4.2.2 Trunk Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type trunk` : set the link type of the interface to trunk.
- `[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { <vlan-id1> to <vlan-id2> } || all` : add the trunk interface to specified VLANs.
- `[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan <vlan-id>` : configure a default VLAN for the trunk interface.

1.4.2.3 Hybrid Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type hybrid` : set the link type of the interface to hybrid.
- `[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan { <vlan-id1> to <vlan-id2> } || all` : dd the hybrid interface to specified VLANs in untagged mode.
- `[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan { <vlan-id1> to <vlan-id2> } || all` : add the hybrid interface to specified VLANs in tagged mode.
- `[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan <vlan-id>` : configure a default VLAN for the hybrid interface.

1.4.3 MAC Address-based VLAN Assignment

1.4.3.1 Associating MAC with a VLAN

- `[Huawei-vlan10] mac-vlan mac-address <mac-address> <mac-address-mask> || <mac-address-mask-length>` : Associate MAC address with a specific VLAN.

> - **mac-address:** The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or any multicast address.
> - **mac-address-mask:** specifies the mask of a MAC address. The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
> - **mac-address-mask-length:** specifies the mask length of a MAC address. The value is an integer ranging from 1 to 48.

1.4.3.2 Enabling MAC-based Assignment on an Interface

- `[Huawei-GigabitEthernet0/0/1] mac-vlan enable` : Enable MAC address-based assignment on an interface.

1.4.3.3 Display MAC-VLAN

- Display MAC-VLAN associations: `[Huawei] display mac-vlan mac-address all`

```
[SW1]display mac-vlan mac-address all
-----------------------------------------------------------------
MAC Address          MASK         VLAN         Priority
-----------------------------------------------------------------
001e-10dd-dd01       ffff-ffff-ffff  10        0
001e-10dd-dd02       ffff-ffff-ffff  10        0
001e-10dd-dd03       ffff-ffff-ffff  10        0

Total MAC VLAN address count: 3
```

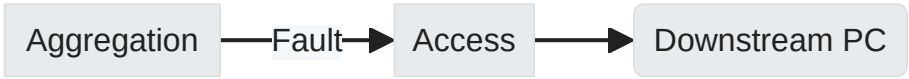
STP Principles and Configuration

1 STP Principles and Configuration

1.1 STP Overview

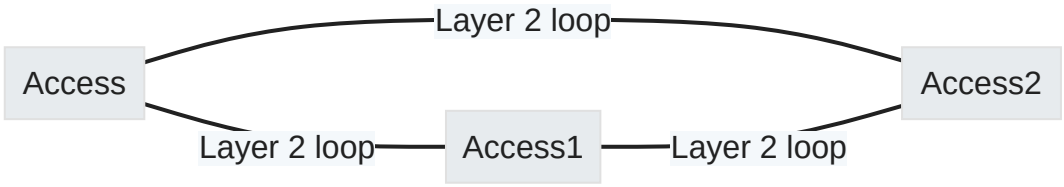
1.1.1 Network Without Redundancy

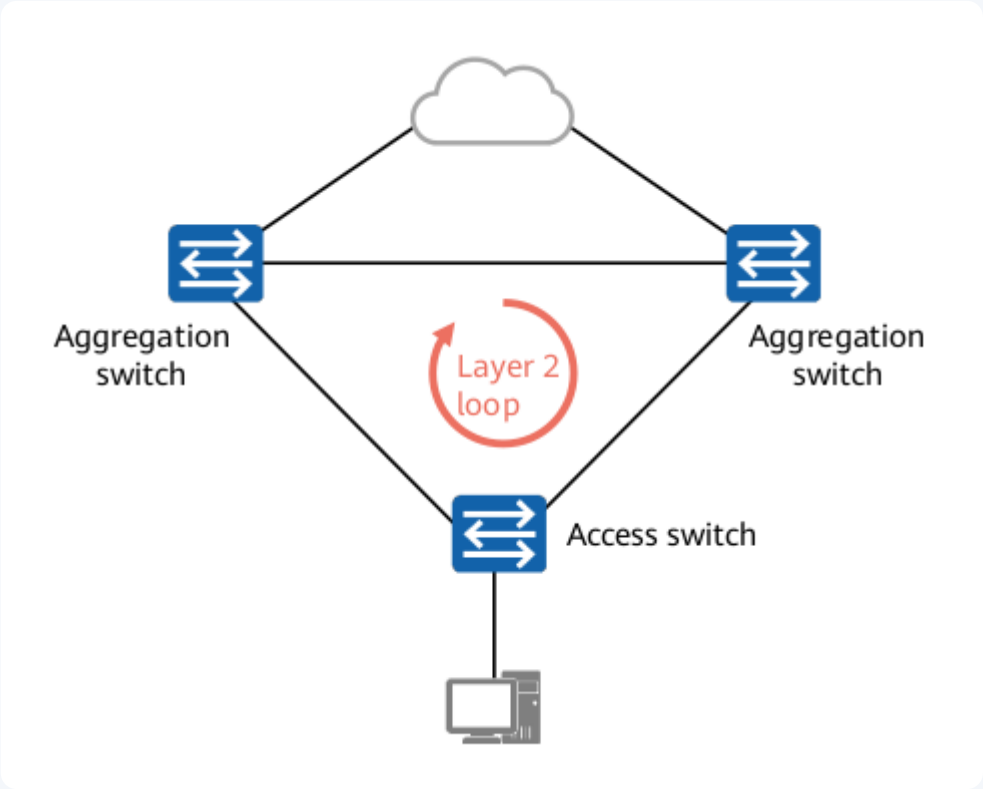
> - If a fault occurs, downstream hosts are disconnected.
> - Single Point of Failure (SPOF) issue.



1.1.2 Redundancy and Loops

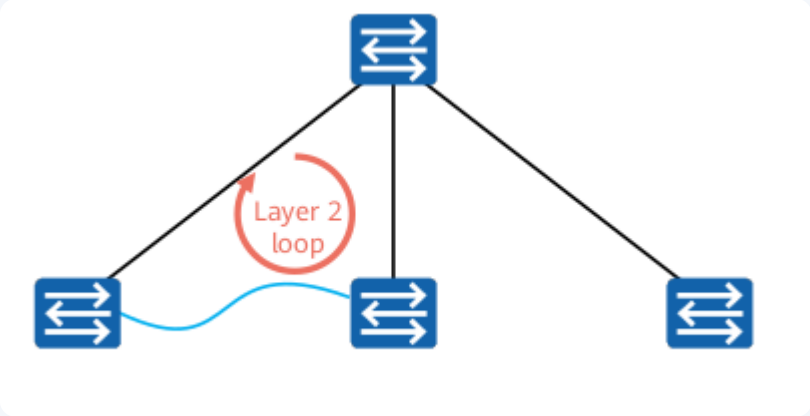
- Redundant links improve network reliability.
- However, they introduce Layer 2 loops.



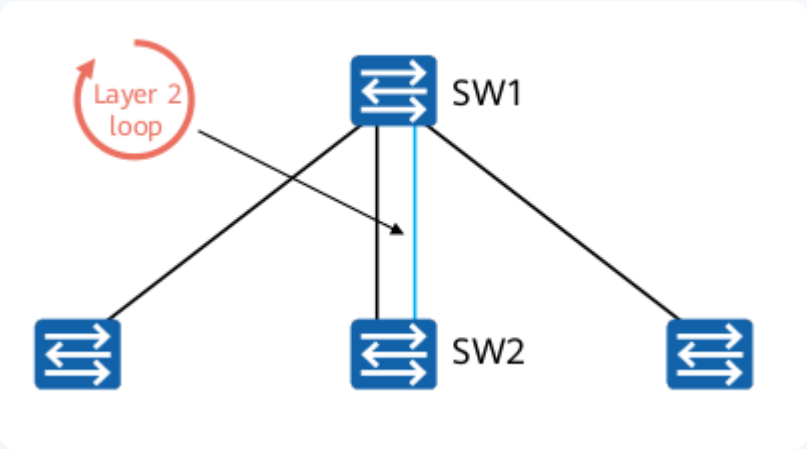


1.1.3 Human Errors Causing Loops

1.1.3.1 Case 1: Incorrect Cable Connections



1.1.3.2 Case 2: Incorrect Manual Configurations

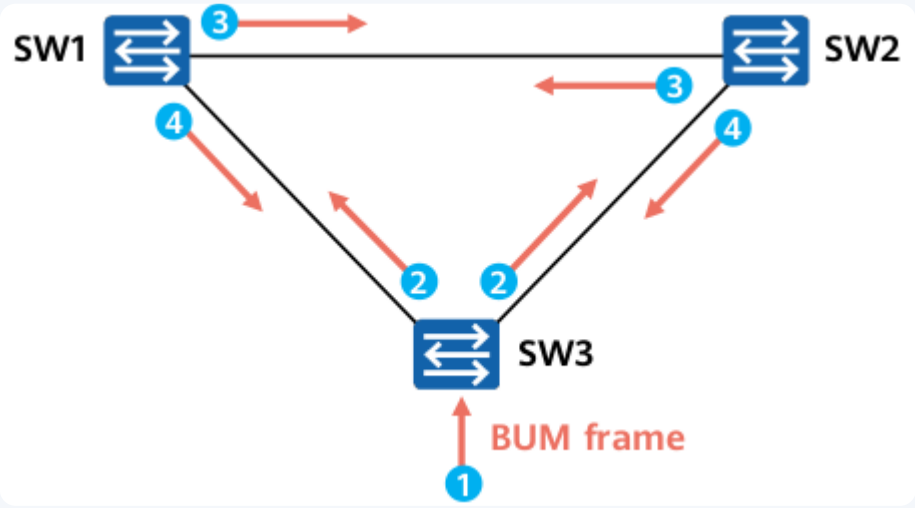


binding the link between SW1 and SW2 to a logical link (aggregation link)

1.1.4 Issues Caused by Layer 2 Loops

1.1.4.1 Issue 1: Broadcast Storm

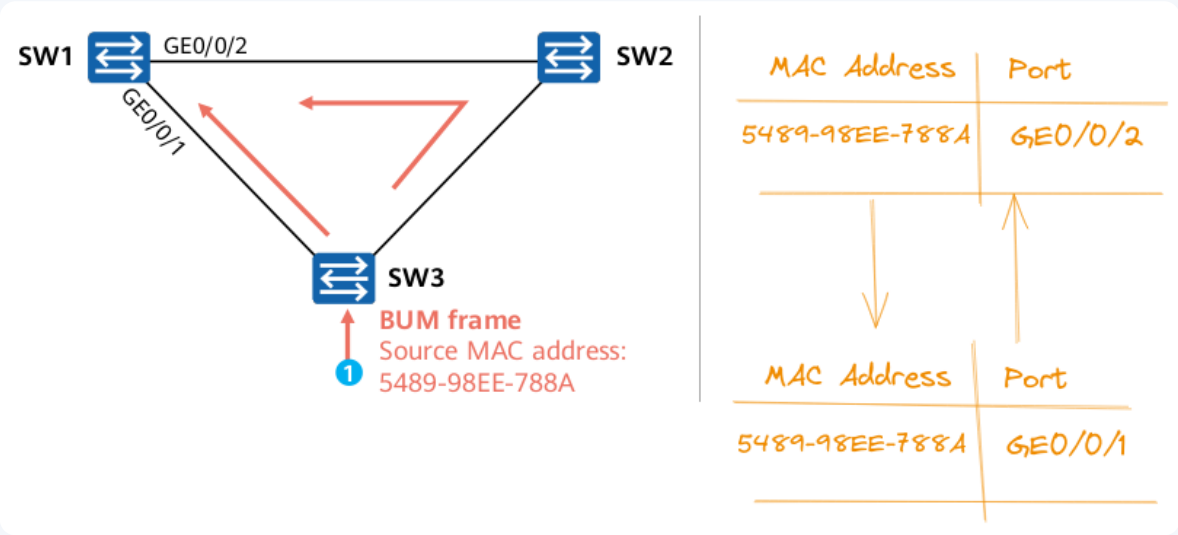
- BUM frames (broadcast, unknown unicast, multicast) are flooded repeatedly.
- Causes network resource exhaustion and service interruption.



When SW3 receives the BUM frames, it floods the frames. After SW1 and SW2 receive the BUM frames, they flood the frames again.

1.1.4.2 Issue 2: MAC Address Flapping

- Frequent switching of MAC address between ports.
- Results in unstable MAC address table entries.

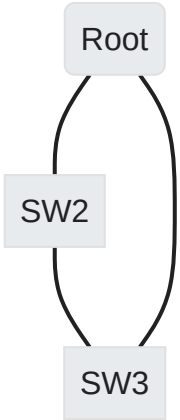


SW1 is used as an example. The MAC address of 5489-98EE-788A is frequently switched between GE0/0/1 and GE0/0/2, causing MAC

> address flapping

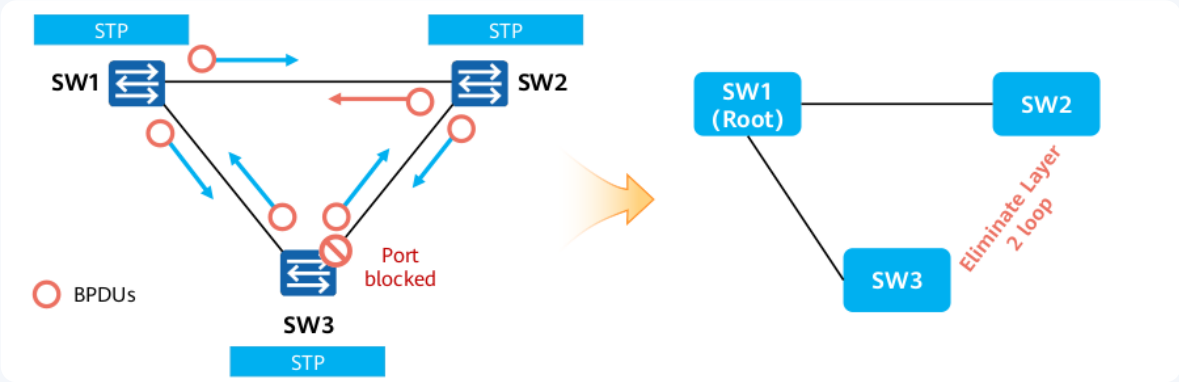
1.1.5 Spanning Tree Protocol (STP)

1.1.5.1 STP Introduction



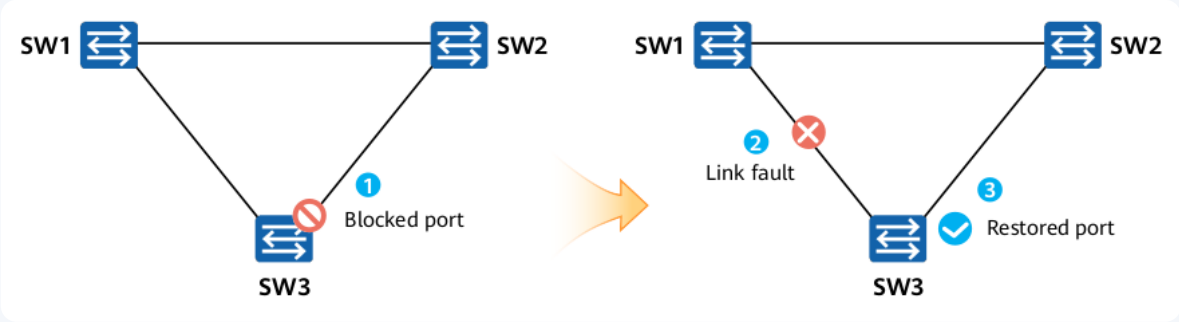
STP prevents loops by:

- Blocking one or more ports on the network.
- Calculating a loop-free tree topology.



1.1.5.2 Dynamic Response to Topology Changes

STP monitors topology changes and adjusts accordingly:



1.1.6 Comparison of Layer 2 vs. Layer 3 Loops

Factor	Layer 2 Loop	Layer 3 Loop
Root Cause	Redundancy or wrong cabling.	Routing loop.
Prevention	Protocols like STP.	TTL field in IP headers.
Impact	Data frame forwarding issues.	Infinite packet forwarding.

1.2 Basic Concepts and Working Mechanism of STP

1.2.1 Bridge ID (BID)

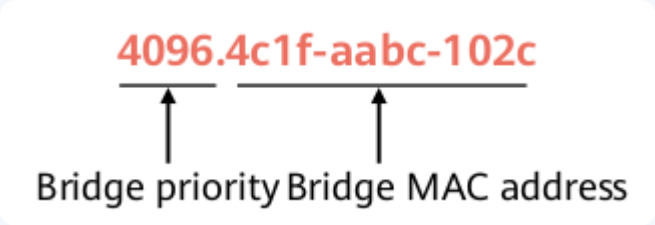
- BID is a unique identifier for each switch running STP.
- It consists of a `16-bit bridge priority` and a `48-bit MAC address`.
- The device with the smallest BID becomes the `root bridge`.

> As defined in IEEE 802.1D,

> The default bridge priority is 32768.

> The bridge priority can be changed but must be a multiple of 4096.

> If the priorities are the same, devices compare MAC addresses. A smaller MAC address indicates a `Root Bridge` .

> 
>

1.2.2 Root Bridge

- The root bridge serves as the root of an STP network tree.
- Elected based on lowest BID.

> Once the network is set up,root bridge regularly sends out configuration `BPDUs` to other devices at specific intervals so they can pass on info about any changes, keeping the network running smoothly.

1.2.3 STP Cost

- Each port has a cost that contributes to the Root Path Cost (RPC).
- Higher port bandwidth → Lower cost.

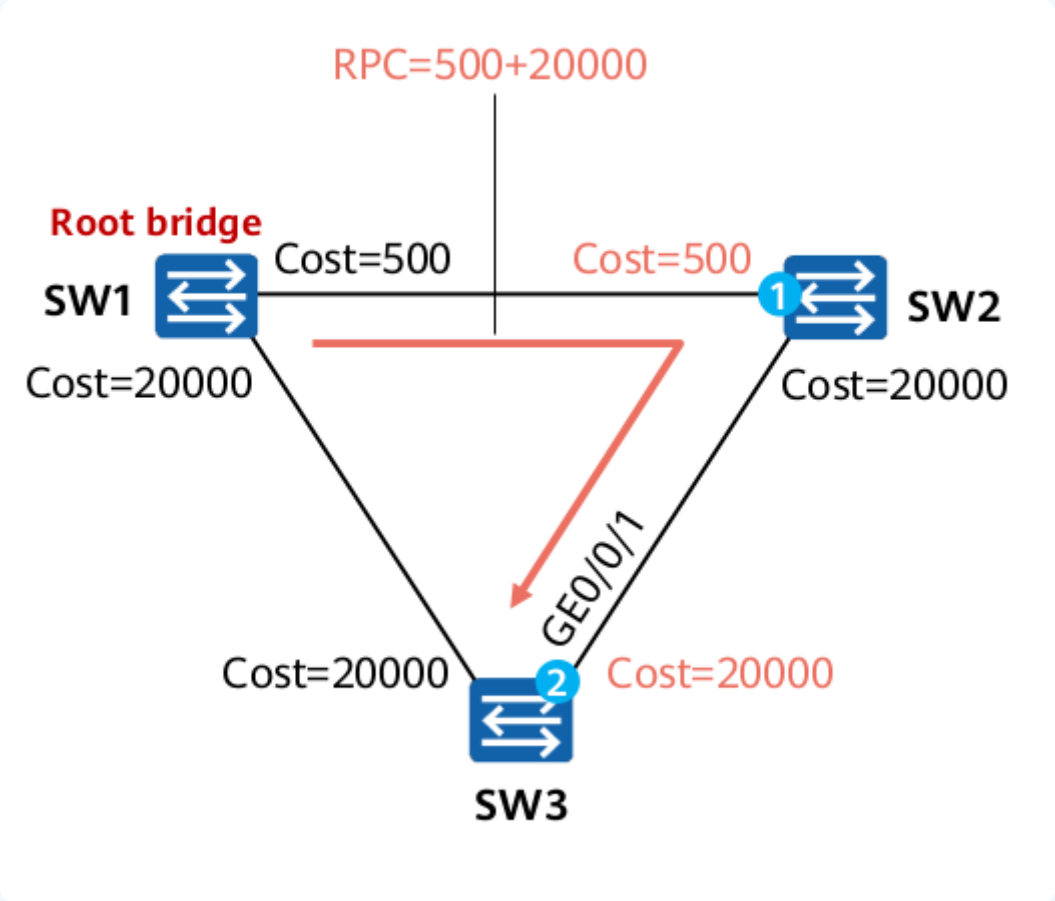
> Huawei switches use IEEE 802.1t to calculate the path cost.

1.2.3.1 Cost Calculation Methods

Port Rate	Port Mode	Recommended STP Cost		
		IEEE 802.1d-1998	IEEE 802.1t	Huawei Legacy Standard
100 Mbit/s	Half-duplex	19	200,000	200
	Full-duplex	18	199,999	199
	Aggregated link: two ports	15	100,000	180
1000 Mbit/s	Full-duplex	4	20,000	20
	Aggregated link: two ports	3	10,000	18
10 Gbit/s	Full-duplex	2	2000	2
	Aggregated link: two ports	1	1000	1
40 Gbit/s	Full-duplex	1	500	1
	Aggregated link: two ports	1	250	1
100 Gbit/s	Full-duplex	1	200	1
	Aggregated link: two ports	1	100	1
...				

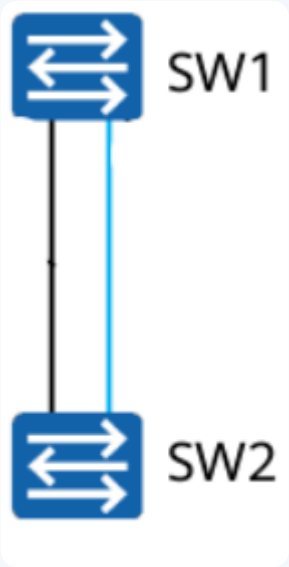
1.2.3.2 Root Path Cost (RPC)

```
RPC = Sum of port costs along the path to root
```



1.2.4 Port ID (PID)

`PID = Port Priority + Port Number (12 bits)`

> PIDs uses to identify ports and to elect a designated port in a specific scenario.
>
> 
>

> Default port priority is `128` . Ranges from 0 to 240 Must be a multiple of `16` .

1.2.5 Bridge Protocol Data Units (BPDUs)

> STP selects the root bridge by transmitting configuration BPDUs between switches and determines the role and status of each switch port.

> Once the network is stable, only the Root Bridge sends out configuration messages by itself, while other bridges send these messages only after getting them from devices upstream devices.

1.2.5.1 Format of Configuration BPDUs

Byte Field	Parameter	Description
2	PID	Protocol Identifier, always set to 0 for STP (Spanning Tree Protocol).
1	BPDU Type	Identifies the type of BPDU: 0x00 for configuration, 0x80 for TCN (Topology Change Notification).
1	Flags	Flags indicating status such as Topology Change or Acknowledgment. Only the first two and last two bits are used in STP.
8	Root ID	Identifier of the root bridge in the network.
4	RPC	Root Path Cost, represents the total cost of the path from the current bridge to the root bridge.
8	Bridge ID	Identifier of the bridge sending this BPDU.
2	Port ID	Identifier of the port sending this BPDU, includes priority and number.
2	Message Age	Time since BPDU left root bridge, increases by one with each hop and indicates distance to root. Default is every second.
2	Max Age	Maximum age before considering a link faulty if no BPDU received; default is typically set to 20 seconds.
2	Hello Time	Frequency at which root bridge sends out BPDUs; default is typically set to every 2 seconds.
2	Forward Delay	Time spent in Listening and Learning states; default is typically set to about 15 seconds.

1.2.5.2 Types of BPDUs

BPDU Type	Description
Configuration BPDU	Key to topology calculation
Topology Change Notification (TCN)	Notifies switches about topology changes

1.2.5.3 BPDU Comparison Rules

Use this order when comparing fields within a configuration BPDU:

1. **Smallest Root Identifier (`BID` of root):** to elect root bridge
2. **Smallest Root Path Cost (`RPC`):** to change port Role to Root port
3. **Smallest Bridge Identifier (`BID` of sender):** If there's a tie in path costs, STP looks at who sent the BPDU. The switch with the smallest BID wins and its path is used.
4. **Smallest Port Identifier (`PID`):** If there's still a tie after looking at BIDs, STP looks at port IDs. Each port on a switch has its own identifier, and once again, smaller is better - so the port with the smallest ID is chosen for forwarding traffic.

1.2.6 Port Roles in STP

Role	Description
Designated Port	Forwards data frames; one per network segment
Root Port	Optimal path to root; one per non-root switch
Alternate Port	Blocked to prevent loops

1.2.7 STP Calculation

1.2.7.1 Root Bridge Election

1.2.7.1.1 Steps:

1. Each switch considers itself as the root bridge initially.

2. Switches compare received BPDUs and elect the switch with the smallest BID as the root bridge.

> Plan STP network in advance by setting the bridge priority to 0 for the planned root switch to ensure Continuity.

1.2.7.2 Port Roles

1.2.7.2.1 Root Port Selection

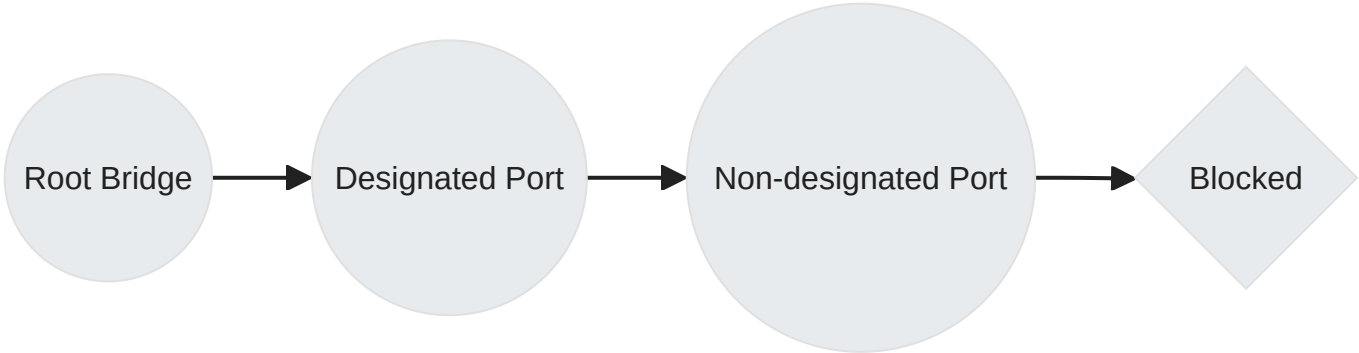
- Each non-root bridge selects one root port with **optimal path** to the root bridge based on:
  - Smallest Root Path Cost (RPC)
  - Smallest Bridge ID (BID)
  - Smallest Port ID (PID)

1.2.7.2.2 Designated Port Selection

- A designated port is elected on each link to ensure unique and optimal paths.
- Uses same criteria as root port selection: RPC $->$ BID $->$ PID (Smallest)

1.2.7.2.3 Non-designated Port Blocking

- Any port that is neither a root nor designated port becomes a non-designated or alternate port.
- Non-designated ports are blocked by STP to prevent loops.

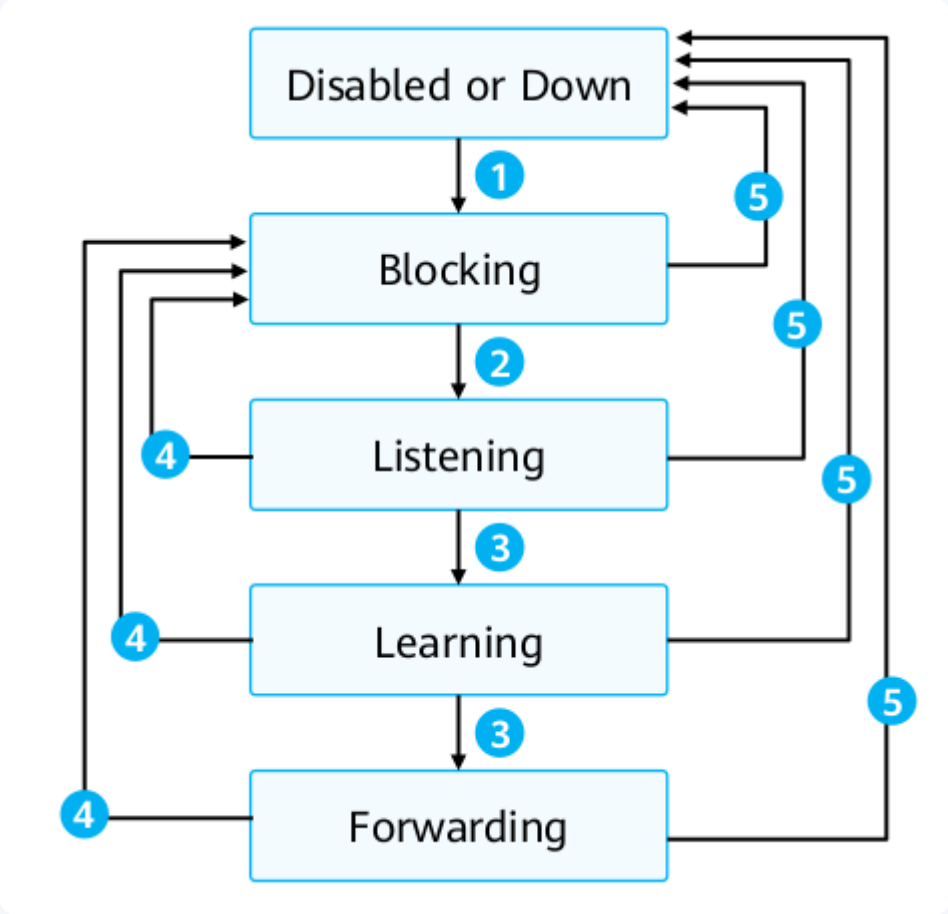


1.2.8 STP Port States

State	Description
Disabled	No BPDU/service data frame processing.
Blocking	Listens to BPDUs without forwarding data frames or learning MAC addresses.
Listening	Considers port as candidate for root/designated but still in calculation.The port can send and receive BPDUs but cannot send or receive service data frames or learn MAC addresses.
Learning	Creates MAC entries without forwarding traffic.
Forwarding	Sends/receives service data frames and processes BPDUs; final state for active ports.

> **Service data frames:** are the actual network traffic carrying user data, such as emails or website content

1.2.8.1 State Transitions



1. When a port is initialized or activated, it automatically enters the blocking state.
2. The port is elected as the root port or designated port and automatically enters the Listening state.
3. The Forward Delay timer expires and the port is still the root port or designated port.

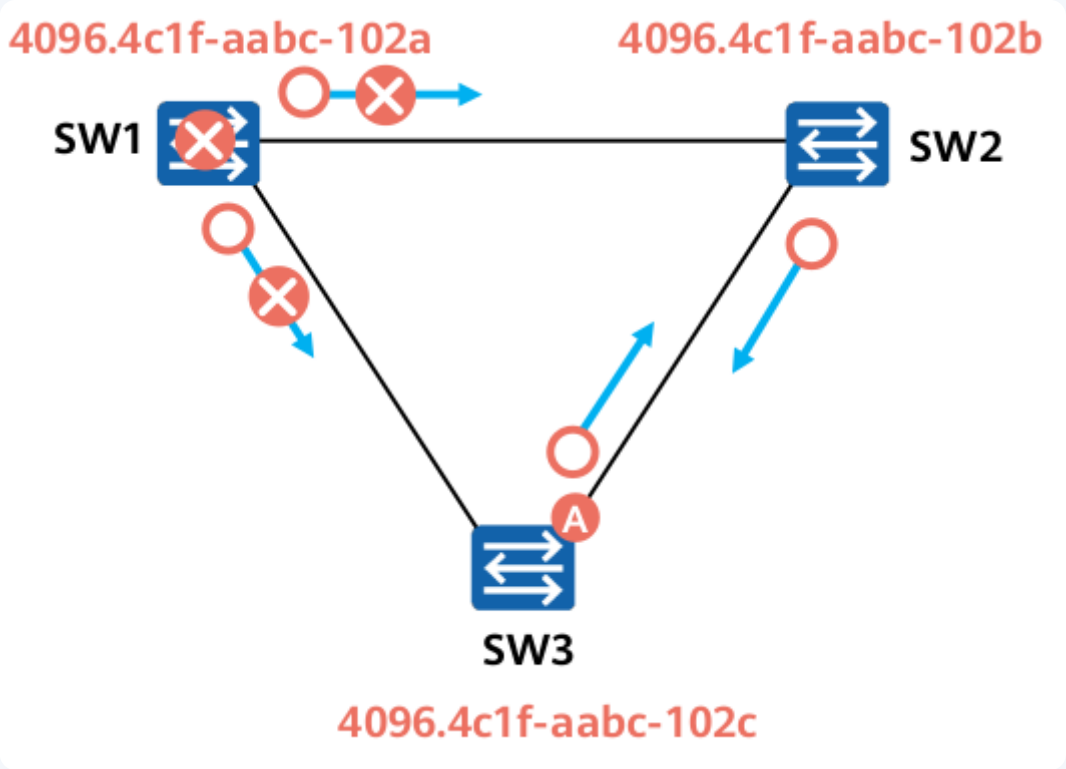
> Upon Forward Delay timer expiration, if a port remains the root port or designated port, it means no better path was discovered and STP received no information prompting a change in the port's status.

4. The port is no longer the root port or designated port.
5. The port is disabled or the link fails.

> **STP transitions** require 15 seconds from listening to learning state and another 15 seconds from learning to forwarding state.

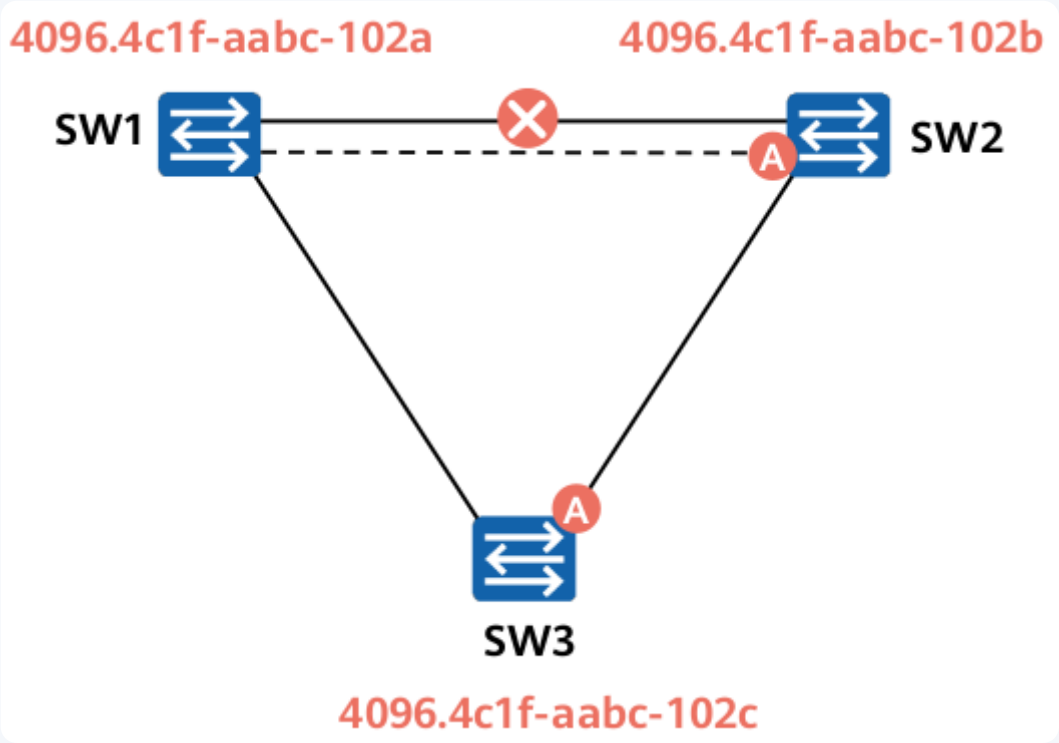
1.2.9 Topology Changes Handling

1.2.9.1 Root Bridge Fault



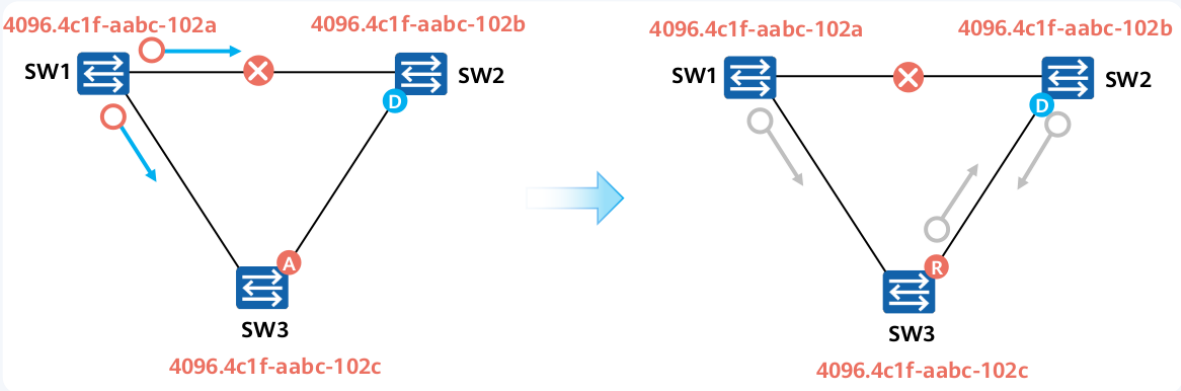
1. The root bridge SW1 fails and stops communicating with other switches.
2. SW2 detects the failure after waiting 20 seconds, prompting a re-election among the remaining switches to choose a new root bridge.
3. SW3 becomes the new root bridge, and its port A starts forwarding traffic after 30 seconds (two Forward Delay intervals from listening to forwarding 30 sec).
4. Network recovery from root bridge failure takes approximately 50 seconds total.

1.2.9.2 Direct Link Failure Recovery



1. When SW2's root port link fails, the alternate port becomes the new root port and starts forwarding traffic after 30 seconds(two Forward Delay intervals from listening to forwarding 30 sec)..
2. The alternate port moves from blocking to listening, then learning, and finally to forwarding state during this transition.

1.2.9.3 Indirect Link Failure Recovery

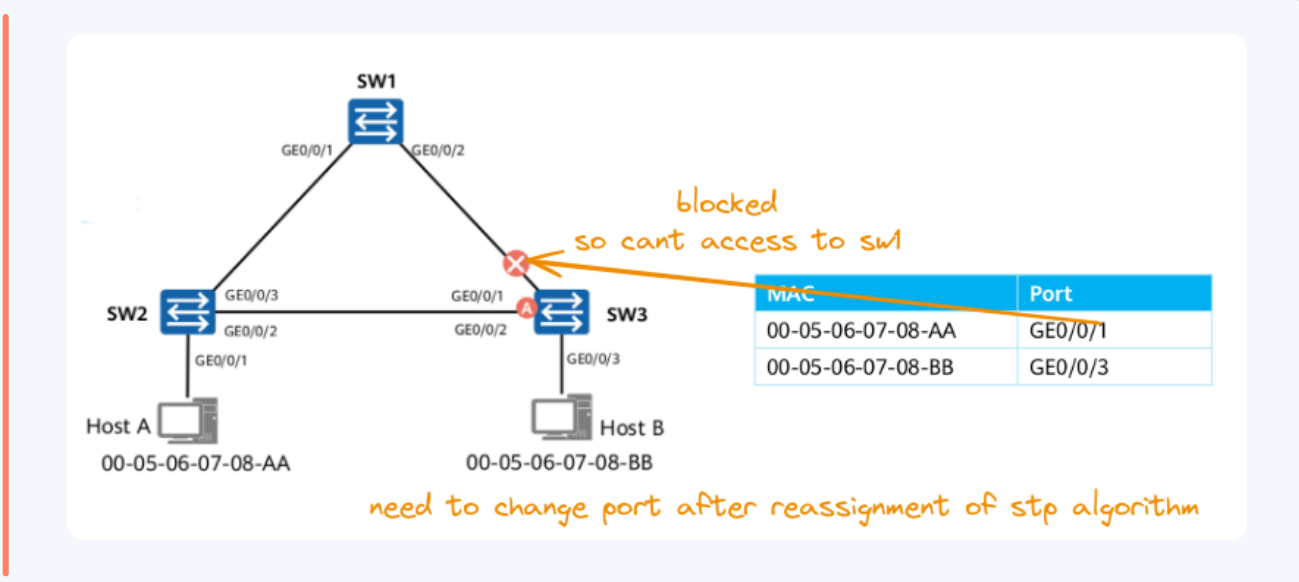


1. An indirect link failure between SW1 and SW2 prevents SW2 from receiving STP BPDUs from SW1.

2. After 20 seconds, the Max Age timer on SW2 expires, indicating outdated topology information.
3. SW2 may assume it's the root bridge and starts issuing its own BPDUs.
4. When SW3 receives these BPDUs from both switches, it compares them and realizes the BPDU from SW1 is better, so it doesn't switch to using SW2 as the root bridge.
5. The alternate port on SW3 transitions from Blocking to Listening for 15 seconds, then Learning for another 15 seconds, before moving to Forwarding state.
6. It takes about 50s to recover from an Unphysical link failure, which is equal to the value of the Max Age timer plus twice the value of the Forward Delay timer.

1.2.9.4 Topology Change Notification (TCN)

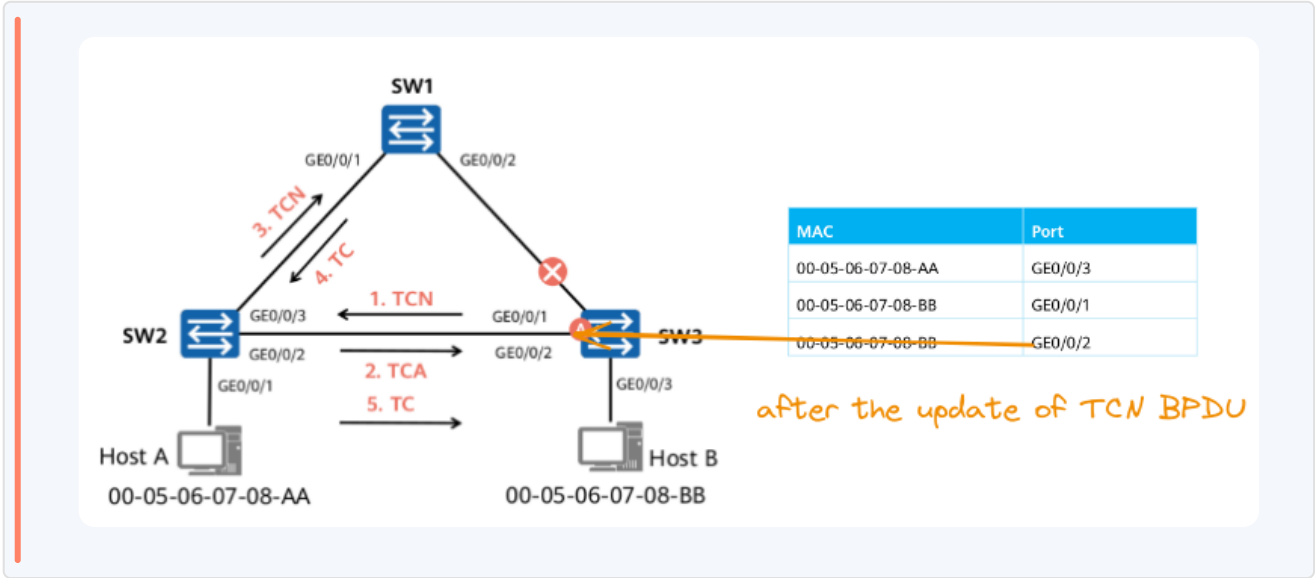
Problem:



- SW3's root port is broken, causing the network's path layout to change.
- Host B can't get frames from Host A because of outdated MAC address information in the switches.
- Switches use a MAC address table to decide where to send data, with entries aging out after 300 seconds by default.

- After a network change, switches must quickly update their MAC address tables to prevent sending data the wrong way.

When topology changes occur:



1. Switches send out TCN BPDUs.
2. Root bridge sets TC flag in BPDU To update Mac Table address, Quickly others to shorten MAC entry aging time from default (300s) to Forward Delay value (~15s).

1.3 Basic STP Configurations

1.3.1 Configuration Commands

1.3.1.1 Set Working Mode

```
[Huawei] stp mode  <stp> || <rstp> || <mstp>
```

- `stp` : Classic Spanning Tree Protocol.
- `rstp` : Rapid Spanning Tree Protocol.

- `mstp` : Multiple Spanning Tree Protocol.

> Default mode is MSTP.

1.3.1.2 Root Bridge Configuration

```
[Huawei] stp root primary   // Sets switch as root bridge with priority 0.
[Huawei] stp root secondary // Sets switch as secondary root with priority 4096.
```

1.3.1.3 Set STP Priority

```
[Huawei] stp priority <priority>
```

> Default priority is 32768.

1.3.1.4 Configure Path Cost Method

```
[Huawei] stp pathcost-standard <dot1d-1998> || <dot1t> || <legacy>
```

> All switches must use the same path cost calculation method.

> Default path cost is dot1t on Huawei.

1.3.1.5 Set Port Path Cost

```
[Huawei-GigabitEthernet0/0/1] stp cost <cost>
```

1.3.1.6 Set Port Priority

```
[Huawei-GigabitEthernet0/0/1] stp priority <priority>
```

> Default priority is 128.

1.3.1.7 Enable STP/RSTP/MSTP Globally

```
[Huawei] stp enable
```

> By default, STP, RSTP, or MSTP is enabled on a switch.

1.3.1.8 Checking Port States

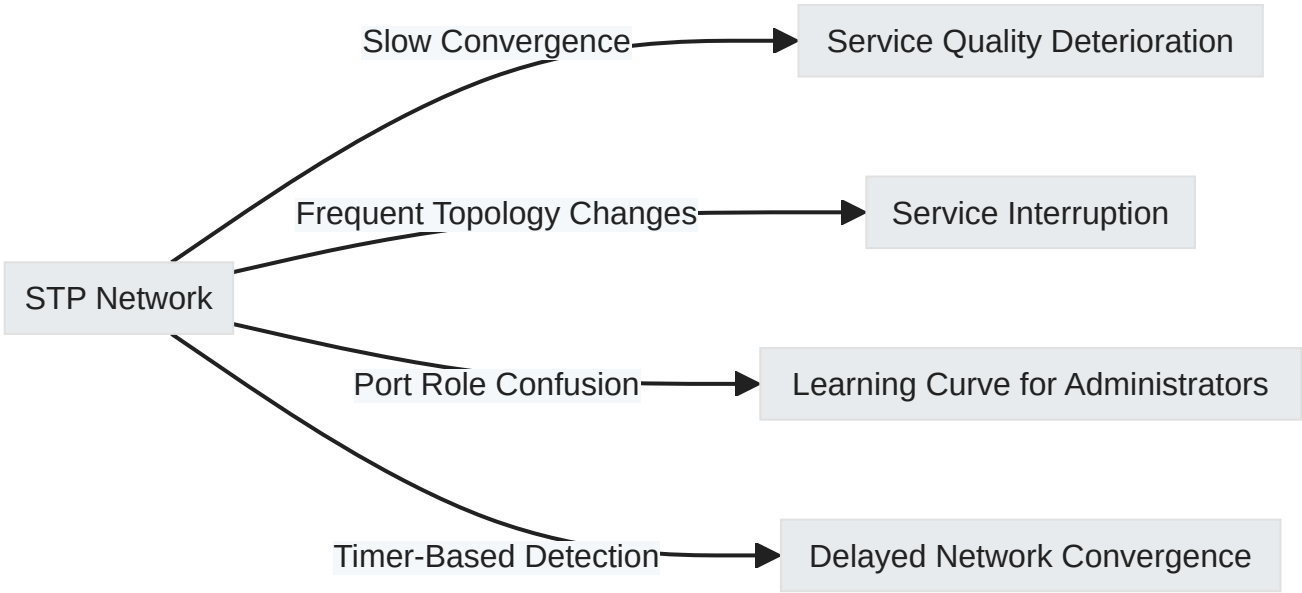
```
<Huawei> display stp brief
```

MSTID	Port	Role	State
0	GigabitEthernet0/0/21	ROOT	FORWARDING
0	GigabitEthernet0/0/22	ALTE	DISCARDING

1.4 Improvements Made in RSTP

1.4.1 Disadvantages of STP

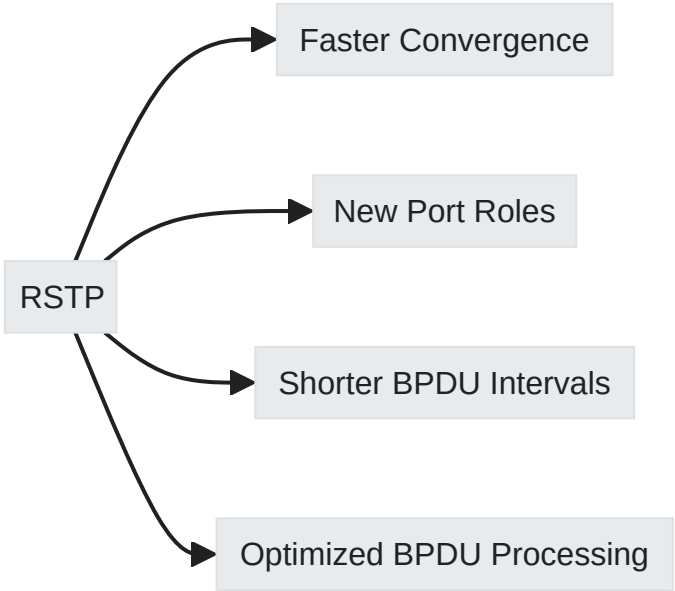
- Frequent network changes can cause slow protocol convergence, resulting in potential Interference or degraded performance of network services.
- The complexity and Unexpected nature of port roles and states in some protocols can be challenging for inexperienced network administrators to understand and manage.
- Protocols that rely on timers to detect changes in the network topology may not recognize these changes promptly, leading to a delayed response.
- Protocols that send Bridge Protocol Data Units (BPDUs) across the whole network Hurt from slow convergence times, as the propagation of these units takes time and can slow down the overall response to changes.



1.4.2 Advantages of RSTP over STP

- Faster convergence compared to STP.
- Defines new port roles for better understanding and deployment simplicity.
- Shorter timeout intervals for BPDUs.
- Optimized BPDU processing methods.

> RSTP defined in IEEE 802.1w.



1.4.3 Port Roles in RSTP

1.4.3.1 Traditional Port Roles

- Root Port (R)
- Designated Port (D)

1.4.3.2 New Port Roles in RSTP

- **Alternate Port (A):** Provides an alternative path to the root bridge when the root port fails.
- **Backup Port (B):** Serves as a backup path from the root bridge.

1.4.4 Edge Ports in RSTP

1.4.4.1 Characteristics of Edge Ports:

> An edge port connects directly to user terminals, not switches. It transitions immediately to Forwarding state upon initialization so no delay occur.

> If an edge port receives a configuration BPDU, it reverts to a common STP port and triggers recalculation of the spanning tree, potentially causing network flapping.

1.4.5 Port States in RSTP vs. STP

1.4.5.1 Reduced Number of States in RSTP:

1. **Discarding:** Neither forwards traffic nor learns MAC addresses.
2. **Learning:** Learns MAC addresses but does not forward traffic.
3. **Forwarding:** Forwards user traffic and learns MAC addresses.

1.4.5.2 Corresponding States Between Protocols:

STP State	RSTP State	Port Role
Disabled	Discarding	Disabled
Blocking	Discarding	Alternate or Backup
Listening	Discarding	Root or Designated
Learning	Learning	Root or Designated
Forwarding	Forwarding	Root or Designated

> Discarding: This combines Disabled, Blocking, and Listening from STP

> into one state where the port isn't forwarding frames.

1.5 STP Advancement

1.5.1 Overview

- STP and RSTP ensure a loop-free topology for Ethernet networks.
- Both protocols have limitations when dealing with multiple VLANs.
- All VLANs share one spanning tree, leading to inefficient link utilization.

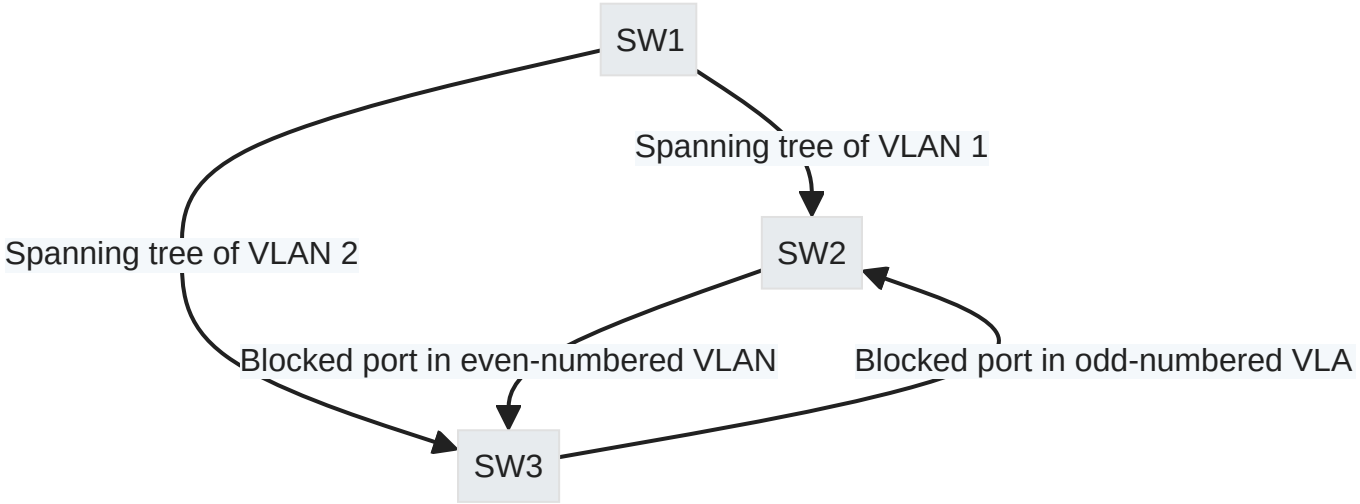
1.5.2 Defects of STP/RSTP

> **Note**
>
> A single spanning tree across all VLANs can result in Insufficient load balancing and underutilization of network links.

1.5.2.1 Issues

- **Inter-VLAN Load Balancing:** Cannot be performed effectively.
- **Blocked Links:** Do not transmit any traffic, causing potential packet transmission failures within VLANs.

1.5.3 Huawei's VBST (VLAN-Based Spanning Tree)



1.5.3.1 Benefits

---

1. Eliminates loops per VLAN.
2. Implements link multiplexing for improved efficiency.
3. Reduces configuration and maintenance costs.

1.5.4 MSTP (Multiple Spanning Tree Protocol)

- Defined by IEEE 802.1s standard.
- Compatible with STP/RSTP; provides rapid convergence and load balancing.
- MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other.

> **region:** is a subsection of a network that operates its own MSTP, functioning as a singular switch externally.

> **spanning tree:** is a loop-free network path architecture ensuring a single active route between devices to prevent network issues.

1.5.4.1 Key Concepts

- **MSTIs:** Multiple spanning trees that are independent within different regions.
- **VLAN Mapping:** Multiple VLANs can share a single spanning tree within an MST instance.

1.5.5 Network Optimization Techniques

1.5.5.1 iStack Networking

`iStack` technology enables stacking switches to function as a single logical device, simplifying network management and enhancing performance.

Example

Merging individual light switches into a single master switch for ease of control.

1.5.5.2 Smart Link

`Smart Link` is designed for dual-uplink networks, providing fast failover without the need for STP by having one active and one standby link.

> Smart Link does not involve **protocol packet exchange**

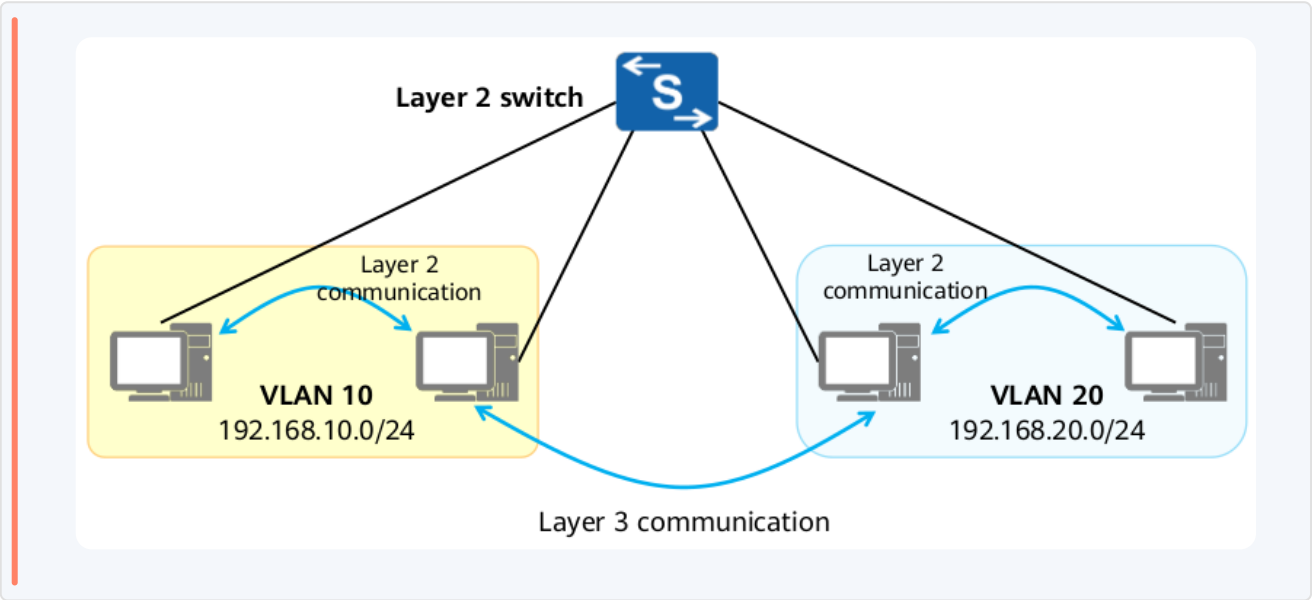
Inter-VLAN Communication

1 Inter-VLAN Communication

1.1 Background

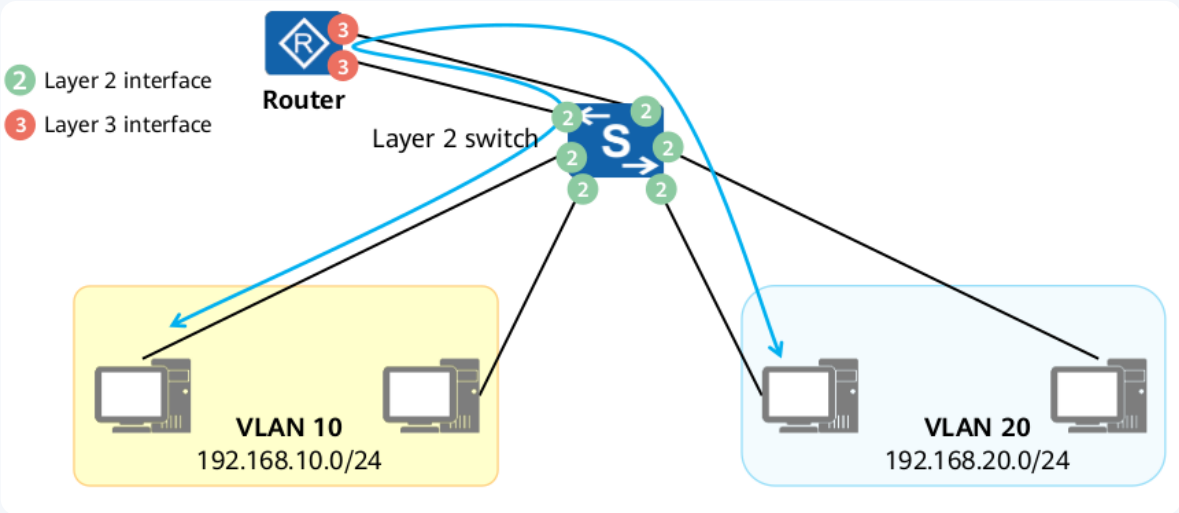
1.1.1 Layer 2 Communication

- Devices within the same VLAN and IP segment can communicate directly.
- This is called **Layer 2 communication** because it operates on the data link layer of the OSI model.
- No Layer 3 devices (routers) are required for this communication.



1.1.2 Layer 3 Communication (Inter-VLAN)

- Inter-VLAN communication requires crossing between different network segments.
- This necessitates the use of **Layer 3 devices** for routing packets between VLANs.
- **Common Layer 3 devices:** routers, Layer 3 switches, firewalls, etc.



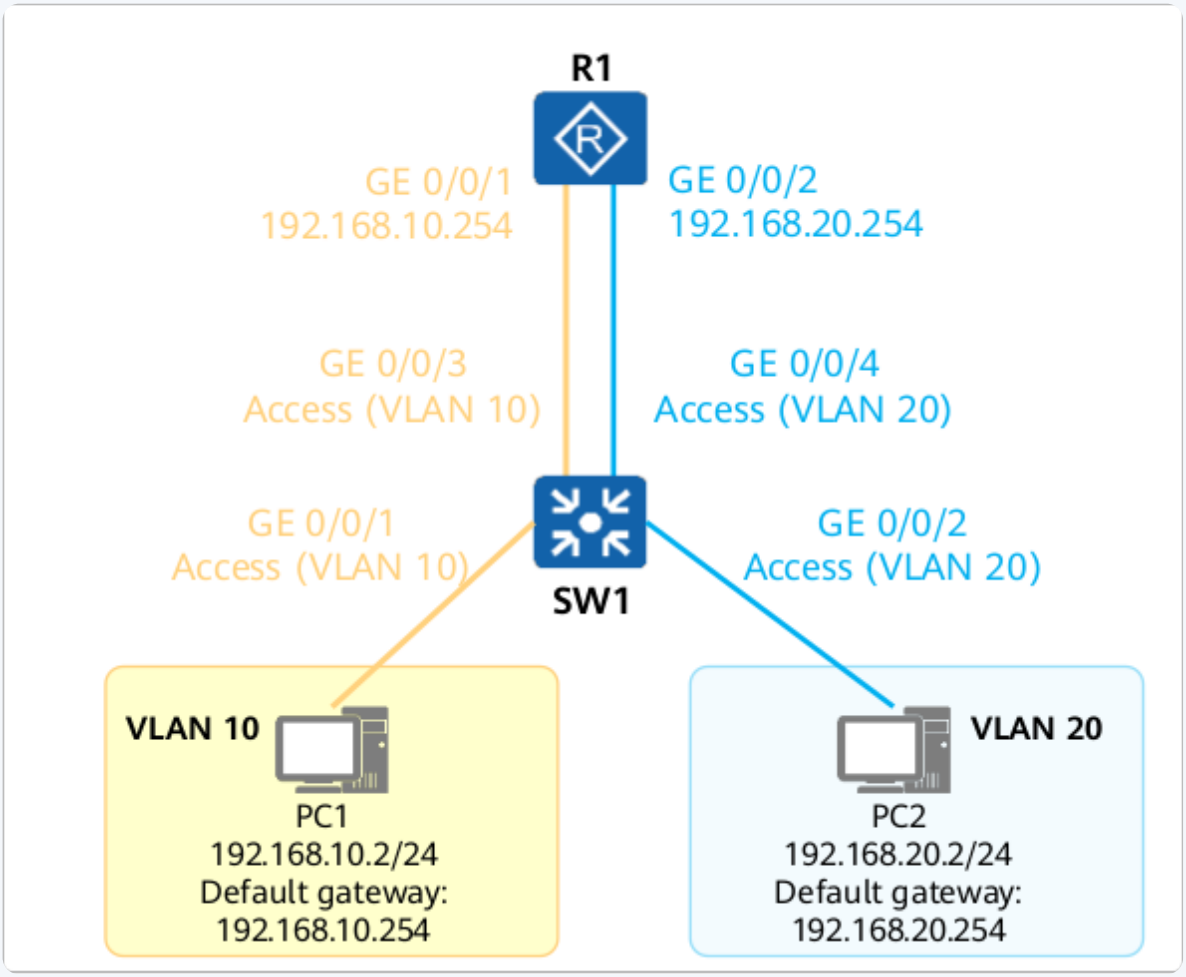
1.2 Using Routers' Physical Interfaces or Sub-interfaces to Implement Inter-VLAN Communication

1.2.1 Physical Interface Overview

Routers use physical interfaces to connect to different network segments and act as gateways. Each interface has its own IP address to manage traffic for specific VLANs. However, scalability is limited since one physical interface handles only one VLAN.

> The Layer 3 interfaces of the router cannot process data frames with VLAN tags. Therefore, the interfaces of the switch connected to the router

must be set to the access type.



Example

- R1 GE 0/0/1: `192.168.10.254` (VLAN 10)
- R1 GE 0/0/2: `192.168.20.254` (VLAN 20)

1.2.2 Sub-interface Overview

Sub-interfaces allow a single physical interface to manage multiple VLANs by using VLAN tags. They are Virtual interfaces that can perform Layer 3 forwarding and process tagged frames.

- **Benefits**:
  - Increased scalability

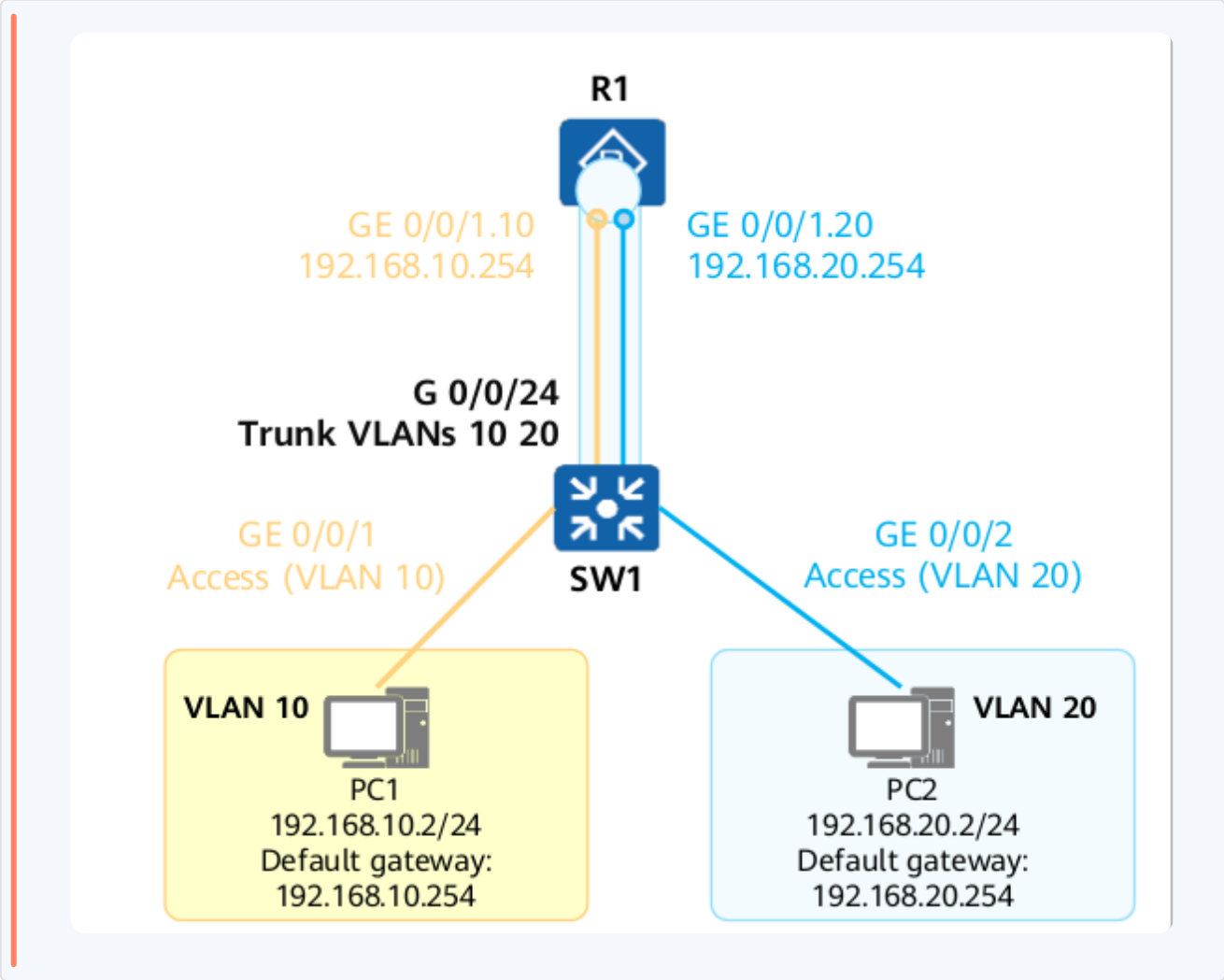
- Efficient use of physical interfaces

1.2.2.1 Sub-interface Processing Steps

---

1. Connect router's physical interface to switch's trunk port.
2. Router forwards packets based on VLAN tags to appropriate sub-interface.

> - VLANs use tagging to distinguish frames on a trunk port, typically using IEEE 802.1Q to add VLAN ID and priority information to Ethernet frame headers.
> - Routers use sub-interfaces for each VLAN and logically strip the VLAN tag to make routing decisions based on Layer 3 IP addresses.
> - Routers retag frames with new VLAN IDs if they need to be sent back into a VLAN-enabled network segment after Layer 3 processing.



1.2.2.2 Configuring Sub-interfaces (Huawei CLI)

```markdown
[R1]interface <interface-type> <interface-number>.<sub-interface number>
[R1-GigabitEthernet0/0/1.1]dot1q termination vid <vid>
[R1-GigabitEthernet0/0/1.1]ip address <IP_ADDRESS> <SUBNET_MASK>
[R1-GigabitEthernet0/0/1.1]arp broadcast <option>
```

- **Sub-interface number:** number/VLAN ID.
- **vid:** Set the VLAN ID for tag termination.
- **option:** set ARP broadcast if needed.

> `dot1q termination vid <vid>` : This command applies the IEEE 802.1Q standard to terminate VLAN traffic from a trunk link, associating it with a specified VLAN ID on that subinterface.

> `arp broadcast <option>` : disable/enable ARP broadcasting on the sub-interface, typically used when a host initiates communication without knowing its gateway's MAC address

1.2.3 Key Points Table

Feature	Physical Interface	Sub-interface
Layer	Layer 3	Layer 3
VLAN Support	One per interface	Multiple with tagging
Scalability	Poor (limited by number of interfaces)	Good (multiple sub-interfaces per physical port)
Tag Processing	Cannot process tagged frames	Can terminate and add tags

1.3 Using VLANIF Interfaces to Implement Inter-VLAN Communication

---

1.3.1 Overview

- A **Layer 2 switch** provides **only Layer 2 switching functions**.
- A **Layer 3 switch** combines Layer 2 switching with **routing functions** through VLANIF interfaces.

1.3.1.1 VLANIF Interface

> A VLANIF interface is a virtual Layer 3 interface used for inter-VLAN routing. It can add or remove VLAN tags to facilitate communication between different VLANs.

> A frame arriving at a switch is tagged for a VLAN, routed via the VLANIF interface, decapsulated, re-encapsulated with a new VLAN tag after IP examination since routing module dont support Vlan and its workd with ip address, and sent to the destination VLAN.

> each VLANIF interface is associated with one specific VLAN ID.

1.3.2 Configuration Example

1.3.2.1 Basic Configurations

Markdown

```
[SW1]interface Vlanif <vid>
[SW1-Vlanif10]ip address <ip address> <mask>
```

> The IP address of a VLANIF interface is used as the gateway IP address

1.3.2.2 Step by Step Explanation

---

1. PC determines if destination is on the same network segment.
2. Packet sent to switch's routing module based on MAC address.
3. Routing module performs L3 forwarding decision based on routing table.
4. Switch obtains destination MAC from ARP table and sends to switching module.

5. Switching module determines outbound interface and whether the frame needs a VLAN tag.

1.4 Layer 3 Communication Process

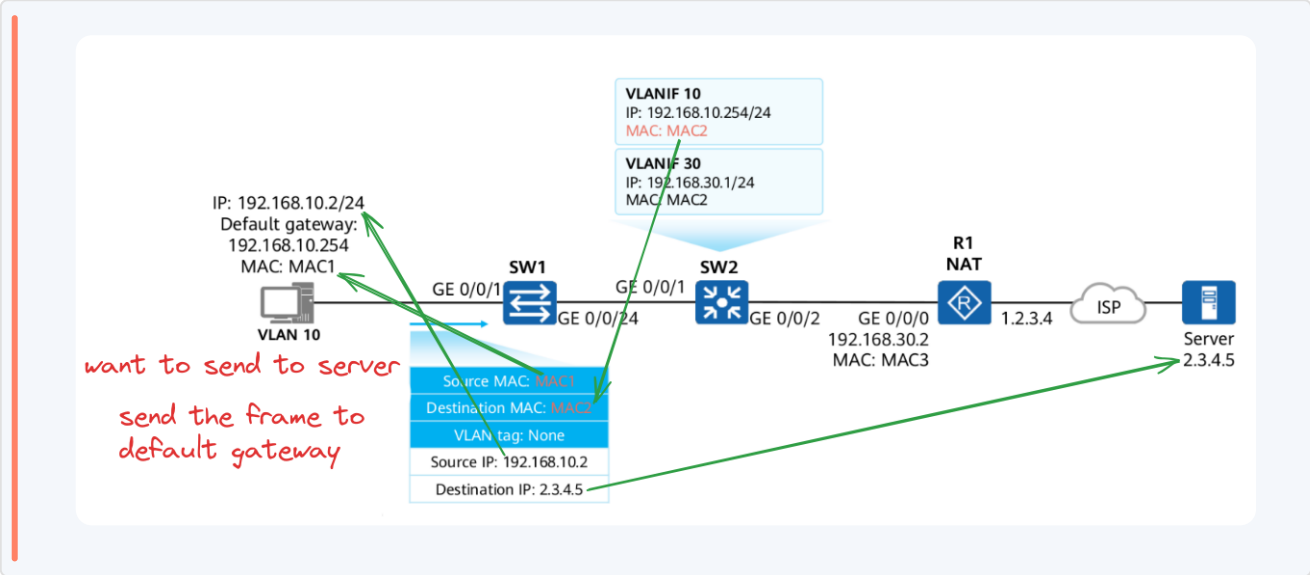
1.4.1 Communication Process from PC1 to Server

1.4.1.1 Step by Step Process:

1.4.1.1.1 Step 1:

PC Processing:

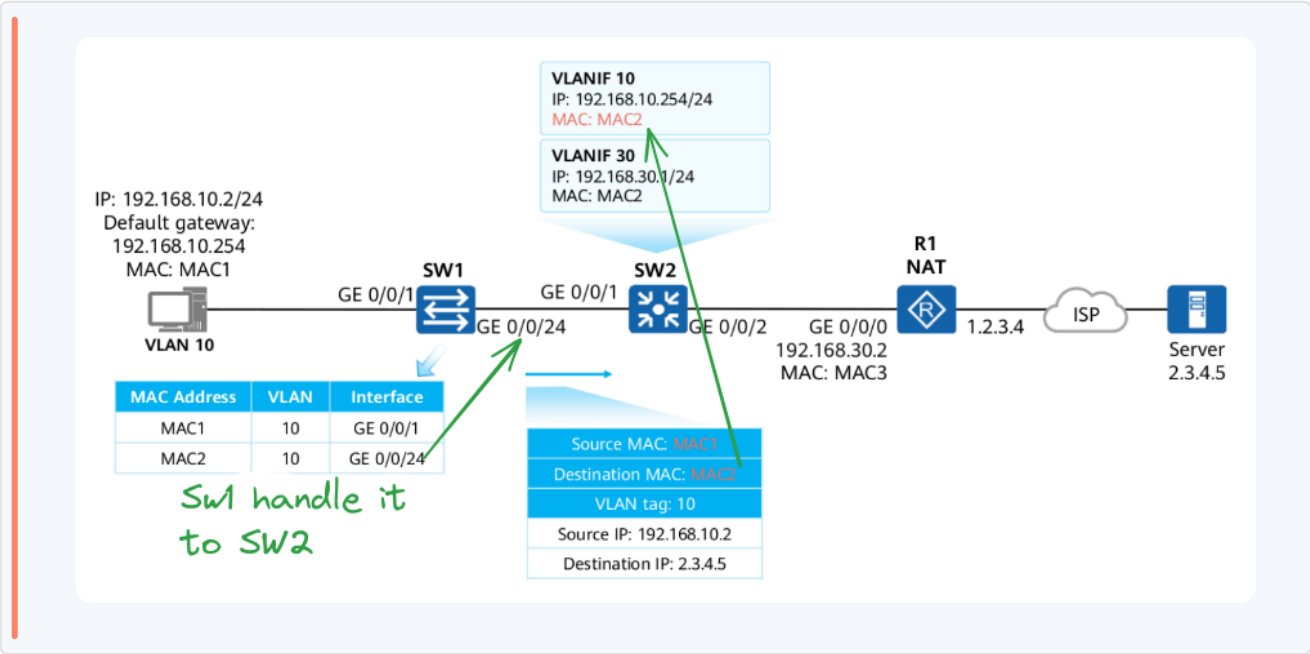
- PC checks if destination IP is local.
- Sends packet to its default gateway if not local.



1.4.1.1.2 Step 2:

SW Processing:

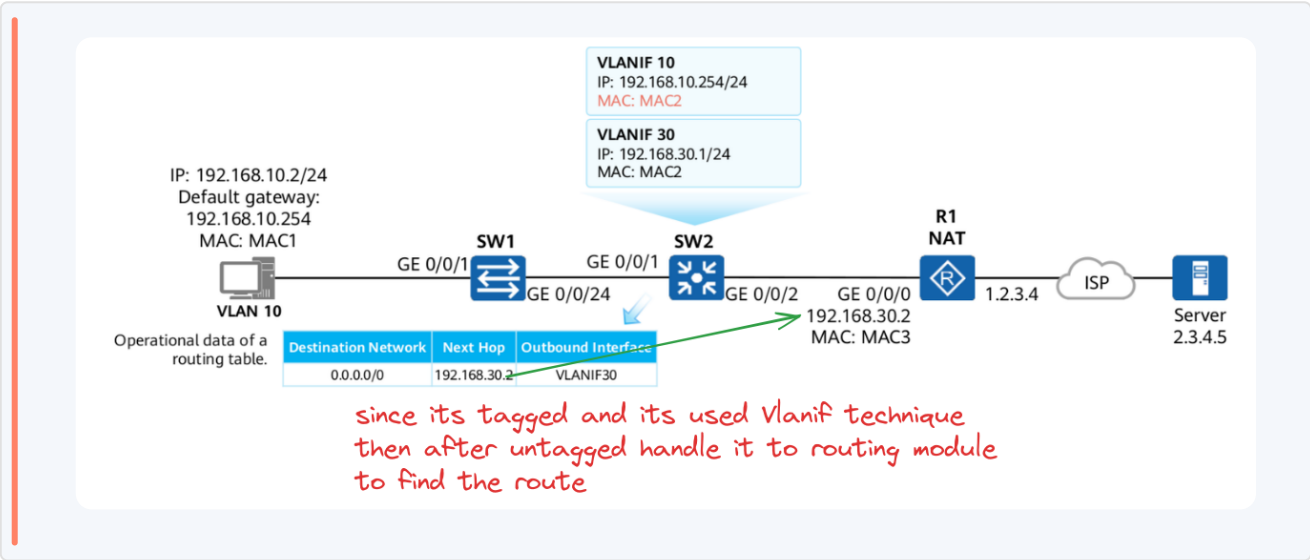
- Looks up MAC address table.
- Forwards frame based on destination MAC.



1.4.1.1.3 Step 3:

Routing Module Processing at SW:

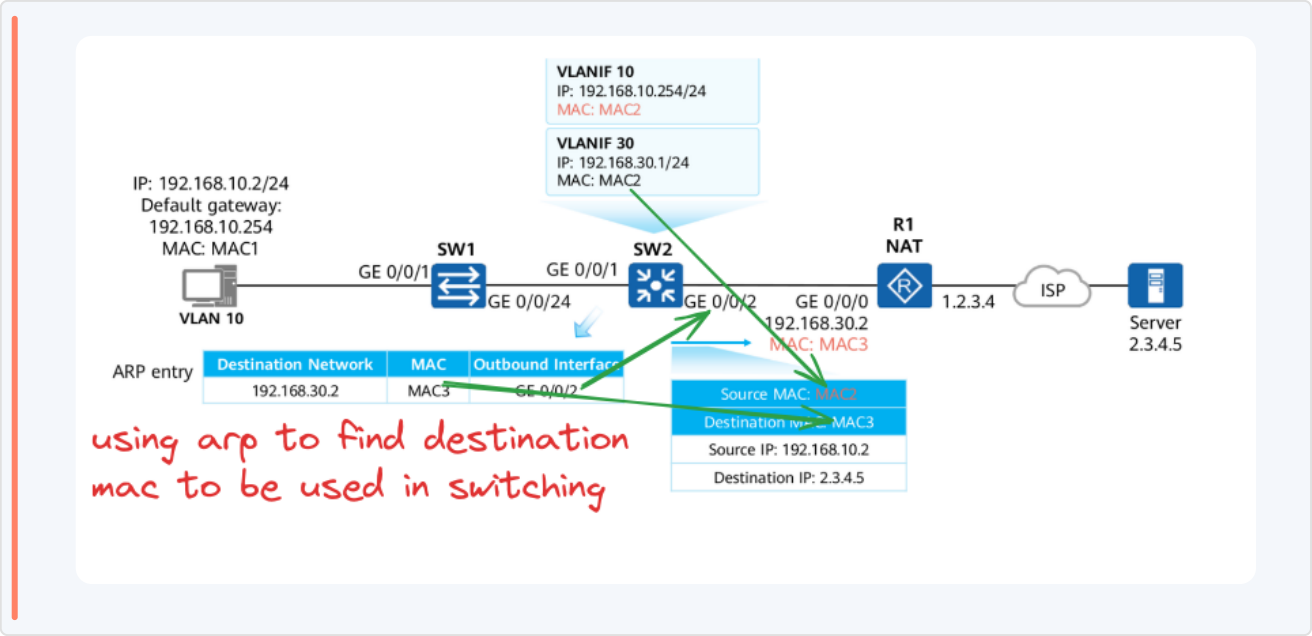
- Receives frame meant for another network.
- Checks routing table, forwards to next hop.



1.4.1.1.4 Step 4:

SW Processing:

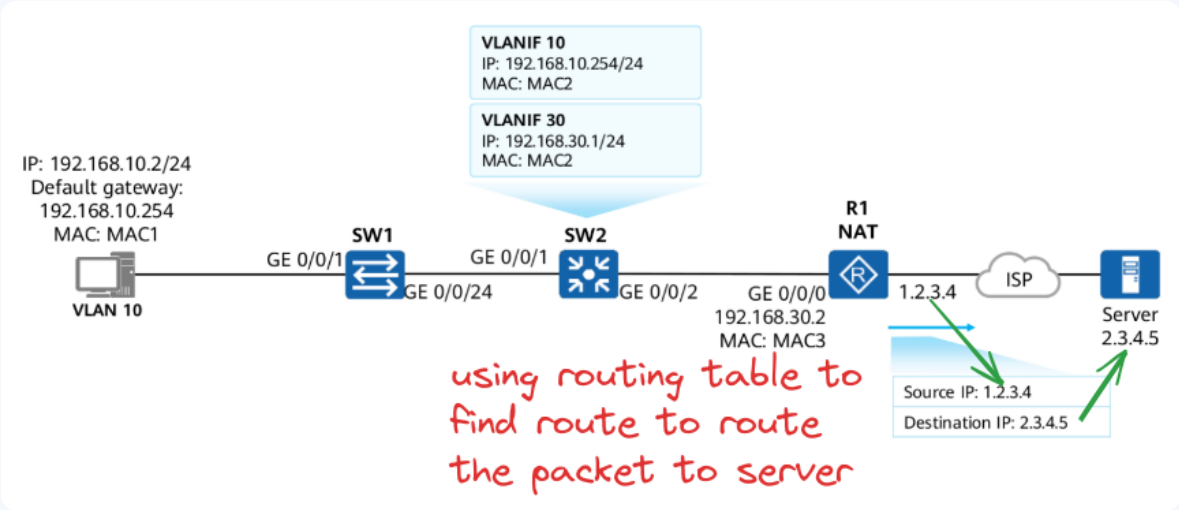
- After finding the MAC address switch Prepares Packet for Outbound interface



1.4.1.1.5 Step5:

R Router NAT Processing:

- Checks the destination IP address and finds that it is not a local IP address.
- Searches the routing table, finds a default matching route, and forwards the packet
- Performs NAT on packets leaving intranet.



1.4.2 Comparison between Layer 2 and Layer 3 interfaces

Aspect	Layer 2 Interface	Layer 3 Interface
IP Address Configuration	Cannot be assigned an IP address.	Can be assigned an IP address.
MAC Address Presence	Doesn't have a MAC address.	Has a MAC address.
Data Handling	Uses MAC table to forward or flood frames.	Uses routing table to forward packets or discards them.
Typical Devices	Found on Layer 2 switches.	Found on routers and Layer 3 switches.
Broadcast Domain Isolation	Does not isolate; floods broadcasts.	Isolates; terminates broadcasts without flooding.

> In Huawei networking devices, physical interfaces with IP addresses also have MAC addresses for Layer 2 communication, except for logical or virtual interfaces like loopbacks or tunnels that don't handle Ethernet frames.

Eth-Trunk, iStack, and CSS

1 Eth-Trunk, iStack, and CSS

1.1 Network Reliability Requirements

1.1.1 Overview

- **Network reliability** ensures continuous network services Even with failures.
- Implemented at various levels: **card**, **device**, **link**.
- Essential due to the impact of Confusion on services and economics.

1.1.2 Card Reliability

1.1.2.1 Modular Switch Components

- **Chassis**: Slots for cards and modules for inter-card communication.

- **Power Module**: Supplies power to the device.
- **Fan Module**: Dissipates heat within the device.
- **Main Processing Unit (MPU)**: Manages control plane and management plane.

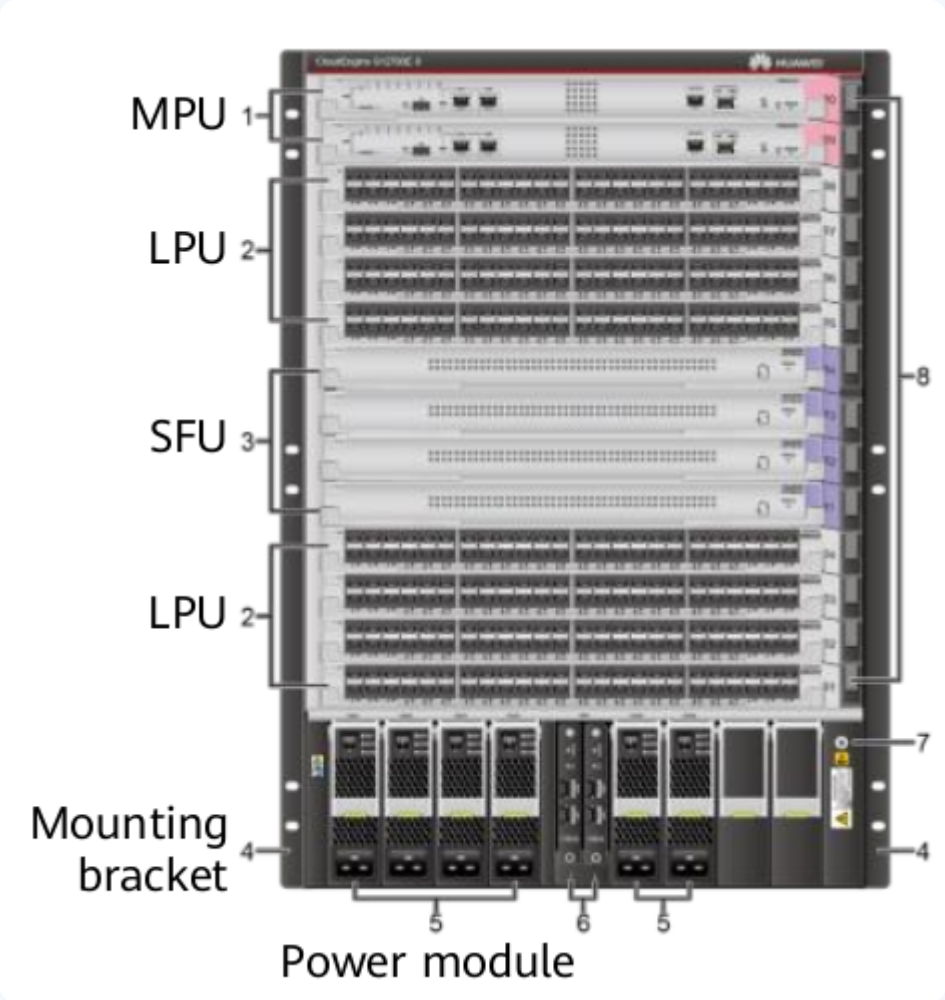
> **Control Plane:** Handles the network routing decisions, determining how data packets should flow through the network.

> **Management Plane:** Involves tasks related to administering the network, such as configuration, maintenance, and monitoring.

- **Switch Fabric Unit (SFU)**: Handles data plane with high-speed data channels.

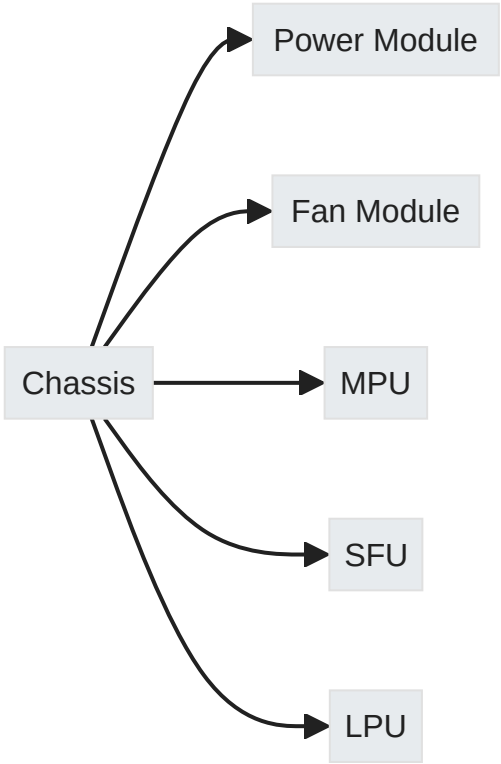
> **data plane:** is the part of a network that carries user traffic from one point to another.

- **Line Processing Unit (LPU)**: Provides data forwarding and physical interfaces.



1.1.2.2 Fault Tolerance

> The failure of a single MPU or SFU does not Stop the switch's operation. Faulty LPUs affect only their own interfaces.

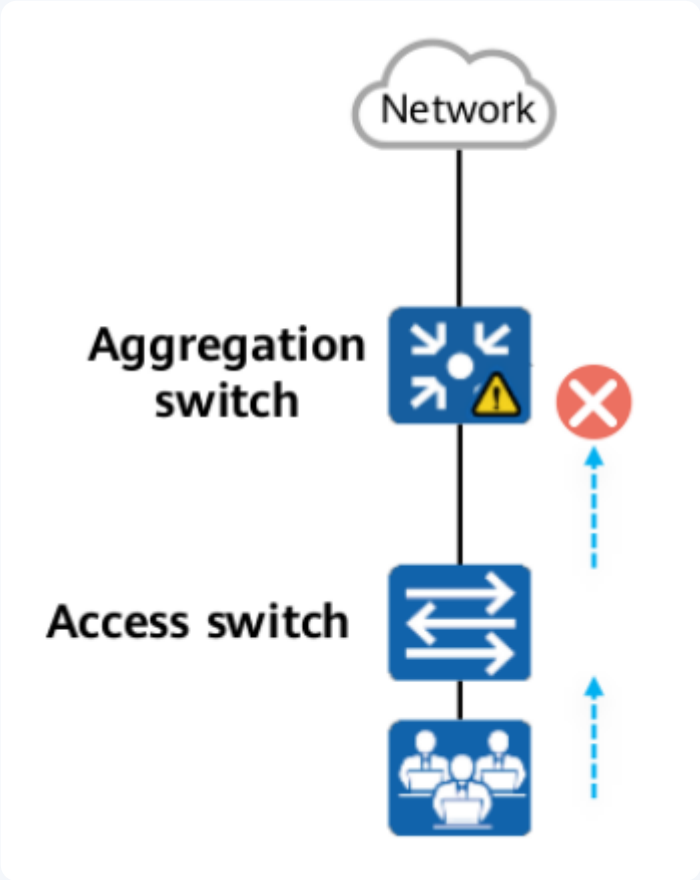


1.1.3 Device Reliability

1.1.3.1 Redundancy Modes

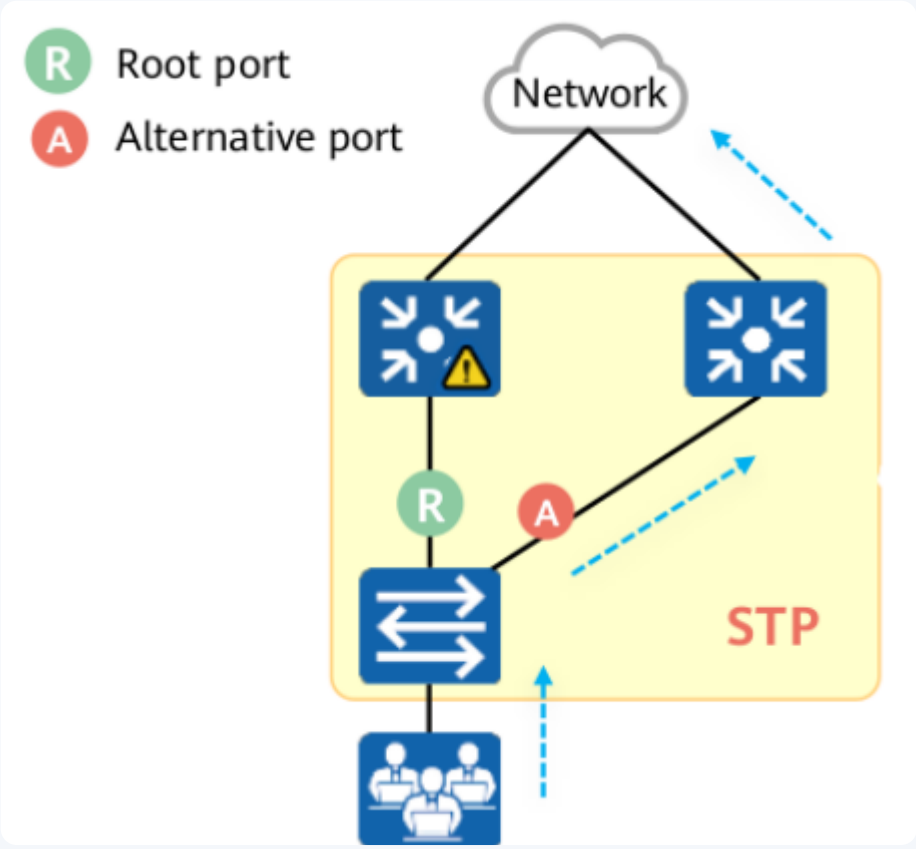
1.1.3.1.1 No Backup Mode

- If upstream fails, all downstream networks are interrupted.



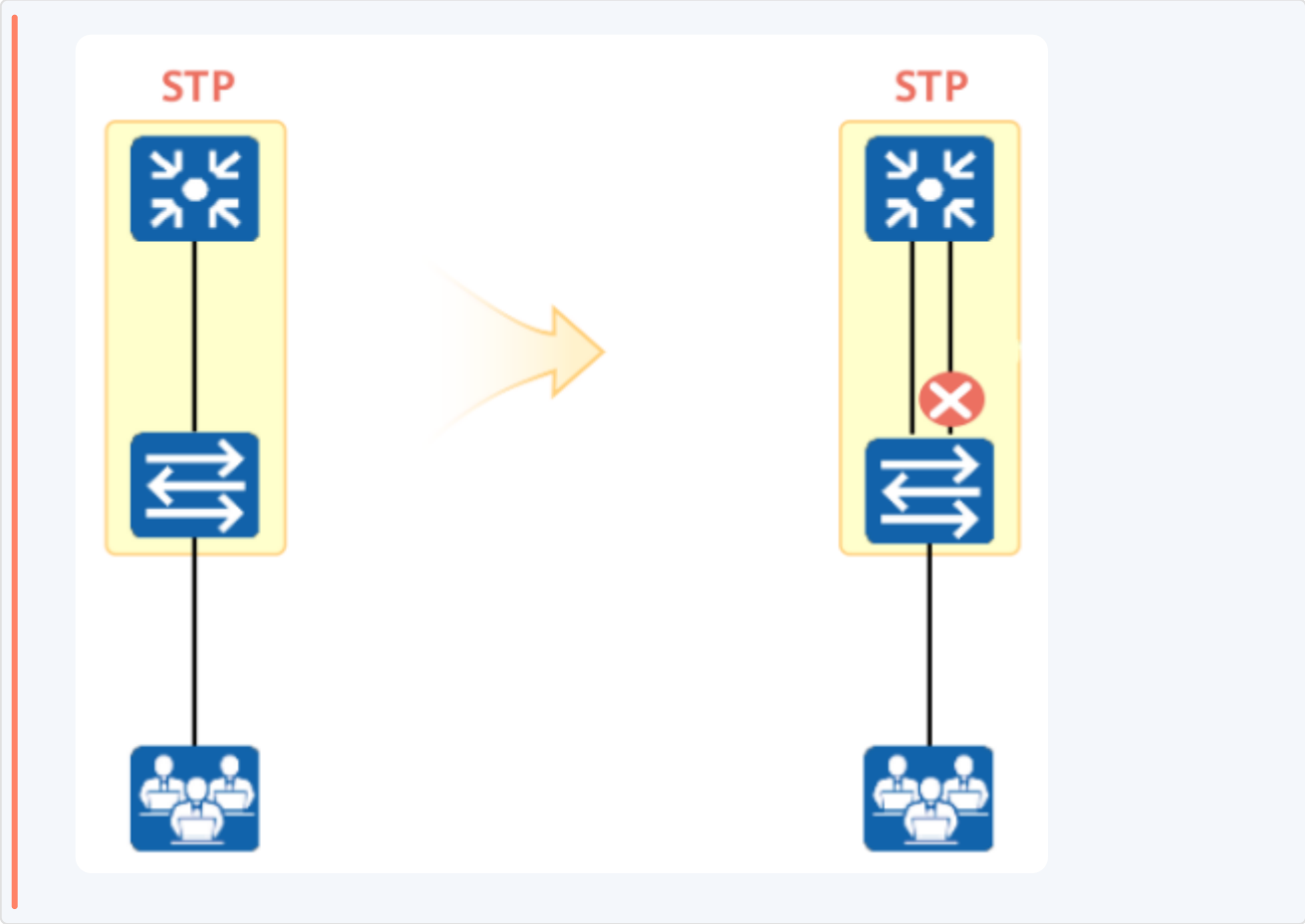
1.1.3.1.2 Master/Backup Mode (Dual-Homing)

- Alternative port takes over if root port fails. Ensures continuity.



1.1.4 Link Reliability

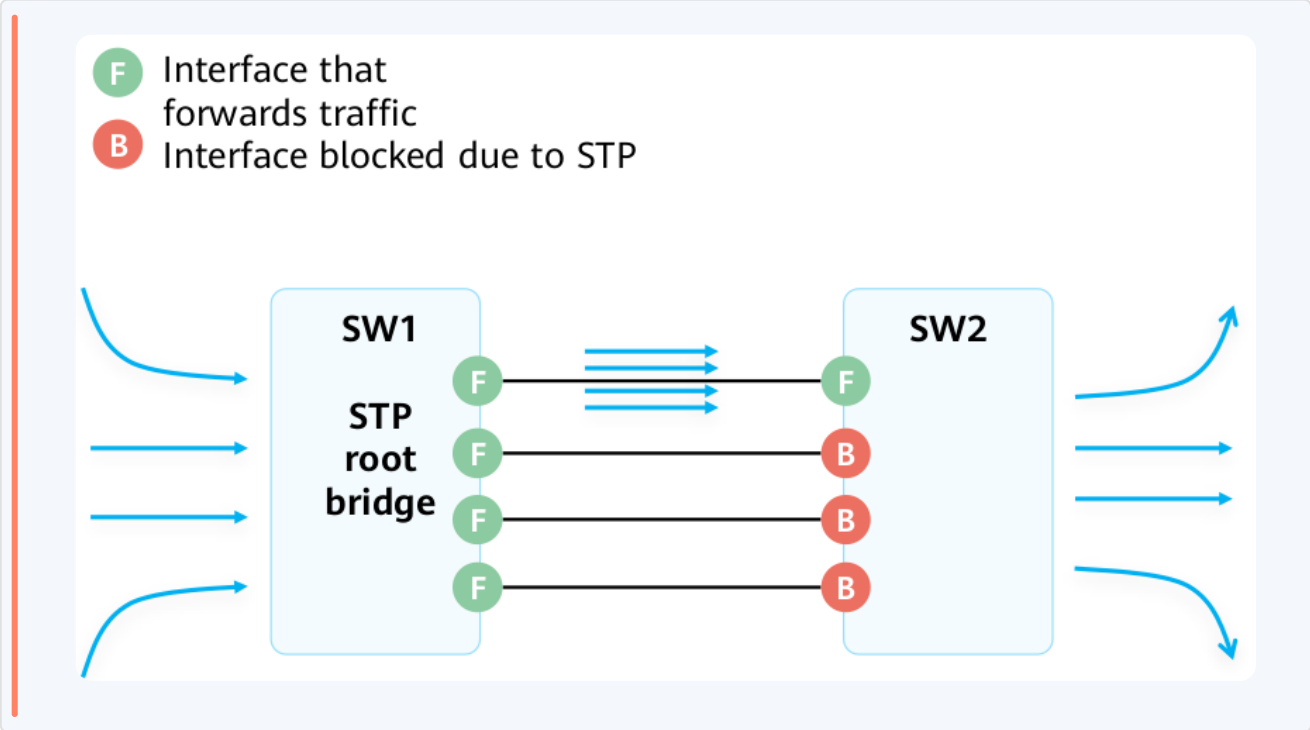
- STP blocks additional links to prevent loops; these serve as backups.



1.2 Principle and Configuration of Link Aggregation

1.2.1 Principle

1.2.1.1 Increasing Link Bandwidth

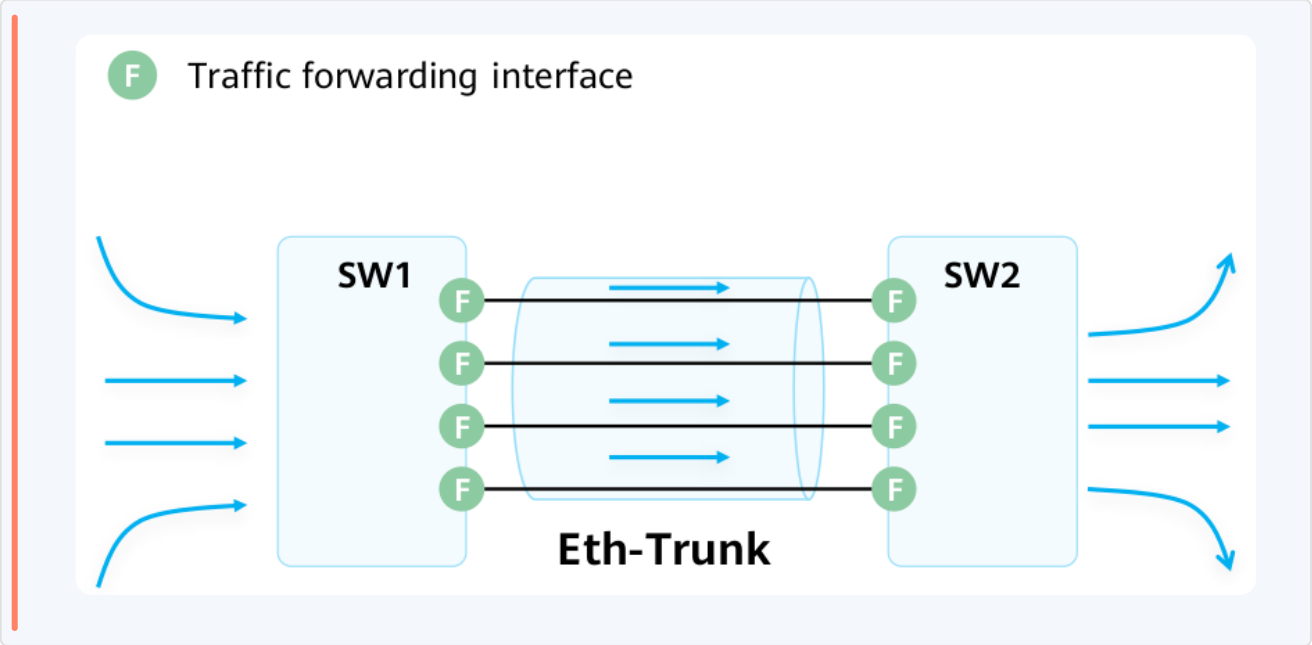


Note

With STP, only one link is active for forwarding traffic. Other links are in a blocking state.

1.2.1.2 Eth-Trunk (Ethernet Link Aggregation)

- Combines multiple physical links into a single logical link.
- Increases total link bandwidth without hardware upgrades.



1.2.1.2.1 Basic Concepts of Eth-Trunk

1.2.1.2.1.1 LAG (Link Aggregation Group)

- A logical interface created from multiple physical links.
- Known as an LAG interface or Eth-Trunk interface.

1.2.1.2.1.2 Member Interface and Member Link

- **Member interfaces:** Physical interfaces within an Eth-Trunk.
- **Member links:** actual physical connections.

1.2.1.2.1.3 Active vs Inactive Interfaces/Links

- **Active Interface/Link**: Selected for data forwarding.
- **Inactive Interface/Link**: Not selected for data forwarding.

1.2.1.2.1.4 Link Aggregation Modes

Mode	Description
Manual	No LACP; manual configuration required.
LACP	Uses LACP protocol for dynamic configuration.

> LACP (Link Aggregation Control Protocol) **automatically** manages the bundling of multiple network connections, while Manual mode requires the user to configure and manage these connections **without any protocol assistance.**

1.2.1.2.1.5 Configuration Consistency in Eth-Trunk

> ⚠ **Warning**
>
> **All member interfaces must have consistent parameters:**
>
> - Interface rate (speed)
> - Duplex mode (full/half duplex)
> - VLAN configurations (access/trunk/hybrid type, allowed/default VLANs)

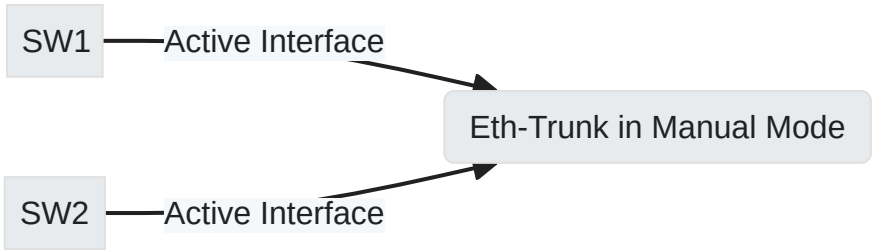
1.2.1.2.1.6 Advantages of Using Eth-Trunk

1. **Enhanced Throughput:** Combines bandwidth of individual links.
2. **Redundancy:** Provides link failover capabilities.
3. **Flexibility:** Allows addition or removal of links without disruption.

1.2.2 Manual Mode

1.2.2.1 Overview

- An Eth-Trunk is created **manually**, and member interfaces are added **without** using Link Aggregation Control Protocol (LACP).
- Typically used when one or both devices do not support LACP.
- Traffic is evenly shared across all active links.



> All links are active and forward data.

> Traffic is automatically rebalanced among remaining active links if a fault occurs.

Note

Manual mode requires precise Exact as no dynamic negotiation is done to confirm settings between devices.

Warning

Ensure all peer interfaces in an Eth-Trunk:

- Reside on the same device.
- Are added to the same Eth-Trunk.

1.2.2.1.1 Physical Layer Status Only

The device only uses physical layer status to determine interface health; it cannot detect higher-level faults.

1.2.3 LACP Mode

1.2.3.1 Overview

LACP facilitates automatic creation of Eth-Trunks by exchanging LACPDUs between devices.

1.2.3.1.1 Key Terms

- **LACPDU**: A protocol data unit used by LACP to carry information like device priority, MAC address, interface priority, and interface number.
- **Actor**: The participating device in an Eth-Trunk with lowest priority based on system priority or MAC address when priorities are equal.

> **Participating:** refer to helps coordinate which links are used and how data traffic is split across them.

1.2.3.2 Priorities and Election Process

1.2.3.2.1 Device Priority

- Election by lowest system priority.

> Default system priority: `32768` .

1.2.3.2.2 Interface Priority

- Election by lowest interface priority values.

> Default interface priority: `32768` .

1.2.3.2.3 Active Link Election

---

1. Devices exchange LACPDUs To Compare priority to elect actor.
2. Actor is determined based on lowest system priority or MAC address if priorities are equal.
3. Actor selects active interfaces based on lowest interface numbers when priorities are equal.
4. The actor informs the peer about the chosen active interface so that the peer can configure its interfaces to match.

Callout

Flags used in an LACPDU to identify active interfaces:

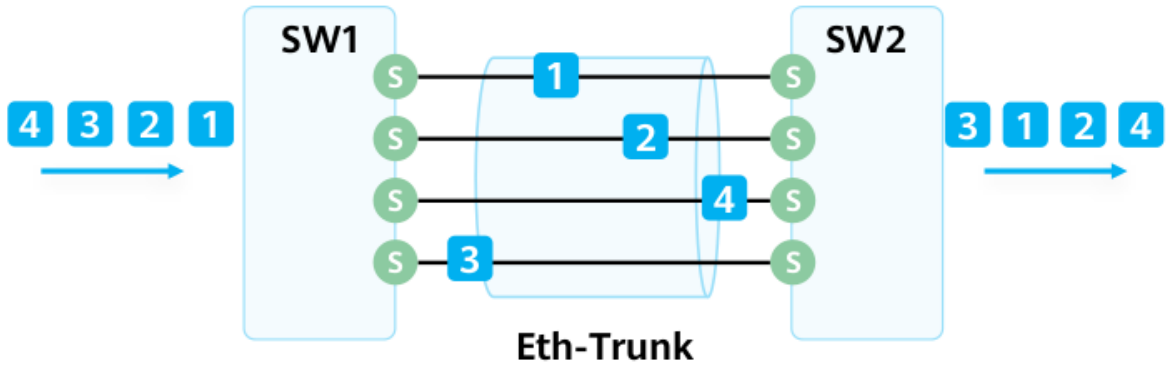
- Synchronization (`1` for active)
- Collecting (`1` for active)
- Distributing (`1` for active)

if flags set to `0` then the interface is inactive

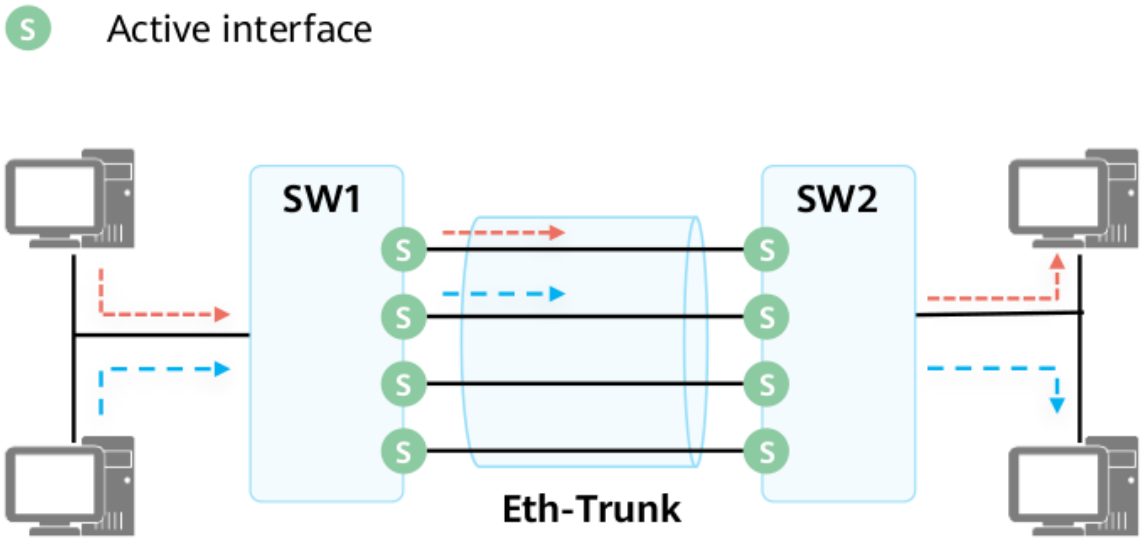
1.2.3.3 Load Balancing

1.2.3.3.1 Strategies

- **Per-packet:** Can cause out-of-order packets due to different transmission times across links.



- **Per-flow:** Ensures frames from the same flow are transmitted over the same physical link for order Uniformity.

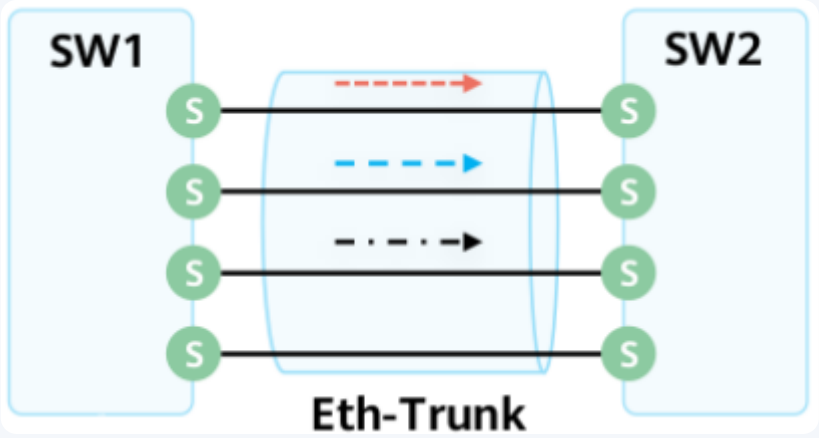


1.2.3.3.2 Load Balancing Modes

Configure load balancing modes based on traffic characteristics like IP or MAC addresses:

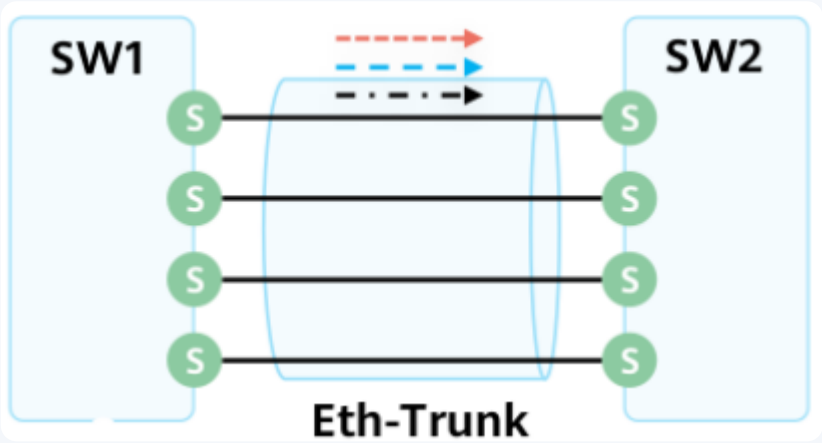
- **Proper load balancing algorithm:** IP-based load balancing algorithm that keeps the MAC addresses of the source and destination unchanged.

> Each packet may travel various links as the destination IP address typically changes.



- **Improper load balancing algorithm:** MAC-based load balancing algorithm that keeps the IP addresses of the source and destination unchanged.

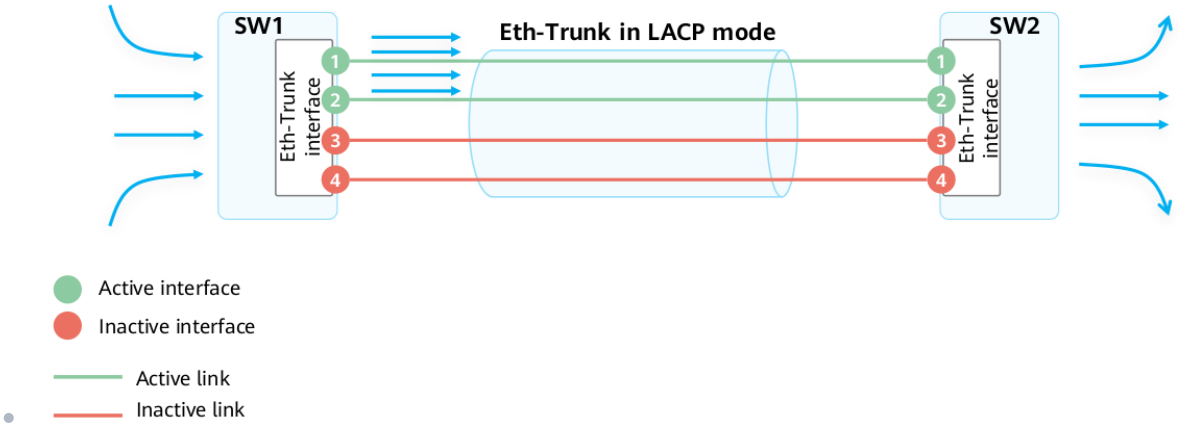
> Each packet might travel the same links, as the MAC address usually remains unchanged for a single hop towards the same destination.



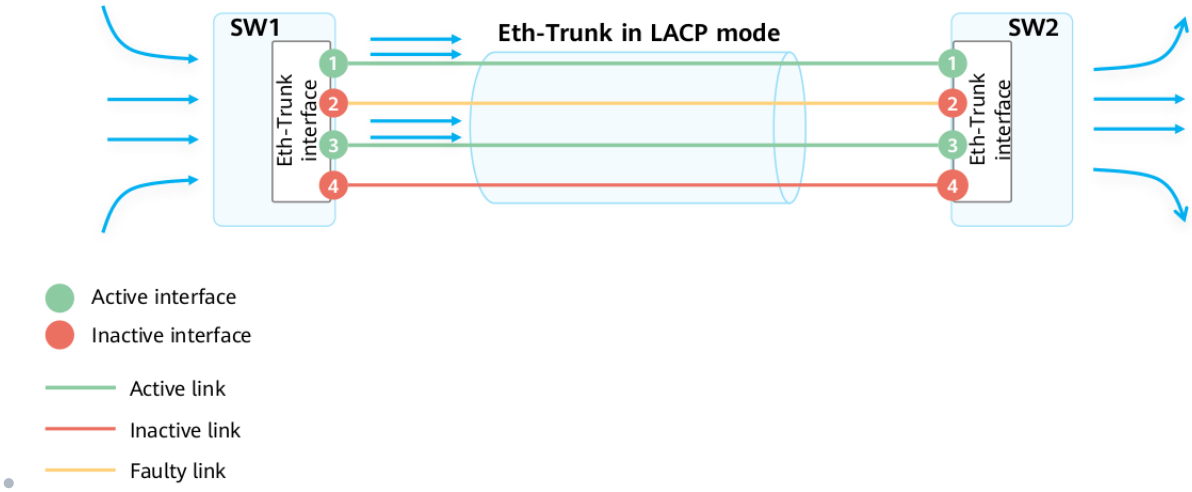
1.2.3.4 Maximum Number of Active Interfaces

You can configure a maximum number of active interfaces:

- Extra interfaces serve as backups (inactive).



- If an active link fails, Lowest-priority inactive link becomes active.



1.2.4 Typical Application Scenarios

1.2.4.1 Eth-Trunk Applications

- Between Switches (Aggregation Layer)
- Between Switch and Server (Access Layer)
- Between a Switch and iStack (Stacking)
- Heartbeat Link of Firewalls in Hot Standby Mode

1.2.5 Configuration Example

1.2.5.1 Creating an Eth-Trunk

```markdown
[Huawei] interface eth-trunk <trunk-id>
```

1.2.5.2 Configuring Link Aggregation Mode

```markdown
[Huawei-Eth-Trunk1] mode <lacp> || <manual load-balance>
```

> Both ends of the Eth-Trunk must have the same aggregation mode configured.

1.2.5.3 Adding Interfaces to an Eth-Trunk

1.2.5.3.1 From Ethernet Interface View

```markdown
[Huawei-GigabitEthernet0/0/1] eth-trunk <trunk-id>
```

1.2.5.3.2 From Eth-Trunk View

```markdown
[Huawei-Eth-Trunk1] trunkport <interface-type>
<interface-number>
```

1.2.5.4 Mixed-Rate Link Configuration

```markdown
[Huawei-Eth-Trunk1] mixed-rate link <option>
```

- **option:** either enable or disable

> Allows interfaces with different rates to join the same Eth-Trunk (disabled by default).

1.2.5.5 LACP Configuration

1.2.5.5.1 System Priority

```markdown
[Huawei] lacp priority <priority>
```

> Default 32768.

1.2.5.5.2 Interface Priority within an Eth-Trunk

```markdown
[Huawei-GigabitEthernet0/0/1] lacp priority <priority>
```

> Must run this command after adding the interface to the Eth-Trunk.

> Default 32768.

1.2.5.6 Active Links Configuration

1.2.5.6.1 Maximum Number of Active Interfaces (`LACP Mode`)

Markdown

```
[Huawei-Eth-Trunk1] max active-linknumber <number>
```

> Configure equal values on both ends for maximum active links in LACP mode.

> Different switches have varying maximums for active interfaces

1.2.5.6.2 Minimum Number of Active Interfaces (`Manual & LACP Modes`)

Markdown

```
[Huawei-Eth-Trunk1] least active-linknumber <number>
```

1.3 Overview of iStack and CSS

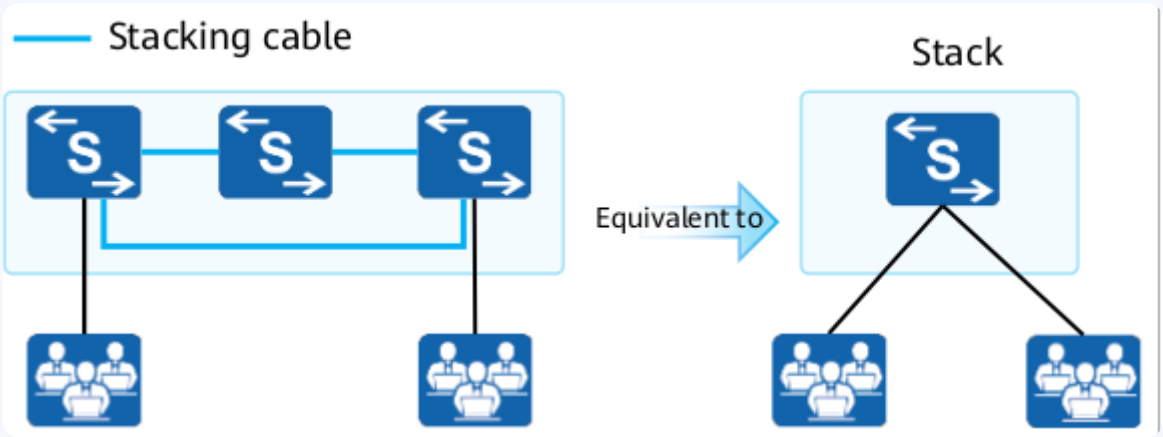
1.3.1 Key Terms

1.3.1.1 iStack

- **Definition**: A technology that allows multiple switches with iStack capabilities to be connected using stacking cables, forming a single logical switch for data forwarding.
- **Use Case**: Increases port density and uplink bandwidth; provides redundancy.

> Fixed switches support iStack.

> **Fixed switches:** network switches with a set number of ports and features that cannot be expanded by adding modules or cards.

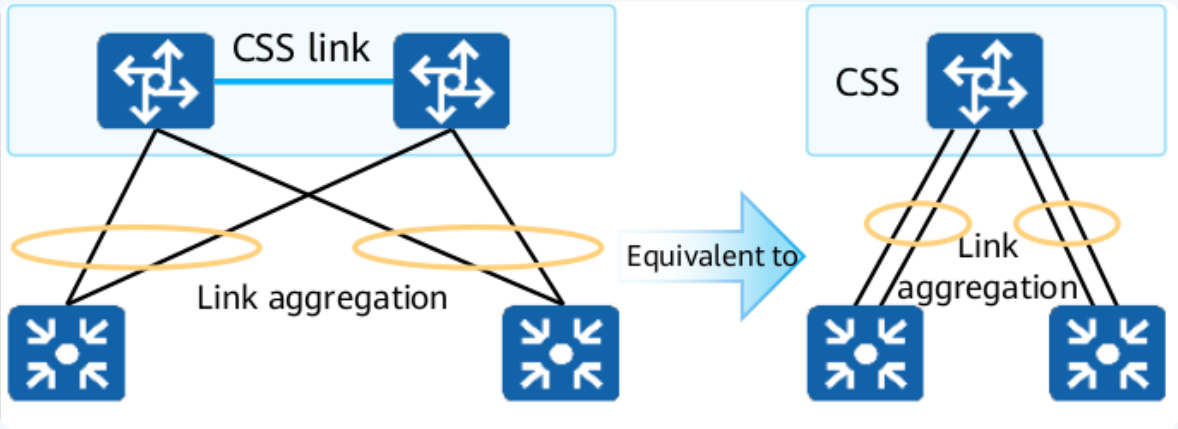


1.3.1.2 CSS (Cluster Switch System)

- **Definition**: A system where two CSS-capable switches are combined into one logical switch.
- **Use Case**: Simplifies network by eliminating the need for MSTP or VRRP; enhances network convergence and reliability.

modular switches support CSS

Modular switches: devices that can be customized with extra parts for different functions as your needs grow.



1.3.2 Advantages of iStack and CSS

Both technologies aim to simplify operations & management (O&M) while enhancing reliability by preventing single points of failure.

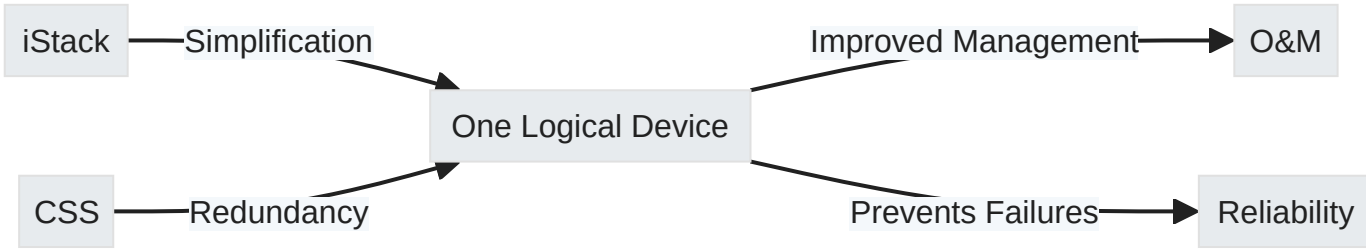
- **Many-to-one virtualization:** Switches can be virtualized into one logical switch (CSS) that has a unified control plane for unified management.
- **Unified forwarding plane:** Physical switches in a CSS use a unified forwarding plane, and share and synchronize forwarding information in real time.

The forwarding plane is the part of a network device responsible for moving packets to their destination based on pre-determined rules.

Tip

Control plane decides where packets should go while the forwarding plane actually moves the packets to their destination

- **Inter-device link aggregation:** Links between physical switches are aggregated into a single Eth-Trunk interface to interconnect with downstream devices.



1.3.3 Applications

1.3.3.1 Extending Bandwidth & Redundancy Backup

- **iStack**: Increases uplink bandwidth using multiple physical links in an Eth-Trunk, improving reliability.

1.3.3.2 Extending Port Quantity

- **iStack**: Adds new switches to increase the number of accessible ports when current port density is insufficient.

1.3.3.3 Simplified Network Configuration

- **CSS**: Forms a single logical device from two devices, streamlining network setup without MSTP or VRRP.

ACL Principles and Configuration

1 ACL Principles and Configuration

1.1 ACL Overview

1.1.1 Network Security and QoS

1.1.1.1 Key Issues

- Unauthorized access to enterprise key servers.
- Confidential information leakage.
- Internet viruses threatening intranet security.
- Random service traffic occupying bandwidth.
- Lowered user experience due to compromised QoS for delay-sensitive services.

1.1.1.2 Solution: Traffic Filtering

1.1.1.2.1 Access Control List (ACL) Overview

1.1.1.2.1.1 What is an ACL?

> An ACL is a set of sequential rules composed of permit or deny statements that matches and distinguishes packets based on predefined criteria.

1.1.1.2.1.2 Matching Criteria

- Source IP address
- Destination IP address
- Protocol type
- Source port number (TCP/UDP)
- Destination port number (TCP/UDP)

1.1.1.2.1.3 Applications of ACLs

Application	Description
Traffic Filter	Filters traffic as part of network security measures.
NAT	Used in Network Address Translation configurations.
Routing Policy	Influences route selection processes.
Firewall Policy	Part of defining firewall behaviors.
QoS	Improves Quality of Service by prioritizing traffic.

1.1.1.2.1.4 Importance of ACLs

> ACLs are crucial for identifying and controlling packets to manage network access behaviors, prevent attacks, and improve bandwidth

utilization.

1.2 Basic Concepts and Working Mechanism of ACLs

1.2.1 Composition of ACLs

- **ACL Number**: Unique identifier for each ACL.
- **Rule ID**: Identifier for each rule within an ACL; ranges from 0 to 4294967294.
- **Action**: Specifies whether to "permit" or "deny" matching packets.
- **Matching Option**: Criteria used to match packets (e.g., source IP address).

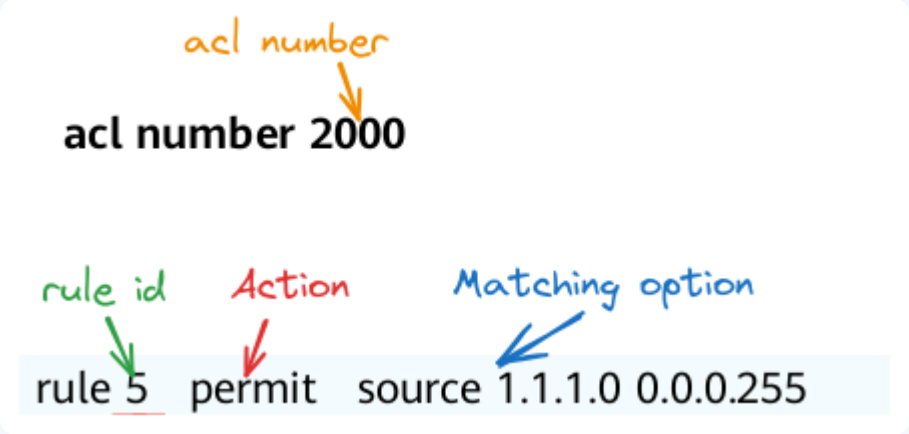
Rule IDs can be **manually** defined or **automatically** (The default step is 5 for increment between rules Therefore, rule IDs are 5, 10, 15, and so on.) allocated by the system.

When a new rule is manually defined added without a specified number, the computer assigns the next-highest number following an adjustable stepwise pattern, renumbering all rules accordingly if the step size changes.

Rule hidden at the end of the ACL:

```
rule 4294967294 deny
```

It acts as a last final option to deny access when all other rules have been checked and don't grant permission.



1.2.2 Classification of ACLs

Based on how rules are defined, we have different types of ACLs:

Basic	Source IP / fragmentation / time ranges	2000-2999
Advanced	More Criteria	3000-3999
Layer2	Ethernet Frame Header	4000-4999
UserDefined	Custom Headers/Strings	5000-5999
User	User Groups/IPs	6000-9999

More Criteria:

- source and destination IPv4 addresses.
- IPv4 protocol types.
- ICMP types.
- TCP source/destination port numbers.

- UDP source/destination port numbers.
- effective time ranges.

Ethernet frame headers:

- source and destination MAC addresses.
- Layer 2 protocol types.

Custom Headers/Strings:

- packet headers.
- offsets.
- character string masks.
- user-defined character strings.

Basic ACL

```
acl number 2000
 rule    5    deny    source  10.1.1.1  0
```

Advanced ACL

```
acl number 3000
 rule   5  permit  ip   source  10.1.1.0  0.0.0.255  destination  10.1.3.0  0.0.0.255
 rule  10  permit  tcp  source  10.1.2.0  0.0.0.255  destination  10.1.3.0  0.0.0.255  destination-port eq 21
```

1.2.2.1 Identification Methods

There are two ways to identify an ACL: by number or by name. Named ACLs are easier to remember and manage.

1.2.3 Matching Rules in ACLs

1.2.3.1 Wildcards

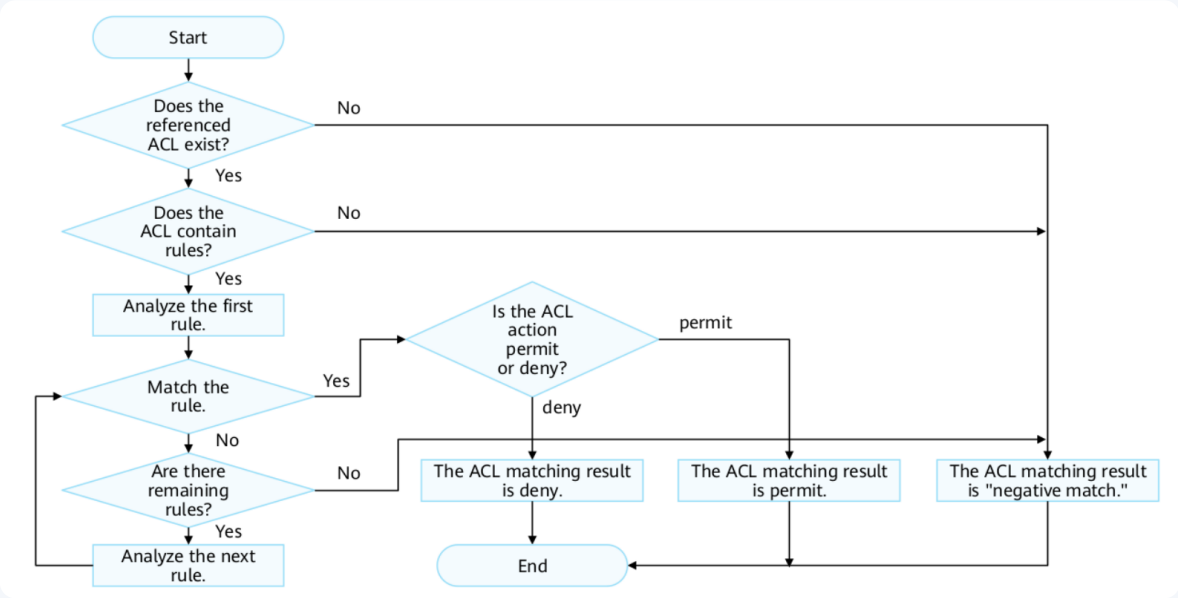
Wildcards determine which bits in an IP address must match exactly (`0`) and which bits can vary (`1`).

> A wildcard is a 32-bit number.

> A wildcard is usually expressed in dotted decimal notation.

> IP Address: 192.168.100.0
> Wildcard mask: 0 . 0 . 0 .255
>
> its mean 192.168.100 must match and for last part is from 1 -255
>
> IP Address: 192.168.100.1
> Wildcard mask: 0 . 0 . 0 .0
>
> its mean 192.168.100.1 must match
>
> IP Address: 0.0.0.0
> Wildcard mask: 255.255.255.255
>
> its mean any address

1.2.3.2 Matching Order & Result

> 
>

- ACL matching checks packets against rules sequentially.

- Stops at first match, performs action (permit/deny), no further checks.
- No ACL or no rules results in negative match.
- Matches are either positive (permit or deny) or negative.

ACL rules are processed in ascending order of their Rule IDs until a match is found.

Rule ID	Action	Source	Description
1	permit	192.168.1.1/32	Permits only from 192.168.1.1
2	permit	192.168.1.2/32	Permits only from 192.168.1.2
3	deny	192.168.1.3/32	Denies from 192.168.1.3

> The first matching rule determines the action taken; subsequent rules are ignored.

Note

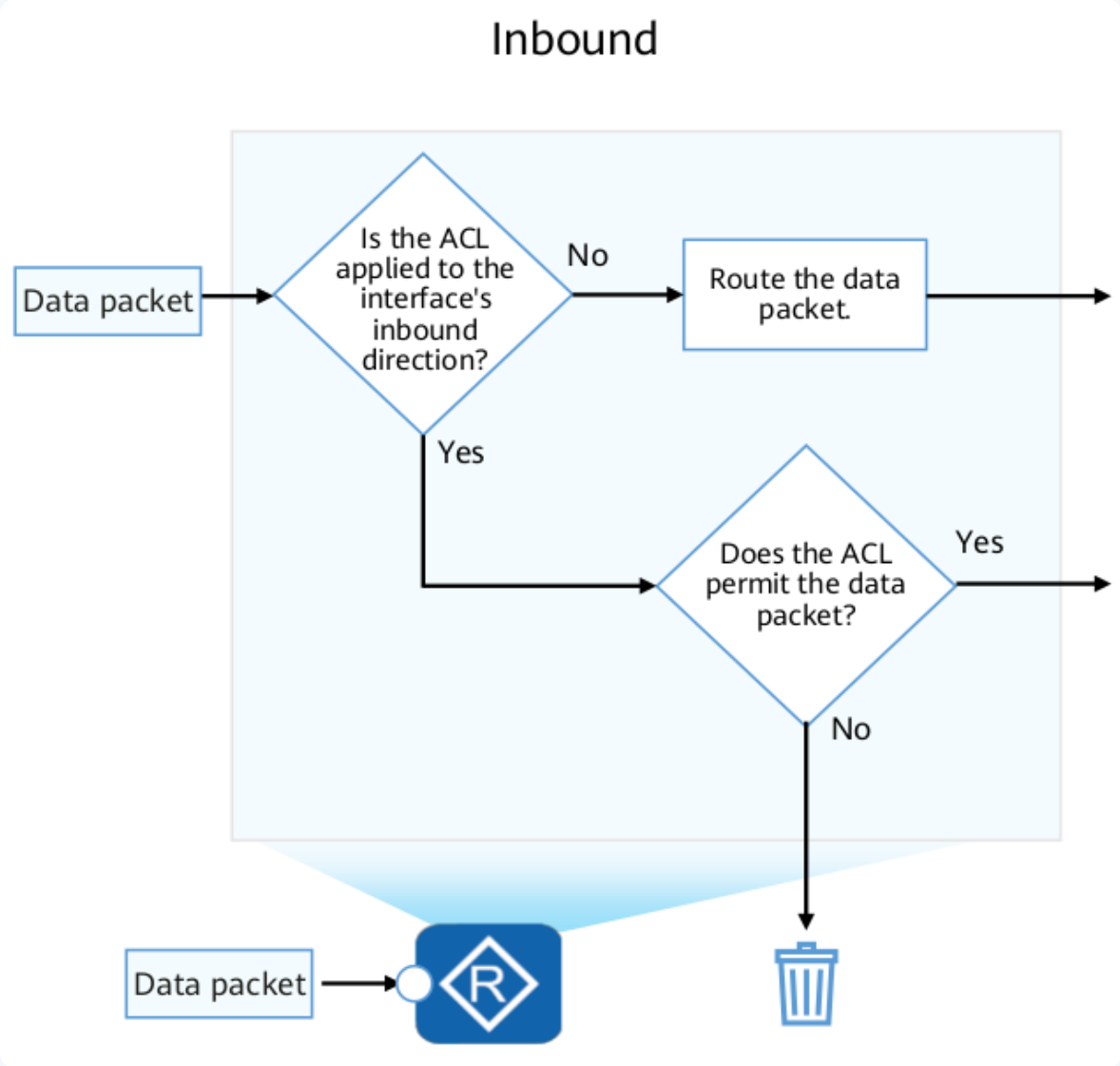
Huawei devices have two ways to decide which rule gets applied first when filtering network traffic:

- **auto:** automatically prioritizes network traffic rules by placing more specific instructions higher on the list for accurate traffic management.
- **config:** The device checks network traffic against the rules starting from the one with the lowest ID number and moving upwards. By default, this is how rules are matched.

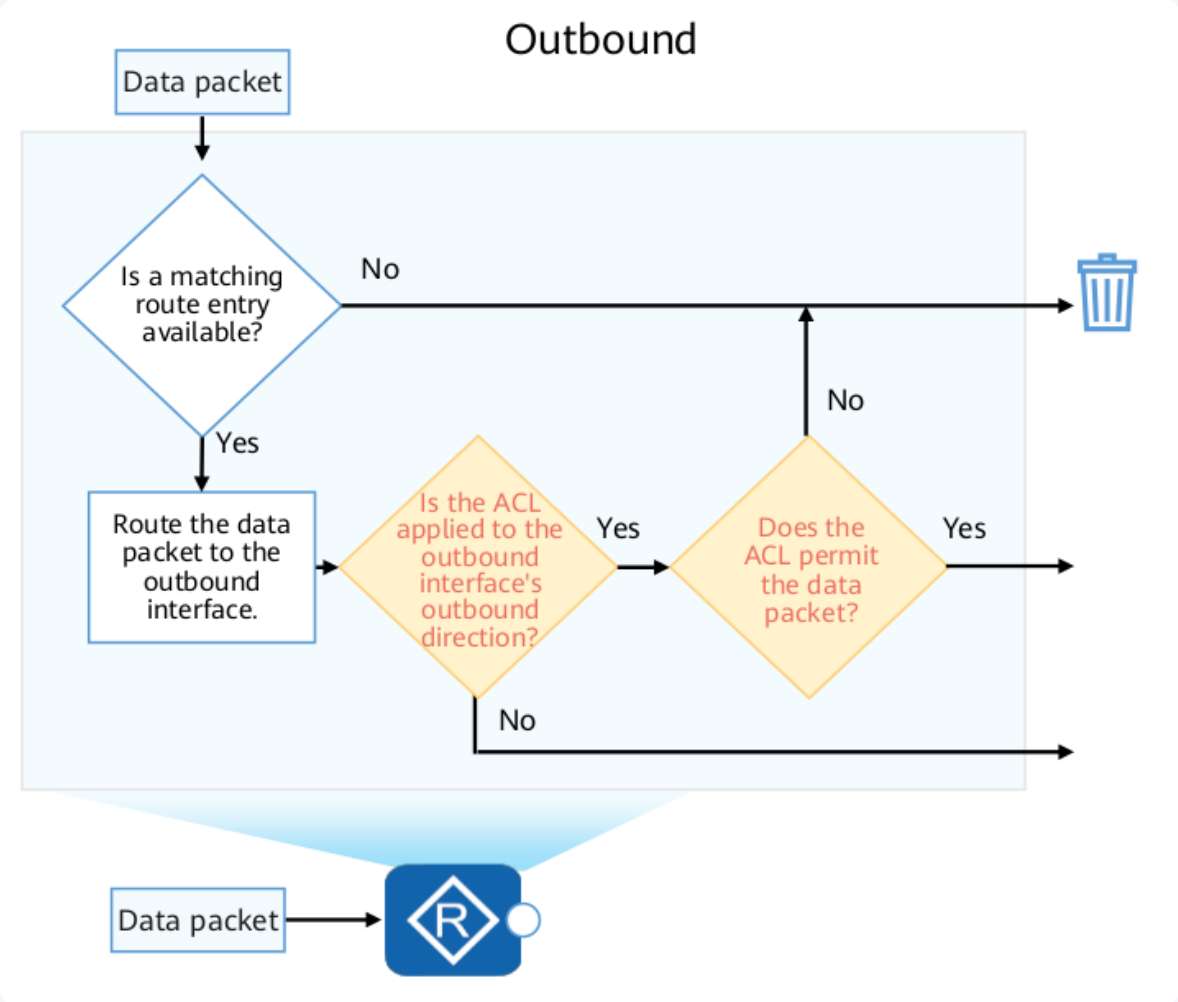
1.2.4 Applying ACLs

1.2.4.1 Directionality

Inbound interface:



Outbound interface:



1.3 Basic Configurations and Applications of ACLs

1.3.1 Creating a Basic ACL

Markdown

```
acl number <acl-number> <match-order config>
```

- `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.

- `sequential` : Rules are evaluated in the order they were entered.

```markdown
acl name <acl-name> <basic>||<acl-number> <match-order config>
```

- `<acl-name>` : Name of the ACL.
- `basic` : Specifies a basic ACL type.
- - `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

1.3.2 Configuring Basic ACL Rules

```markdown
rule <rule-id> <action> source <source-address> <source-wildcard>||any || time-range <time-name>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.

- `<time-name>` : Time range name for rule applicability.

1.3.3 Apply acl into interface

```markdown
traffic-filter <interface-bound> acl <acl-option>

```

- `<interface-bound>` :
  - **inbound:** configures ACL-based packet filtering in the inbound direction of an interface.
  - **outbound:** configures ACL-based packet filtering in the outbound direction of an interface.
- `<acl-option>` :
  - **acl-number**
  - **name acl-name**

1.3.4 Creating an Advanced ACL

```markdown
acl number <acl-number> <match-order config>
```

- `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

```markdown

```

```
acl name <acl-name> <advance>||<acl-number> <match-order config>
```

- `<acl-name>` : Name of the ACL.
- `basic` : Specifies a basic ACL type.
-
  - `<acl-number>` : ACL identification number.
- `match-order config` : Order of rule matching.
  - `auto` : The system determines the best order for matching.
  - `sequential` : Rules are evaluated in the order they were entered.

1.3.5 Configuring Advanced ACL Rules

Markdown

```
rule <rule-id> <action> ip destination <destination-address> <destination-wildcard>||any source <source-address> <source-wildcard>||any || time-range <time-name>
|| dscp <dscp> || tos <tos> || precedence <precedence>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- **ip:** indicates that the protocol type is IP.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.

- `<time-name>` : Time range name for rule applicability.
- `<dscp>` : Sets a priority label (0-63) for matched packets.
- `<tos>` : Sets a type of service label (0-15) for matched packets.
- `<precedence>` : Assigns a priority rank (0-7) for matched packets.

Markdown

```
rule <rule-id> <action> <protocol> destination <destination-address> <destination-wildcard>||any ||destination-port { eq <port> || gt <port> || lt <port> || range <port-start port-end> }  source <source-address> <source-wildcard>||any source-port { eq <port> || gt <port> || lt <port> || range <port-start port-end> } || time-range <time-name> || tcp-flag <flag>
```

- `<rule-id>` : Optional rule identifier.

> ranges from 0 to 4294967294.

- `<action>` :
  - `deny` : Blocks matching packets.
  - `permit` : Allows matching packets.
- **tcp:** indicates that the protocol type is TCP. You can set protocol-number to 6 to indicate TCP.
- `<source-address>` `<source-wildcard>` : Source IP address and wildcard mask.
- `any` : Matches any source IP address.
- **eq** `<port>` : equal to the destination port number
- **gt** `<port>` : greater than the destination port number
- **lt** `<port>` : less than the destination port number
- **range** `<port-start port-end>` : specifies a source port number range.
- `<time-name>` : Time range name for rule applicability.

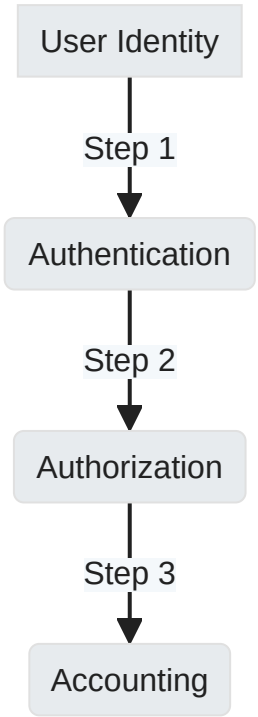
- `<flag>:` indicates the SYN Flag in the TCP packet header.

AAA Principles and Configuration

1 AAA Principles and Configuration

1.1 AAA Overview

1.1.1 AAA Concepts Overview



Note

AAA stands for Authentication, Authorization, and Accounting. It is a framework for controlling access to computer resources, enforcing policies,

and providing the tracking of user activities.

1.1.1.1 Authentication

- Determines **who** can access the network.
- **Modes:**
  - `Non-authentication` : No identity check. Rarely used due to security concerns.
  - `Local authentication` : Credentials are stored on NAS. Quick but hardware-limited.
  - `Remote authentication` : Credentials on an external server (RADIUS/HWTACACS).

User	Domain	Authentication Mode
User1@Domain1	Domain1	Non-authentication
User2@Domain2	Domain2	Local authentication
User3@Domain3	Domain3	Remote authentication

1.1.1.2 Authorization

- Determines **what** users can do after they are authenticated.
- **Modes:**
  - `Non-authorization` : Unrestricted access after-authentication.
  - `Local authorization` : Permissions based on NAS domain config.
  - `Remote authorization` : Permissions granted by RADIUS/HWTACACS server.

User	Domain	Authorization Mode
User1@Domain1	Domain1	Non-authorization

User	Domain	Authorization Mode
User2@Domain2	Domain2	Local authorization
User3@Domain3	Domain3	Remote authorization

> In HWTACACS authorization, all users can be authorized by the HWTACACS server.

> RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed singly.

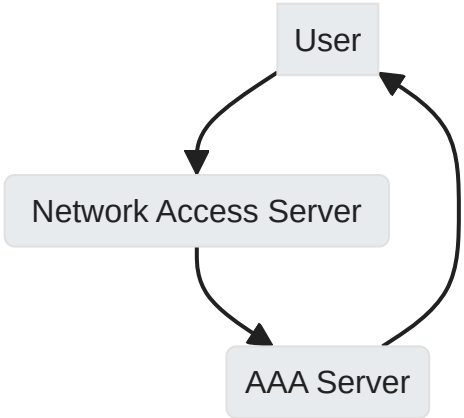
> When using remote authorization, the network access server (NAS) will prioritize the permissions given by the authorization server over its own settings.

1.1.1.3 Accounting

- Tracks network behavior and resource usage by authorized users.
- **Modes:**
  - `Non-accounting` : Free access with no logs.
  - `Remote accounting` : Activity tracking through RADIUS/HWTACACS server.

User	Domain	Accounting Mode
User1@Domain1	Domain1	Non-accounting

1.1.2 Common AAA Architecture



Tip

Different domains on the NAS can be associated with different AAA schemes (authentication, authorization, accounting).

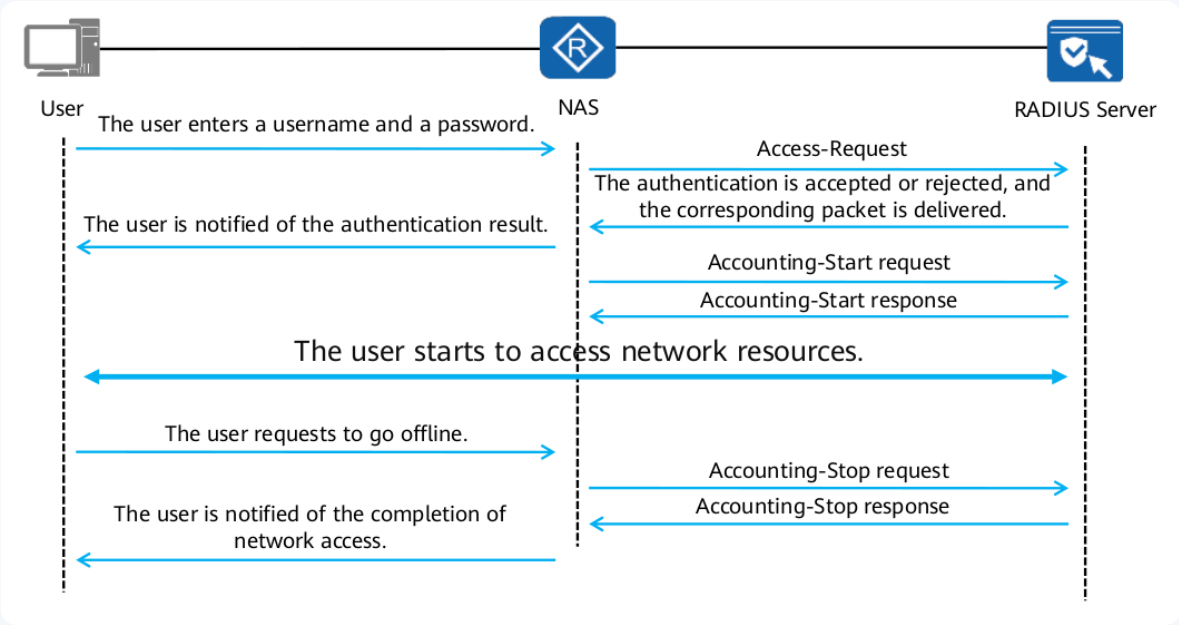
> **NAS (Network Attached Storage):** is a device that connects to a network, allowing multiple users and devices to store and access files from a central location.

1.1.3 RADIUS Implementation Protocol

The RADIUS protocol is commonly used for AAA implementations due to its distributed client/server model which supports user authentication, accounting, and authorization over UDP ports.

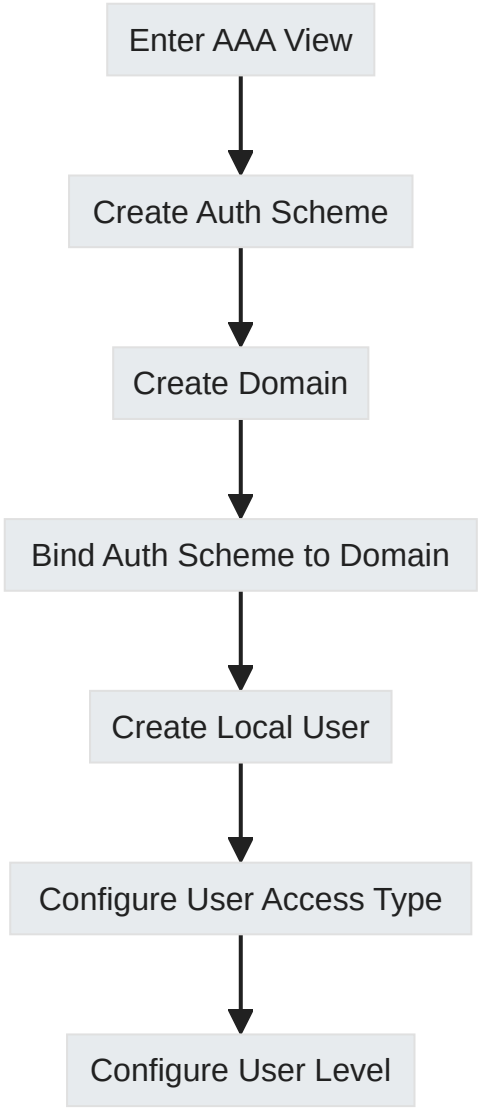
> **RADIUS,** which stands for Remote Authentication Dial-In User Service, is a protocol that helps manage access to network resources by verifying who is trying to connect (authentication), keeping track of what they're doing (accounting), and deciding what they are allowed to do (authorization). It operates over a network using UDP ports, which allows data to be sent quickly between the user's device and the server that checks their access rights.

RADIUS uses UDP ports **1812** and 1813 **as** the authentication and accounting ports, respectively



1.2 AAA Configuration

1.2.1 Steps to Configure AAA



1.2.1.1 Step 1: Enter AAA View

Markdown

```
[Huawei] aaa
```

1.2.1.2 Step 2: Create Authentication Scheme

Markdown

```
[Huawei-aaa] authentication-scheme <scheme-name>
[Huawei-aaa-authentication-scheme-name] authentication-mode <mode>
```

- `<mode>`
  - hwtacacs
  - local
  - radius

> By default, the authentication mode is set to local.

1.2.1.3 Step 3: Create Domain and Bind Authentication Scheme

Markdown

```
[Huawei-aaa] domain <domain-name>
[Huawei-aaa-domain-name] authentication-scheme <scheme-name>
```

> Bind your created authentication scheme to your new domain.

1.2.1.4 Step 4: Create Local User

Markdown

```
[Huawei-aaa] local-user <user-name> password cipher <password>
```

> The username may include a domain if it contains an "@" symbol. Otherwise, it uses the default domain.

1.2.1.5 Step 5: Configure User Access Type

```markdown
[Huawei-aaa] local-user <user-name> service-type <type> <access>
```

- `<type>`:
  - terminal
  - telnet
  - ftp
  - ssh
  - snmp
  - http
- `<access>`:
  - ppp
  - none

> Set the service type for which the user is authorized. By default, all access types are disabled.

1.2.1.6 Step 6: Configure User Level

```markdown
[Huawei-aaa] local-user <user-name> privilege level <level>
```

> Define the user's privilege level within the system.

1.2.2 Verification Commands

1.2.2.1 Display Domain Information

```markdown
[R1]display domain name <domain-name>
```

```
[R1]display domain name default_admin
  Domain-name:                    default_admin
  Domain-state:                   Active
  Authentication-scheme-name:     default
  Accounting-scheme-name:         default
  Authorization-scheme-name:      -
  Service-scheme-name:            -
  RADIUS-server-template:         -
  HWTACACS-server-template:       -
  User-group:                     -
```

Displays configuration of `<domain-name>` domain.

1.2.2.2 Check Offline Records

```markdown
[R1]display aaa offline-record all
```

```
[R1]display aaa offline-record all
  ----------------------------------------------------------------
  User name:          huawei
  Domain name:        default_admin
  User MAC:           00e0-fc12-3456
  User access type:   telnet
  User IP address:    10.1.1.2
  User ID:            1
  User login time:    2019/12/28 17:59:10
  User offline time:  2019/12/28 18:00:04
  User offline reason: user request to offline
```

Shows records of users who have logged off from the system

Network Address Translation

1 Network Address Translation

1.1 NAT Overview

1.1.1 Motivation Behind NAT

- **IPv4 Address Shortage**: As Internet usage grows, public IPv4 addresses are becoming increasingly Limited.
- **Uneven Allocation**: Some regions face a severe shortage due to uneven distribution of addresses.
- **Transition Technologies**: Necessary to Save IPv4 addresses and enable continued internet connectivity.

1.1.2 Public vs. Private IP Addresses

- **Public IP Addresses**:
  - Managed by dedicated organizations.
  - Used for direct communication on the Internet.
- **Private IP Addresses**:
  - Can be assigned by anyone within internal networks.

- Not routable on the Internet.

1.1.2.1 Reserved Private IP Address Ranges

Range	Class
10.0.0.0 – 10.255.255.255	Class A
172.16.0.0 – 172.31.255.255	Class B
192.168.0.0 – 192.168.255.255	Class C

1.1.3 NAT Implementation

Note

NAT is a protocol for translating private IP addresses to public ones and vice versa.

> NAT does provide a layer of obscurity which can complicate direct attacks from external entities on internal network devices.

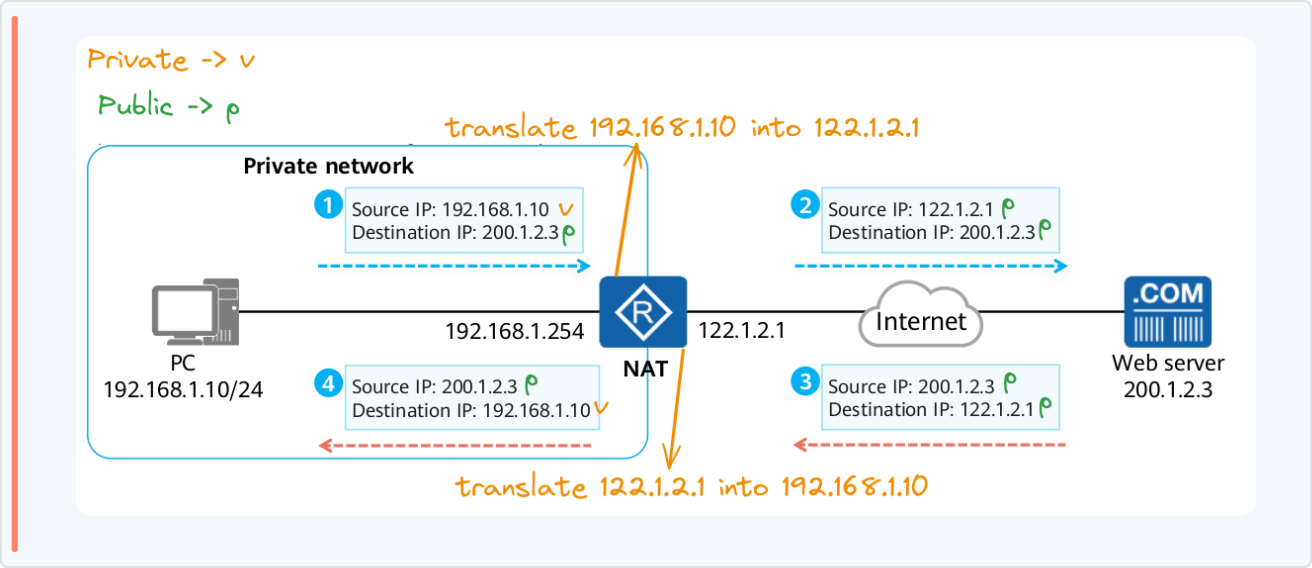
1.1.3.1 Typical NAT Scenarios:

1. **Internal to External**: Translates source private IP to a public IP for outbound traffic.
2. **External to Internal**: Translates destination public IP back to the original private IP for inbound traffic.

1.1.3.2 How NAT Conserves IPv4 Addresses:

- `NAT + Private Addresses` : This combination significantly reduces the need for public IPv4 addresses by allowing multiple devices on a private network to share a single public address.

1.1.3.3 Example of NAT Process:



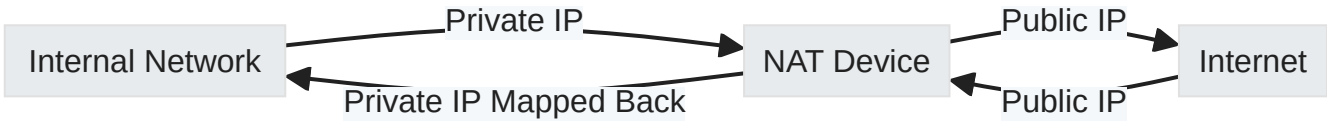
1.2 Static NAT

1.2.1 Static NAT Implementation

Static Network Address Translation (NAT): allows private IP addresses to be mapped to fixed public IP addresses, enabling bidirectional access between an internal host and the Internet.

Private Address	Public Address
192.168.1.1/24	122.1.2.1
192.168.1.2/24	122.1.2.2
192.168.1.3/24	122.1.2.3

1.2.1.1 Key Concepts



1.2.2 Bidirectional Access

- **Outgoing Traffic:** Private IP -> Public IP (Egress)
- **Incoming Traffic:** Public IP -> Private IP (Ingress)

1.2.3 Configuring Static NAT

1.2.3.1 Method 1: Interface View Configuration

```markdown
[Huawei-GigabitEthernet0/0/0] nat static global <public-address> inside <private-address>
```

1.2.3.2 Method 2: System View Configuration

```markdown
[Huawei] nat static global <public-address> inside <private-address>
```

After configuring the above, enable static NAT on the specific interface:

```markdown
```

```
[Huawei-GigabitEthernet0/0/0] nat static enable
```

1.3 Dynamic NAT

1.3.1 Key Concepts of Dynamic NAT

Dynamic NAT maps private IP addresses to a pool of public IP addresses. It efficiently utilizes public addresses by only assigning them when internal hosts require access to an external network.

> Dynamic NAT does not translate port numbers. It uses a No-Port Address Translation (No-PAT) method.

> 1:1 mapping between public and private addresses.

> Does not improve public address utilization since each private IP needs a unique public IP.

1.3.2 Benefits of Dynamic NAT

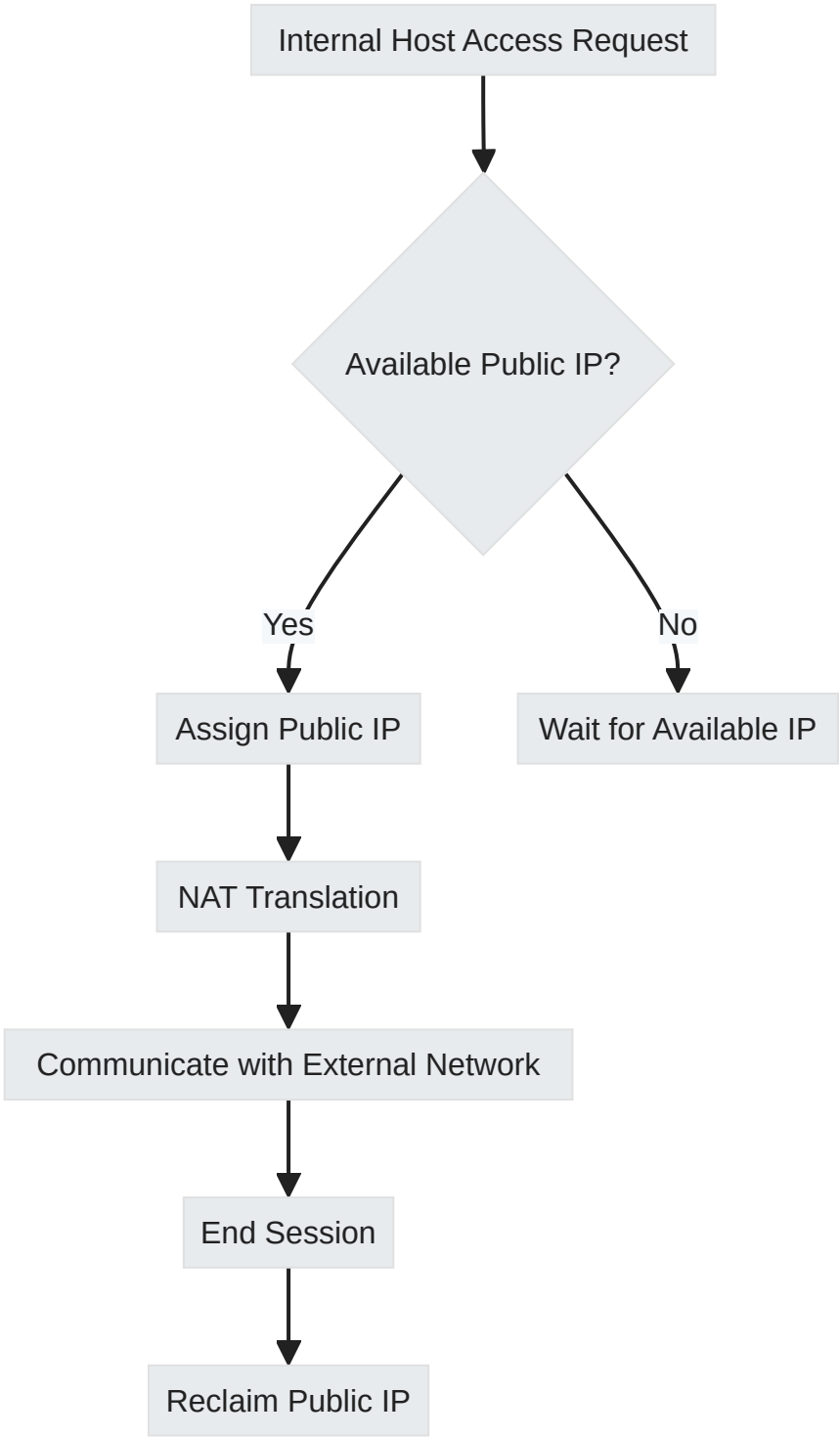
- Efficient usage of public IP addresses.
- On-demand mapping reduces address waste.
- Supports multiple internal hosts with fewer public IPs.

1.3.3 How Dynamic NAT Works

1. **Mapping Request**: Internal host requests access to an external network.

2. **Address Assignment**: A free public IP from the pool is assigned to the host.
3. **Communication**: The internal host communicates using the assigned public IP.
4. **Session End**: Once done, the public IP is returned to the pool for future use.

1.3.4 Dynamic NAT Process



1.3.5 Configuring Dynamic NAT

1.3.5.1 Step 1: Create an Address Pool

Create a range of public IP addresses that can be used for dynamic mapping.

```markdown
[Huawei] nat address-group <group-index> <start-address> <end-address>
```

1.3.5.2 Step 2: Configure an ACL Rule for NAT

Set up an Access Control List (ACL) that specifies which private addresses require dynamic NAT.

```markdown
[Huawei] acl <number>
[Huawei-acl-basic-number] rule permit <source> <source-address> <source-wildcard>
```

1.3.5.3 Step 3: Configure Outbound NAT with Address Pool on Interface View

Link the ACL rule with the address pool for dynamic NAT on the interface, optionally disabling port translation (no-pat).

```markdown
[Huawei-GigabitEthernet0/0/0] nat outbound <acl-number> address-group <group-index> no-pat
```

1.4 NAPT and Easy IP

1.4.1 Network Address and Port Translation (NAPT)

- **Description**: NAPT translates both IP addresses and port numbers, allowing multiple internal hosts to share one public IP address.
- **Mapping**: 1:n mapping between public and private addresses.
- **Address Utilization**: Effectively improves public address utilization.

1.4.1.1 NAPT Implementation Steps

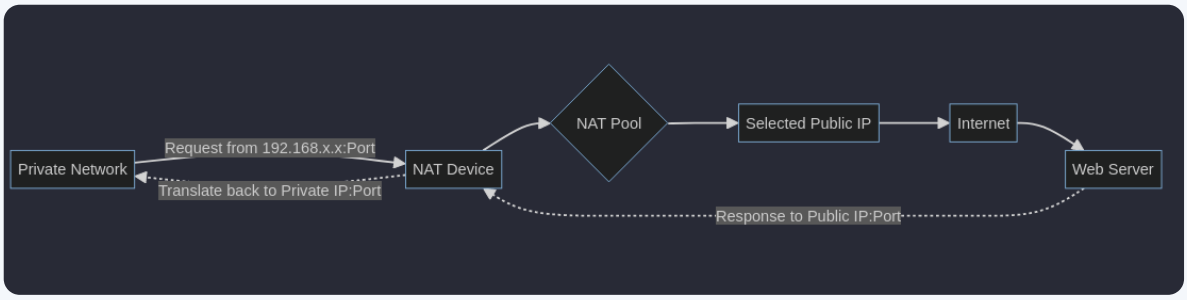
1. Select an address from the pool and translate both the source IP address and port number.
2. Generate a temporary NAT mapping table with pre-translation(private) and post-translation(public) pairs.

> **Note**
>
> NAPT enables multiple private IP addresses to map to a single public IP address through different port numbers.

1.4.1.2 Example NAT Mapping Table

Private IP Address:Port	Public IP Address:Port
192.168.1.1:10321	122.1.2.2:1025
192.168.1.2:17087	122.1.2.2:1026

1.4.1.3 NAPT Process



1.4.1.4 NAPT Configuration

Link the ACL rule with the address pool for NATP on the interface with port translation.

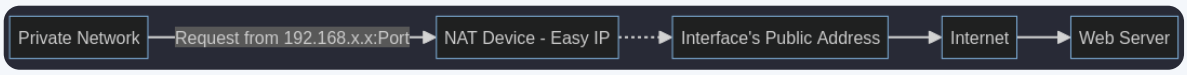
```markdown
[Huawei-GigabitEthernet0/0/0] nat outbound <acl-number>
address-group <group-index>
```

1.4.2 Easy IP

- **Description**: Similar implementation as NAPT but without an Specific address pool.
- **Interface Address**: Uses interface address as the public address for NAT translation.

1.4.2.1 Use Cases for Easy IP

- Suitable for scenarios where public IPs are not fixed or dynamically obtained through DHCP or PPPoE dial-up.



1.4.2.2 Configure Easy IP

Link the ACL rule with Easy IP on the interface

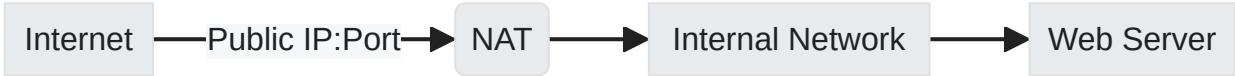
Markdown

```
[Huawei-GigabitEthernet0/0/0] nat outbound <acl-number>
```

1.5 NAT Server

1.5.1 Overview

NAT (Network Address Translation) Server is crucial for mapping an internal server's private IP and port to a public IP and port. This allows the internal server to provide services to the public network.



> **Nat Server:** is NAT Functionality within Routers

1.5.2 Configuration Steps

1.5.2.1 NAT Server Mapping Command

```markdown
[R1-GigabitEthernet0/0/1]nat server protocol <protocol> global <public-address> <port-name> inside <private-address> <private-port>
```

- `<protocol>`:
  - tcp
- `<port-name>`:
  - `www` or `80`

Network Services and Applications

1 Network Services and Applications

1.1 File Transfer

1.1.1 FTP

1.1.1.1 Overview

- **FTP** and **TFTP** were key file transfer protocols in the early internet era.
- They are used for transferring files between hosts on IP networks.

1.1.1.2 FTP Basics

1.1.1.2.1 Transfer Modes

- **ASCII Mode:** For text files (.txt, .log, .cfg)
  - Converts characters to ASCII code for efficient transfer.
  - Recommended for network device config files and logs.

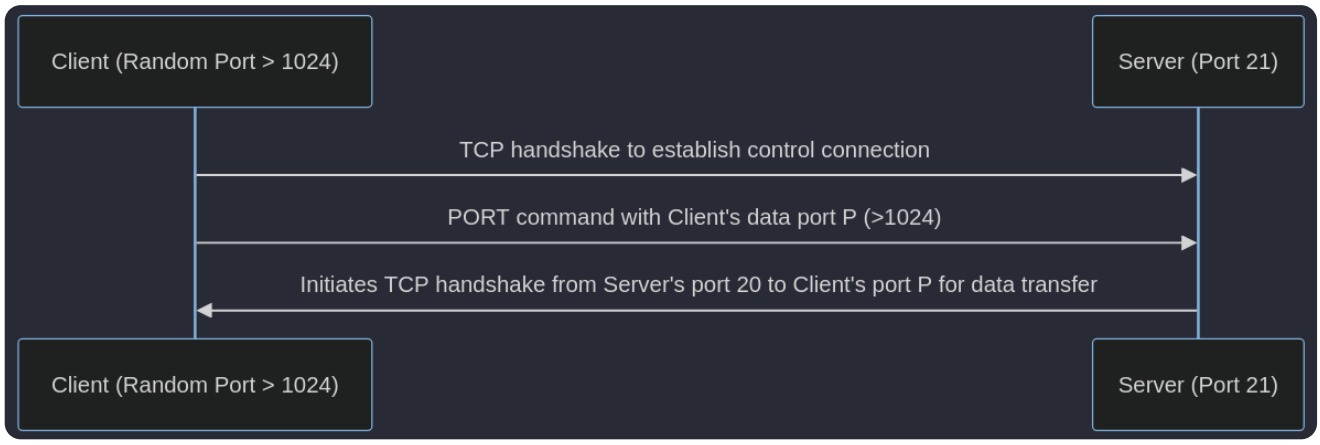
- **Binary Mode:** For non-text files (.cc, .bin, .exe, .png)
  - Transfers data without conversion.
  - Recommended for executable programs and images.

1.1.1.2.2 Client/Server Architecture

- FTP operates on a client/server model.
- A TCP connection is established between the FTP client and server to upload or download files.

1.1.1.3 FTP Transfer Process

1.1.1.3.1 Active Mode (PORT)

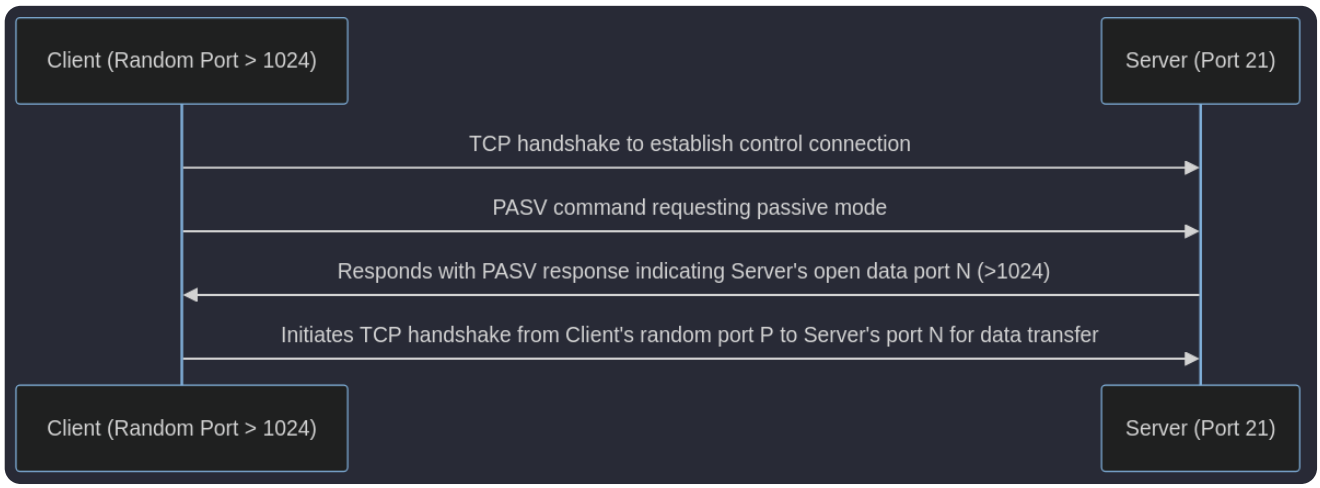


- The client informs the server of its listening data port using the PORT command.
- The server connects back to this port from its data port (20) to establish a data connection.

> **Port greater than** 1024**:** dynamic/private ports, can generally be used

> without any restrictions or need for IANA registration.

1.1.1.3.2 Passive Mode (PASV)



- The server informs the client of its listening data port using the PASV response.
- The client connects to this open server port to start transferring data.

Modes

- **In active mode,** issues may arise with NAT devices blocking incoming connections from the server.
  - Issues can arise if the client is behind a NAT (Network Address Translation) device, like a router, which assigns a different IP address to your machine than the one visible on the internet. Because of this, when the server tries to connect back to the client's data port, the NAT device may not know how to route this incoming connection from an outside source and could block it.
- **In passive mode,** firewall restrictions may prevent outgoing connections from the client.
  - issues might occur if there are strict firewall settings at the client side that prevent outgoing connections to random high-numbered ports that servers typically use in passive mode.

1.1.1.4 Configuration Commands

1.1.1.4.1 As FTP Server

---

1. **Enable FTP Server**
   - **Command:** `ftp <ipv6> server enable`

> By default, disabled.

2. **Configure Local User**

```markdown
[Huawei]aaa
[Huawei]local-user <user-name> password irreversible-cipher <password>
[Huawei]local-user <user-name> privilege level <level>
[Huawei]local-user <user-name> service-type ftp
[Huawei]local-user <user-name> ftp-directory <directory>
```

> Setting up local users on an FTP server helps control who can get in, what they can do, where they go, and keeps things safe and tidy.

> The `ftp-directory` command assigns a specific starting folder for a user's FTP session on a Huawei device.

> Level must be at least level 3.

1.1.1.4.2 As FTP Client

1. **Accessing FTP Server**

```markdown
<FTP Client>   ftp <server IP>
```

2. **Common Commands**

Command	Description
ascii	Set file transfer type to ASCII
binary	Set file transfer type for binary images
ls	List directory contents
passive	Toggle passive mode; default is on
get	Download remote file
put	Upload local file

1.1.2 TFTP

1.1.2.1 Overview

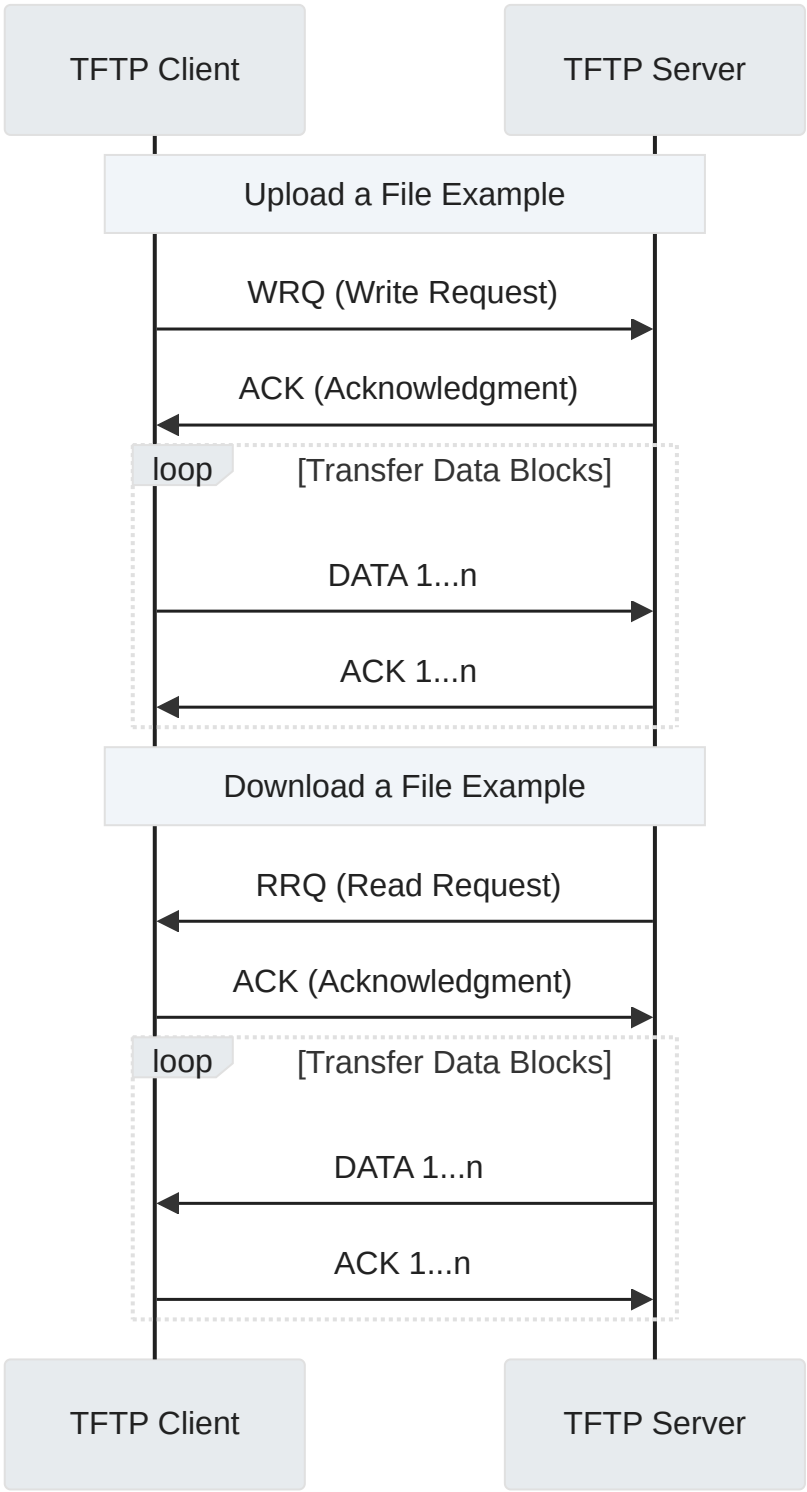
- TFTP is simpler than FTP; designed for transferring small files.
- It uses UDP on port 69, which makes it less reliable but faster for small transfers.
- No authentication is necessary to transfer files.
- Users can upload or download files but cannot see the server's file directory.

> See specefic files or folder like sharing in onedrive

1.1.2.2 Key Differences from FTP

- `Authentication` : TFTP does not require user authentication.
- `Protocol` : Uses UDP instead of TCP.
- `Complexity` : Easier implementation with fewer features.

1.1.2.3 How TFTP Works



1.1.2.3.1 Packet Formats

Type	Description
RRQ	Read Request Packet
WRQ	Write Request Packet
DATA	Data Transmission Packet
ACK	Acknowledgment Packet
ERROR	Error Control Packet

1.1.2.4 Configuration Commands

When using a Huawei VRP device as a TFTP client:

1.1.2.4.1 Downloading Files

```markdown
<HUAWEI> tftp <tftp_server> get <filename>
```

1.1.2.4.2 Uploading Files

```markdown
<HUAWEI> tftp <tftp_server> put <filename>
```

> Note that VRP devices(Huawei) only function as TFTP clients.

1.2 Telnet

1.2.1 Overview

- Telnet allows **device management using commands**.
- **No dedicated cable** needed; operates over IP networks on TCP port 23.

1.2.2 Devices

- Devices managed through Telnet are called **Telnet servers**.
- Devices connecting to these are **Telnet clients**.
- Network devices like ACs, APs, firewalls, routers, switches can be both server and client.

1.2.3 VTY User Interface

1.2.3.1 Purpose

- Allocates a user interface for managing sessions when logged in via console port or Telnet.

1.2.3.2 Configuration Parameters

- Authentication mode
- User privilege level after login

1.2.3.3 Configuration Commands

1.2.3.3.1 Enabling Telnet Server Function

```markdown
[Huawei] telnet server enable
```

> By default, the Telnet server function is disabled.

1.2.3.3.2 Creating virtual interface

```markdown
[Huawei] user-interface vty <first-ui-number> <last-ui-number>
```

> The `first-ui-number` and `last-ui-number` specify the starting and ending VTY line numbers, respectively, for configuring remote access on a Huawei device.

1.2.3.3.3 Configuring Protocols

```markdown
[Huawei-ui-vty0-4] protocol inbound <all>||<telnet>||<ssh>
```

> **Default:** Supports SSH and Telnet.

1.2.3.3.4 Setting Authentication Mode and Password

```markdown
[Huawei-ui-vty0-4] authentication-mode <aaa>||<non>||<password>
[Huawei-ui-vty0-4] set authentication password cipher <password>
```

> By default, no default authentication mode is available.

1.2.3.3.5 Connect via telnet

```markdown
<Host>telnet <ip-address>
```

- `<ip-address>` : ip address of telnet server

1.3 DHCP

1.3.1 Key Issues with Manual Network Configuration

- **Complex Parameters**: Not user-friendly; leads to misconfigurations.
- **Workload**: Administrators face repetitive tasks and heavy workloads.
- **Utilization**: Fixed IP addresses lead to low utilization as some remain unused.
- **Flexibility**: Lack of flexibility when moving between networks or offices.

1.3.2 DHCP Overview

1.3.2.1 Working Principle

- **Dynamic Host Configuration Protocol (DHCP)** automates IP address assignment.
- Uses a client/server model for host plug-and-play connectivity.

1.3.2.2 Advantages of DHCP

Feature	Description
Unified Management	Centralized IP address assignment and management.
IP Address Lease	Temporary allocation with defined lease time improves utilizations.

1.3.2.3 DHCP Process Explained

1. `DHCP Discover` **(Broadcast):** Client searches for a server.
2. `DHCP Offer` **(Unicast):** Server offers an IP address to the client.
3. `DHCP Request` **(Broadcast):** Client accepts the offer and informs all servers.
4. `DHCP ACK` **(Unicast):** Server acknowledges the client's use of the IP address.

1.3.2.4 Lease Renewal

- At 50% of lease time (`T1`), client tries to renew the lease unicastly with original server.
- At 87.5% of lease time (`T2`), client broadcasts request for any server's response if no previous acknowledgment received.

1.3.3 Configuration Commands Overview

1.3.3.1 To Enable DHCP:

```markdown
[Huawei] dhcp enable
```

1.3.3.2 Interface Address Pool Commands:

```markdown
[Huawei-Gigabitthernet0/0/0]dhcp select interface
[Huawei-Gigabitthernet0/0/0]dhcp server dns-list <ip-address>
[Huawei-Gigabitthernet0/0/0]dhcp server excluded-ip-address <start-ip-address> <end-ip-address>
[Huawei-Gigabitthernet0/0/0]dhcp server lease day <day> hour <hour> minute <minute> || unlimited
```

> Enable the interface to use the interface address pool to provide the DHCP server function.

> By default, the IP address lease is one day.

1.3.3.3 Global Address Pool Commands:

```markdown
[Huawei]ip pool <ip-pool-name>
```

```
[Huawei-ip-pool-name]network ip-address mask <mask>|| <mask-length>
[Huawei-ip-pool-name]gateway-list <ip-address>
[Huawei-ip-pool-name]dns-list <ip-address>
[Huawei-ip-pool-name]lease day <day>  hour <hour> minute <minute> || unlimited
[Huawei-Gigabitthernet0/0/0]dhcp select global
```

> When you set `dhcp select global` on a Huawei router interface, it can assign IP addresses from any available pool that fits the network of the device asking for an IP.

> range of IP addresses that can be assigned dynamically in the global address pool.

1.4 HTTP

1.4.1 Overview

- The browser communicates with web servers using the HTTP protocol.
- A URL is entered into a browser to locate and request resources from a server.

1.4.2 Key Concepts

1.4.2.1 HTTP Protocol

- **HTTP**: Application layer protocol for communication between clients and servers.
  - Uses TCP/IP for transmission.
  - Operates in a client/server model.

1.4.2.2 URL Structure

- **URL (Uniform Resource Locator)**: Uniquely identifies the location of resources on the Internet.
  - Example: `www.huawei.com`

1.4.2.3 WWW Components

- **WWW**: World Wide Web, a system for accessing and sharing documents over the Internet.
- Comprised of:
  - **HTML** (Hypertext Markup Language): For document content display in browsers.
  - **HTTP** (Hypertext Transfer Protocol): For document transmission on the network.

- **URL** (Uniform Resource Locator): For specifying document locations on the network.

1.5 DNS

1.5.1 Overview of DNS

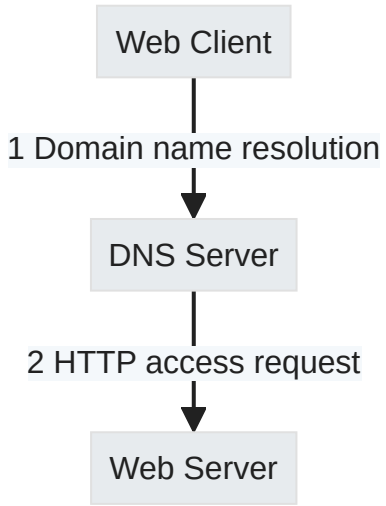
> **DNS** stands for Domain Name System, which is the protocol used for resolving domain names to IP addresses. It's essential for converting human-friendly domain names like `www.example.com` into machine-readable IP addresses like `192.168.1.1`.

1.5.2 Birth of DNS

DNS was created because the early internet, called ARPANET, got too big. Before DNS, there was a file (Host.txt) that listed all the computers on the network, but as more people started using the network, it became too hard to keep that file up to date and to make sure everyone's computer names were unique. DNS made it easier by automating this process.

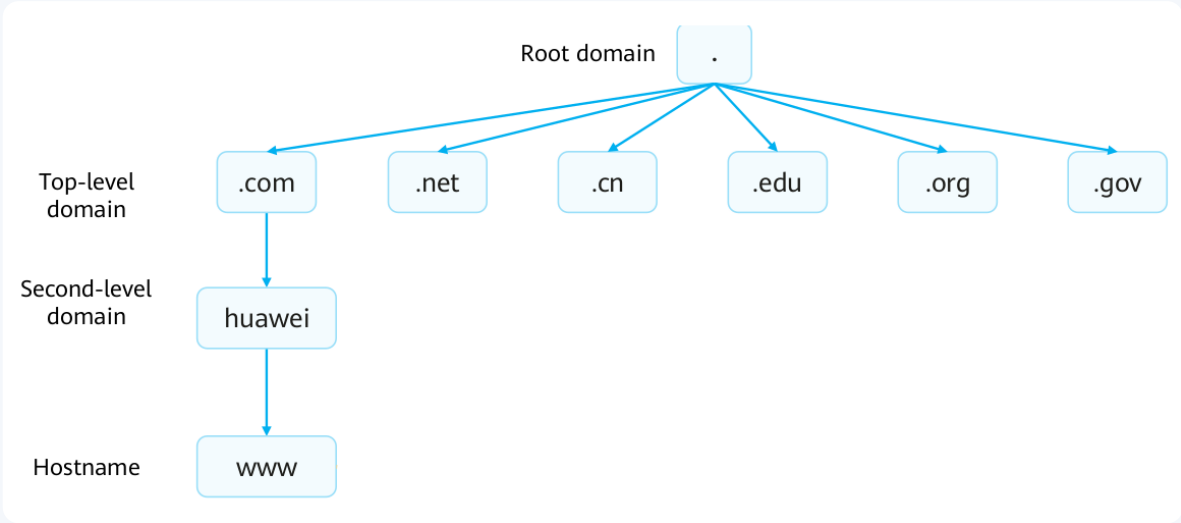
1.5.3 DNS Components

- **Domain Name**: A string used to identify hosts (e.g., www.huawei.com (http://www.huawei.com)).
- **DNS Server**: Manages mappings between domain names and IP addresses.



1.5.4 Domain Name Format

A domain name consists of multiple parts: `hostname.second-level domain.top-level domain.root domain`. The root domain is represented by a dot (`.`).

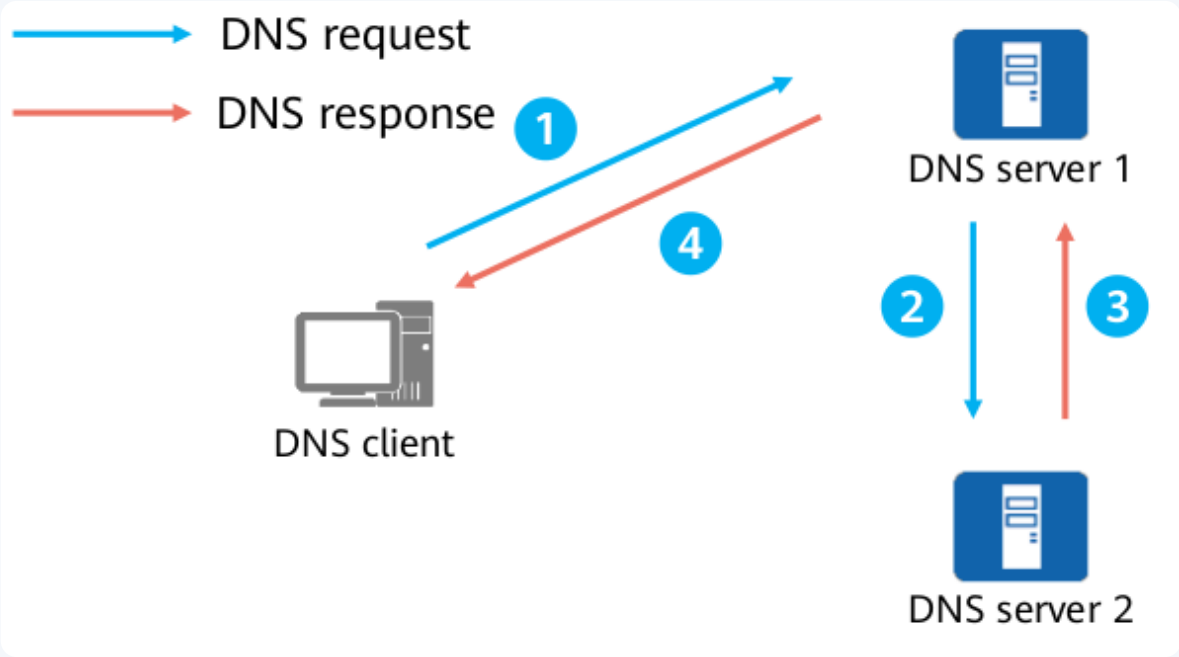


> Example: For `www.huawei.com`, `www` is the hostname, `huawei` is the second-level domain, and `.com` is the top-level domain.

1.5.5 DNS Query Modes

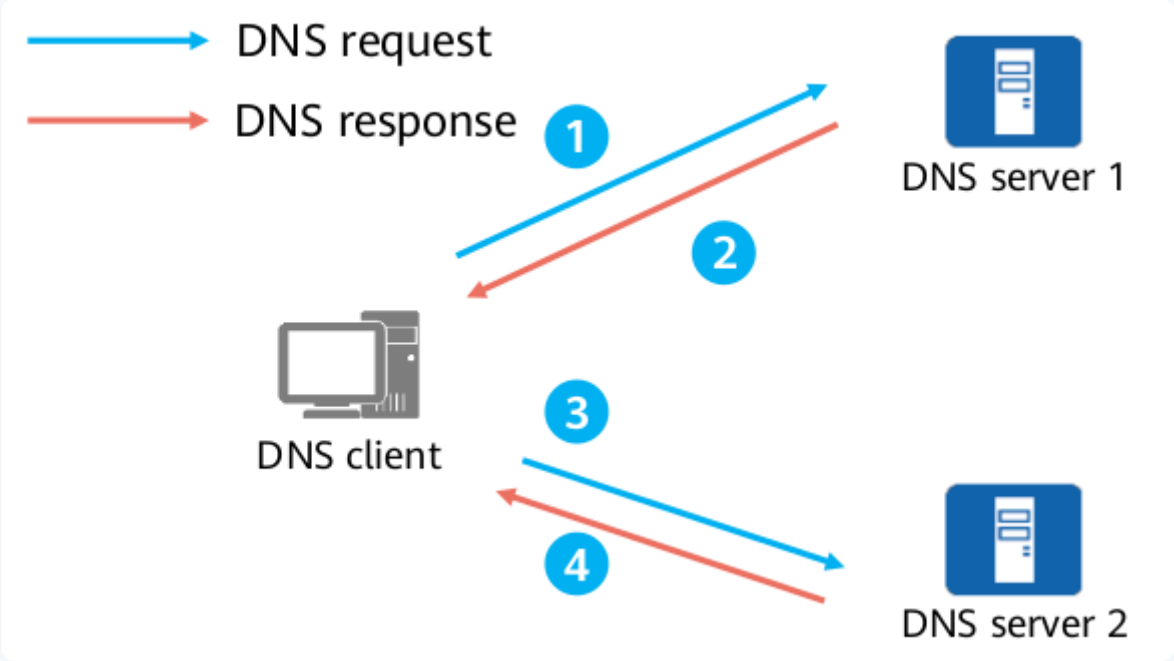
There are two query modes when a client needs to resolve a domain name:

1.5.5.1 Recursive Query



🔄 **Recursive Query**: The client requests a DNS server; if that server doesn't have the answer, the server queries other servers until it finds it.

1.5.5.2 Iterative Query



🔀 **Iterative Query**: The client requests a DNS server; if that server doesn't have the answer, it refers the client to another server.

In recursive queries, each server in chain resolves part of the address until reaching a result. In iterative queries, each server points to another one without doing extra work itself.

1.6 NTP

1.6.1 Time Synchronization Requirements

1.6.1.1 Network Management

- Logs/debug messages analysis requires consistent timestamps.

1.6.1.2 Charging System

- Devices must have synchronized clocks for accurate billing.

1.6.1.3 Collaborative Systems

- Ensures proper sequence for events handled by multiple systems.

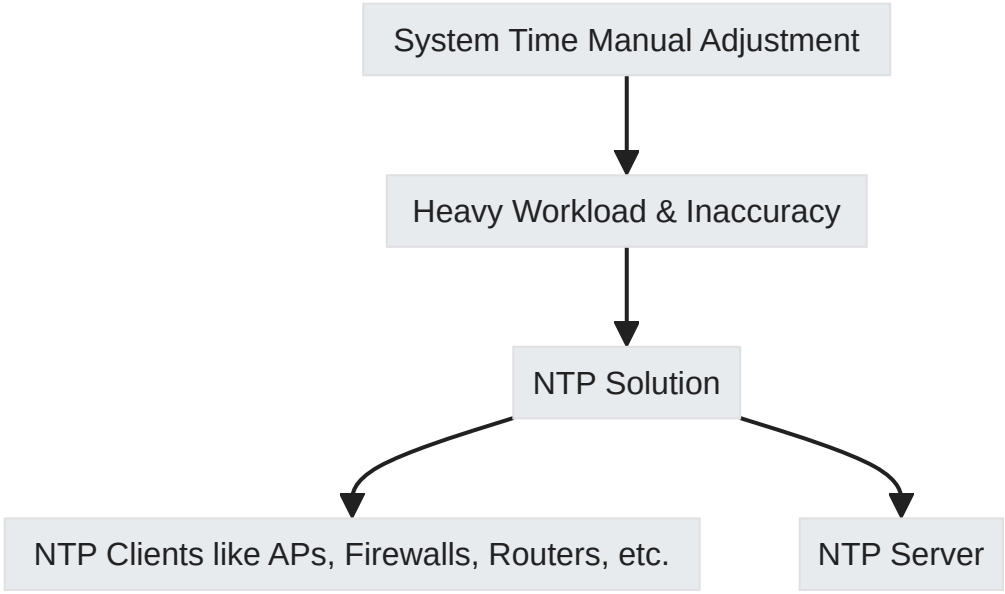
1.6.1.4 Incremental Backup

- Synchronization between backup server and clients is crucial.

1.6.1.5 System Time

- Timestamps needed for user login and file modification tracking.

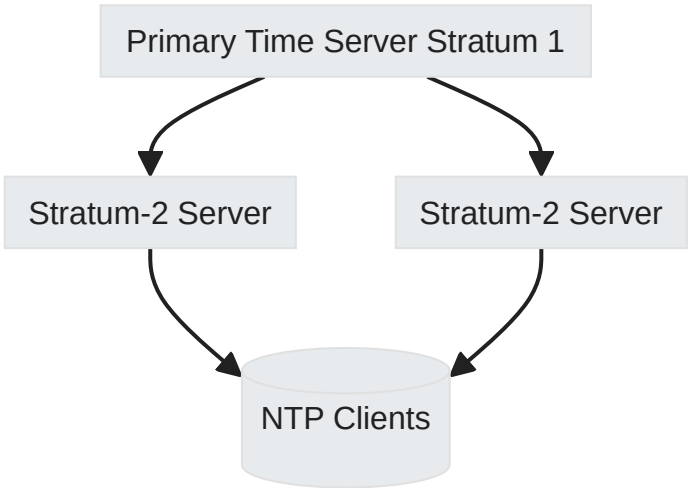
1.6.2 Overview



- **Protocol Layer**: Application layer of TCP/IP suite.
- **Transport**: Uses IP and UDP on port `123`.
- **Function**: Synchronizes time across devices.

> **Note**
>
> Manual adjustments are inefficient. NTP automates clock synchronization with high accuracy.

1.6.3 NTP Network Structure



Stratum Level	Description
1	Highest precision; uses a reference clock (e.g., GPS)
2	Syncs with Stratum 1 or other Stratum 2 servers
3 to 15	Lower precision; higher number indicates less precision

Tip

Smaller stratum value means higher precision for time synchronization.

WLAN Overview

1 WLAN Overview

1.1 WLAN Overview

1.1.1 Basics of WLAN

- Constructed using wireless technologies like Wi-Fi, infrared, Bluetooth, ZigBee.

> - **Infrared**: A wireless communication technology that uses infrared(light below red) light waves to transmit data over short distances, typically used in remote controls for TVs and other devices.
> - **ZigBee**: A low-power, low-data-rate wireless communication protocol designed for creating personal area networks with small, low-power digital radios, often used in home automation and IoT devices.

- **Operates at high frequencies:** 2.4 GHz or 5 GHz.

> 2.4 GHz and 5 GHz are frequency bands used in wireless communications because they are internationally designated for

> unlicensed use, allowing for widespread compatibility with many devices without the need for individual licenses.

- Provides mobility within wireless network coverage.

1.1.2 Components of a WLAN

- **Router**: Connects networks and directs data traffic.
- **Switch**: Filters and forwards data to devices within the network.
- **Access Point (AP)**: Extends wireless coverage and connects devices to the network.

1.1.3 Classification of Wireless Networks

---

1. `WPAN` : Personal area network (Bluetooth, ZigBee).
2. `WLAN` : Local area network (Wi-Fi).
3. `WMAN` : Metropolitan area network (WiMAX).
4. `WWAN` : Wide area network (GSM, LTE).

1.1.4 Advantages of WLAN

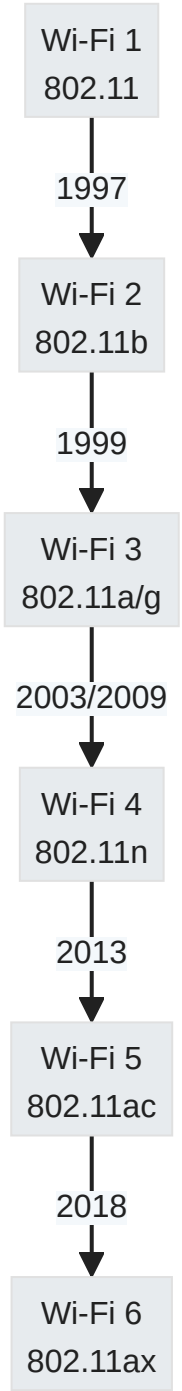
> High mobility and flexible deployment make WLANs suitable for environments with moving users or where cable deployment is difficult.

1.1.5 IEEE 802 Standards & Wi-Fi Generations

1.1.5.1 IEEE 802.11 Standards

- Defines standards for WLANs by IEEE as (IEEE 802.11).
- Located on the lower two layers of TCP/IP model: Data link layer & Physical layer.

1.1.5.2 Wi-Fi Generations



1.1.5.2.1 Frequency Bands & Throughput by Standard

Frequency Band	Throughput	Standard	Wi-Fi	Released In
2.4 GHz	2 Mbit/s	802.11	Wi-Fi 1	1997
2.4 GHz	11 Mbit/s	802.11b	Wi-Fi 2	1999

Frequency Band	Throughput	Standard	Wi-Fi	Released In
2.4 GHz, 5 GHz	54 Mbit/s	802.11a/g	Wi-Fi 3	2003
2.4 GHz & 5 GHz	300 Mbit/s	802.11n	Wi-Fi 4	2009
5 GHz	1300 Mbit/s	802.11ac wave1	Wi-Fi 5	2013
5 GHz	6.9Gbit/s	802.11ac wave2	Wi-Fi 5	2015
2.4 GHz & 5 GHz	9.6Gbit/s	802.11ax	Wi-Fi 6	2018

1.1.6 Evolution of Wireless in Office Scenarios

1.1.6.1 Mobile Office Phases

1.1.6.1.1 Phase 1: Initial Mobile Office Era

> Wireless networks were Add-ons to wired networks with limited requirements on security and capacity.

1.1.6.1.2 Phase 2: Wireless Office Era

> Integration of wired and wireless networks became essential; higher bandwidth required due to services like video and voice.

1.1.6.1.3 Phase 3: All-Wireless Office Era

> Preference for wireless over wired networks; offices covered entirely by Wi-Fi; emergence of high-bandwidth services on wireless networks (e.g., telepresence conference, VR/AR).

1.2 Basic Concepts of WLAN

1.2.1 Enterprise WLAN Products

1.2.1.1 Access Point (AP)

- **Modes:**
  - **Fat AP**: Standalone, simple functions, cost-effective.

> usually, used in wireless router for home network

- **Fit AP**: Managed by AC, Multiple uses, requires skilled persons.
- **Cloud AP**: Managed by cloud platform, supports plug-and-play.

1.2.1.2 Access Controller (AC)

- Deployed in network aggregation layer.
- Manages Fit APs providing large capacity and performance.

1.2.1.3 PoE Switch

- Supplies power over Ethernet to devices like APs.

1.2.2 Basic WLAN Networking Architecture

1.2.2.1 Fat AP Architecture

Independently working Fat APs with limited scalability due to management difficulties.

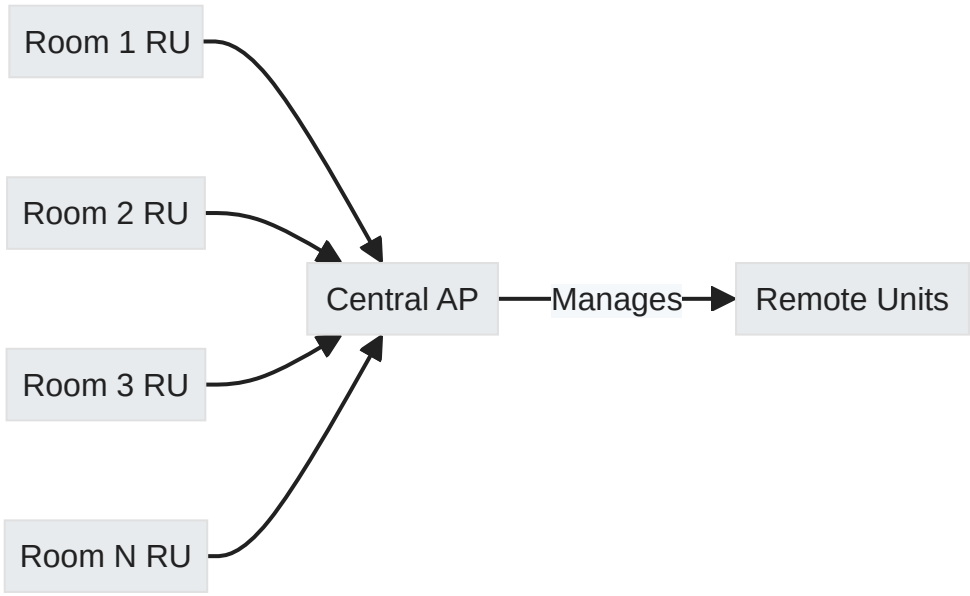
1.2.2.2 AC + Fit AP Architecture

Centralized control through an AC managing multiple Fit APs; scalable for larger enterprises.

Communication Protocols

- **AP uses**
  - Wired Side
    - Ethernet Protocols
  - Wireless Side
    - 802.11 Standards

1.2.3 Agile Distributed Architecture



- Divides an AP into a **central** unit managing **multiple** remote **units**.

1.2.4 CAPWAP Tunnels

Function	Description
Management	Allows the AC to manage and control the APs.
Data Transfer	Facilitates data exchange between STAs and the network through CAPWAP tunnels.

> **CAPWAP** is a system that helps manage wireless networks by securely linking each access point to a main controller, making it easier to handle data sent by devices like phones and laptops.

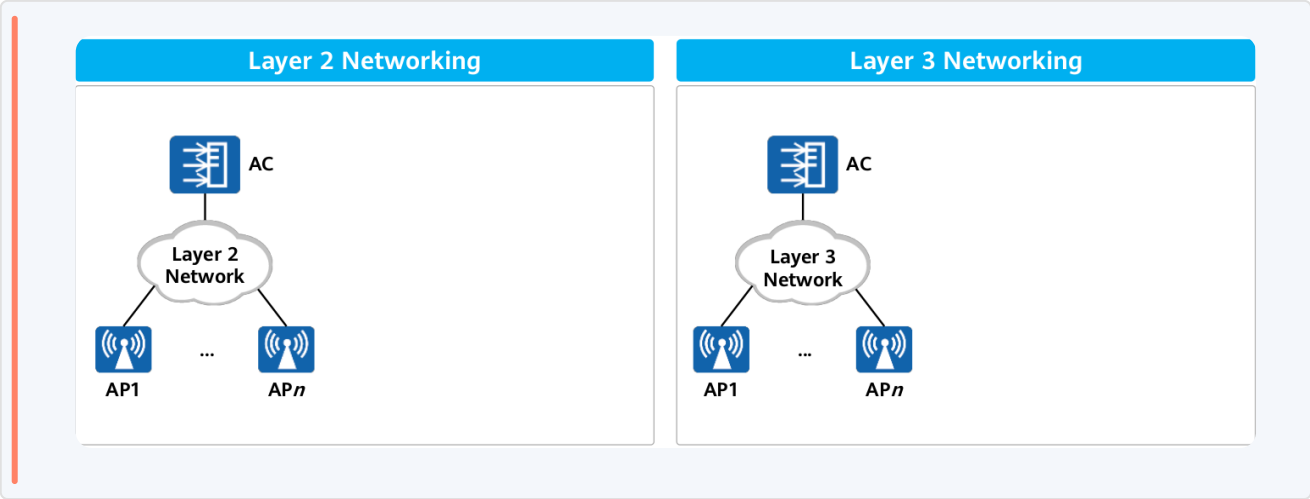
> **A station (STA)** in the context of 802.11 wireless networking refers to any device, like a laptop or smartphone, that has the capability to connect to a Wi-Fi

CAPWAP Port

- CAPWAP is an application-layer protocol based on **UDP** transmission.
- UDP port 5246 for transmitting control packets

- UDP port 5247 for transmitting data packets

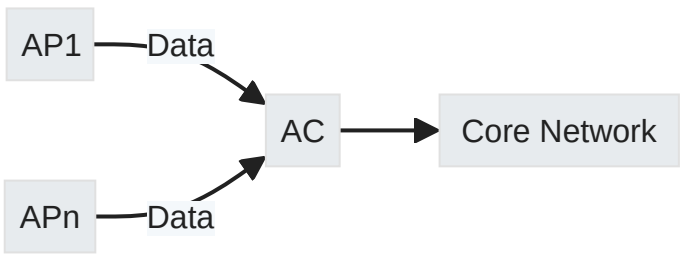
1.2.5 Networking Modes



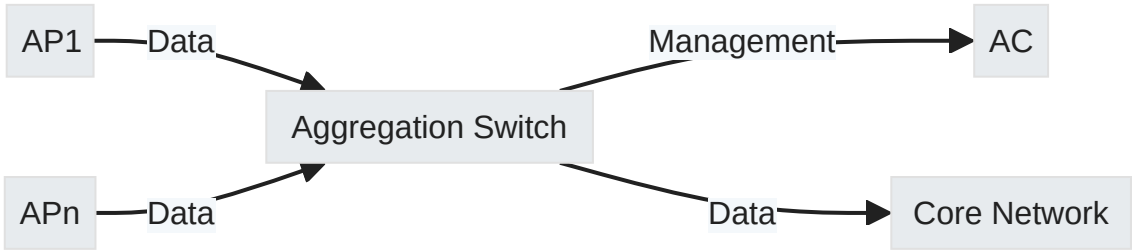
- Layer 2 networking: Access points (APs) connect directly or through a simple network to a controller, making setup fast and suitable for basic or short-term networks.
- Layer 3 networking: Access points (APs) connect through a more complex network to a controller, which is better for managing many APs over larger, more intricate networks.

1.2.6 AC Connection Mode

In-Path Connection Mode:
In in-path mode, the Access Controller (AC) is placed directly in the line of network traffic, meaning all user data flows through the AC.

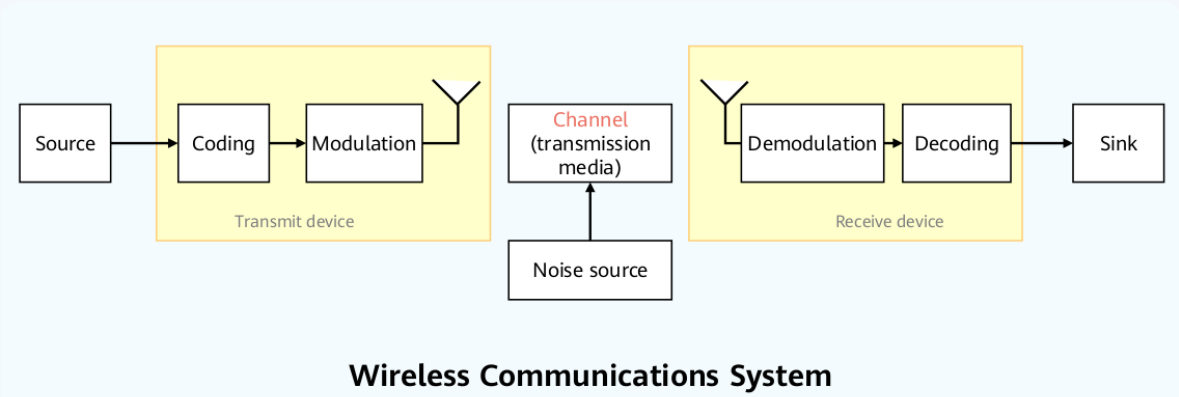


Off-Path Connection Mode:
In off-path mode, the Access Controller (AC) manages the network but does not handle data traffic; instead, data bypasses the AC and goes straight to the core network.



1.2.7 Wireless Communications System

1.2.7.1 Coding & Modulation Process:



Convert raw information into digital signals (source coding), then into radio waves through channel coding and modulation for transmission over air interfaces.

1.2.7.2 Radio Wave Spectrum Utilization

- 2.4 GHz frequency band (2.4–2.4835 GHz)

> - 5 GHz frequency band (5.15–5.35 GHz, 5.725–5.85 GHz)

For WLAN:

- **2.4 GHz Frequency Band:** Channels overlap; used for protocols like IEEE 802.11b/g/n/ax.
- **5 GHz Frequency Band:** Richer spectrum; supports wider channels; used for IEEE protocols including ac/ax.

> Radio channels are specific frequencies used to send information. To avoid interference, these frequencies are carefully divided. The 2.4 GHz band has 14 channels that can be close together and interfere (like channels 1 and 2) or far apart and not interfere (like channels 1 and 6). The 5 GHz band offers more options, including wider channels for more data.

1.2.8 BSS/SSID/BSSID Concepts

- **BSS (Basic Service Set):** A network area covered by a single access point (AP) where devices can connect and communicate wirelessly.
- **SSID (Service Set Identifier):** The name of a wireless network that helps users identify and connect to different WLANs.
- **BSSID (Basic Service Set Identifier):** The unique MAC address of an access point that distinguishes one WLAN from another within the same area.
- **ESS (Extended Service Set):** is a network of multiple Wi-Fi access points with the same SSID (network name) that allows devices to move around freely without losing their connection.

> Each BSS is identified by BSSID (MAC of the respective AP) while SSID is a human-readable identifier of a wireless network spanning across one or more BSSs forming an ESS for seamless roaming capability.

1.2.9 Virtual Access Points (VAP)

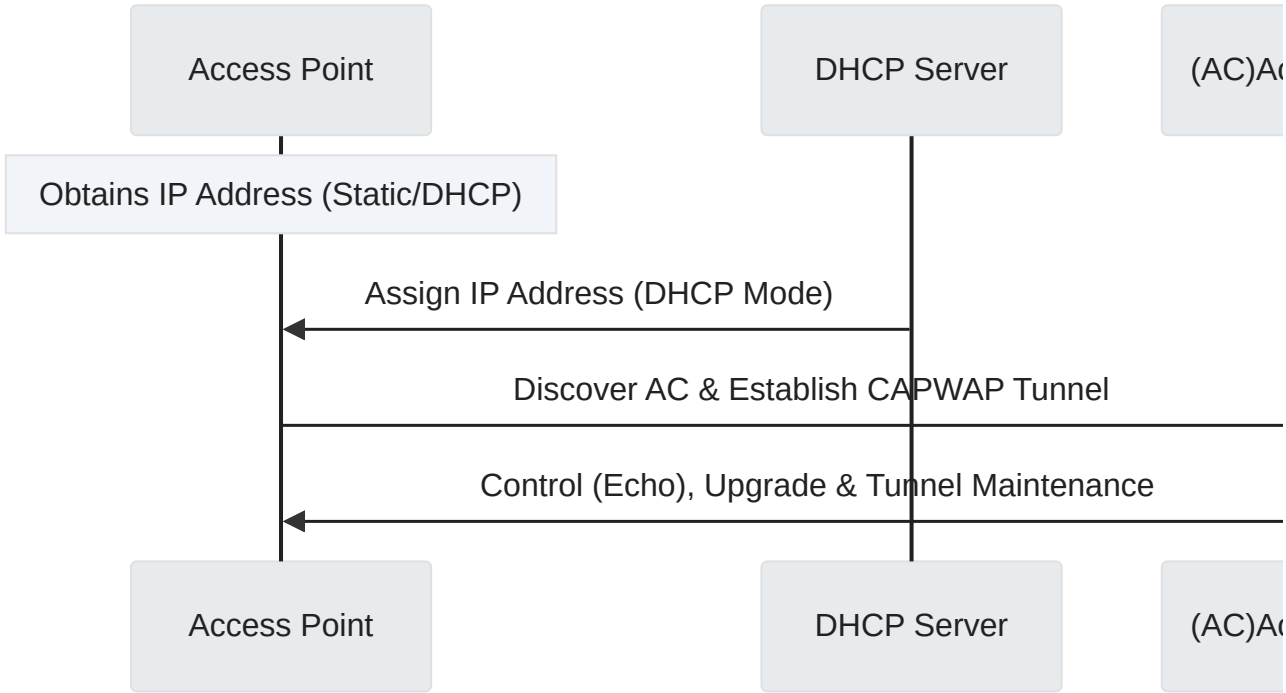
A single physical AP can be virtualized into multiple VAPs each serving different user groups with unique SSIDs but sharing hardware resources of the base physical unit.

1.3 WLAN Fundamentals

1.3.1 WLAN Working Process Overview

1.3.1.1 1. AP Onboarding

> An AP obtains an IP address, discovers an AC, and sets up a connection with the AC.



1.3.1.1.1 Steps:

---

1. Obtain IP Address.

> Access Points (APs) must first obtain an **IP** address, either **statically** or via **DHCP** from a **server**, **controller**, or **network device**. Once assigned an IP, the AP can communicate with the network controller to facilitate wireless connectivity and data management.

2. Discover AC & CAPWAP Tunnel Establishment.

Discover AC & CAPWAP

1. **AP Discovery**: APs locate an AC by either cycling through pre-configured AC IPs (**Static**) or using network services like **DHCP**, **DNS**, or **broadcasts** to find one (Dynamic).
2. **CAPWAP Tunnel Establishment**: APs and ACs establish a Data tunnel for device traffic and a Control tunnel for management communication via the CAPWAP protocol
   - **Data tunnel:** transmits service data packets from APs to the AC Datagram Transport Layer AP access control Security (DTLS) encryption can be enabled over the data tunnel to ensure security.
   - **Control tunnel:** transmits control packets between the AC and APs. DTLS encryption can be enabled over the control tunnel to ensure security

DHCP Mode Steps:

- DHCP Discover
- DHCP Offer (option 43)
- DHCP Request
- DHCP Ack (option 43)

In the absence of advanced DHCP or DNS services, the AP broadcasts discovery requests within the Layer 2 network to find any ACs ready to respond.

3. AP Access Control (Authentication).

Authentication

- APs request to join an AC by sending a **Join Request**, and the AC responds after authenticating the AP using **MAC address**, **serial number** (SN), or **no authentication**. If authenticated successfully, the AC establishes a connection with the AP either through **Manual configuration** , **automatic discovery** of whitelisted APs, or **manual confirmation**.
  - **Manual configuration:** Preconfigure MAC addresses and serial numbers (SNs) of APs on the AC for automatic connection when APs match the preset credentials in offline mode.
  - **Automatic discovery:** The AC automatically discovers and connects to APs that are set to non-authentication mode or whitelisted under MAC or SN authentication.
  - **Manual confirmation:** If the AP uses MAC or SN authentication and isn't imported offline or whitelisted, it's listed as unauthorized by the AC, requiring manual confirmation to activate.

4. Optional AP Upgrade.

AP Upgrade

The AP communicates with the AC to verify software version and, if an update is required, it requests and receives it automatically or through FTP/SFTP based on security requirements, followed by a restart and recheck for version.

There are different ways to upgrade:

- **Automatic upgrade:** This happens as soon as the AP connects to the AC for the first time or after being restarted once upgrade settings are in place.
- **AC mode:** Used for a few APs, where they get updates directly from the AC.
- **FTP mode:** Used when security isn't a major concern; updates are downloaded from an FTP server in plain text.
- **SFTP mode:** Used when security is important; updates are downloaded from an SFTP server with encryption and security protections.
- **In-service upgrade:** For APs that are already online and providing Wi-Fi service without interrupting that service too much.
- **Scheduled upgrade:** Also for online APs, done during times when network use is low to avoid disrupting users.

5. CAPWAP Tunnel Maintenance.

CAPWAP Mainternance

- **Data tunnel maintenance:**
  - The AP and AC exchange Keepalive packets (through the UDP port **5247**) to detect the data tunnel connectivity.
- **Control tunnel maintenance:**
  - The AP and AC exchange Echo packets (through the UDP port **5246**) to detect the control tunnel connectivity.

1.3.1.1.1.1 Preconfigurations on AC for AP Onboarding:

- Configure network connectivity.

> AC can function as a DHCP server.

- Create an AP group.

> Group similar APs together in an AP group for easier management.

- Configure country code (regulatory domain profile).
- Configure source interface/address for establishing CAPWAP with AP.

1.3.1.2 2. WLAN Service Configuration Delivery

After AP goes online:

- AC sends a Configuration Update Request to the AP.
- Upon response, AC delivers service configurations to the AP.

1.3.1.2.1 WLAN Profiles:

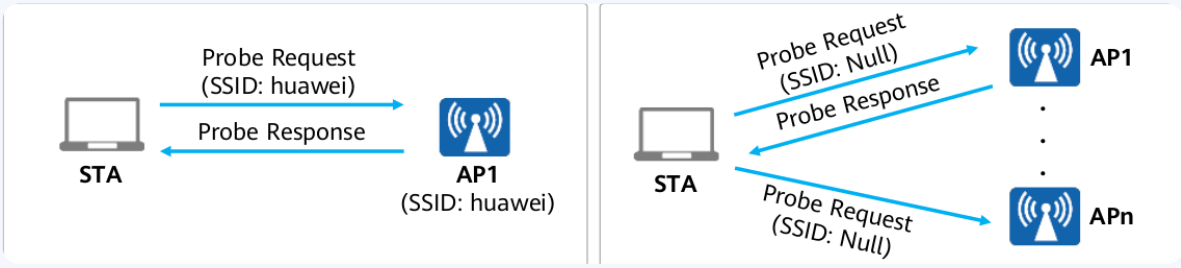
Profiles include regulatory domain profile, radio profile, VAP profile, etc.

- **Regulatory Domain Profile:** Configures country code and radio attributes.
- **Radio Profile:** Optimizes radio parameters like channel and power settings.
- **VAP Profile:** Creates Virtual Access Points with SSID and security settings.

1.3.1.3 3. STA Access

STA access process involves:

1. Scanning for SSID.



Scanning

- **Active Scanning**: A STA searches for wireless networks by broadcasting Probe Request frames.
  - **With SSID**: Searches for an AP with a matching SSID.
  - **Without SSID**: Broadcasts to find what wireless services are available.
- **Passive Scanning**: A STA listens for Beacon frames from APs to discover networks.

> APs send Beacon frames at intervals of 100 TUs (1 TU = 1024 microseconds) by default.

2. Link authentication with the network.

authentication modes:

- Involves two modes:
  - **Open System Authentication**: No actual authentication, any STA can connect.
  - **Shared Key Authentication**: Requires a pre-configured shared key on both STA and AP.

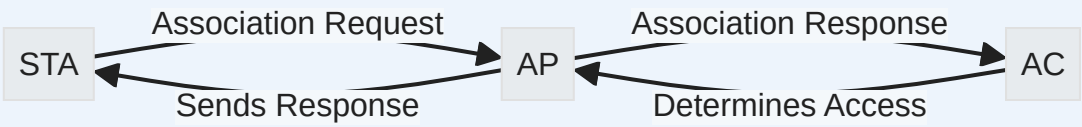
TIP

link authentication is about establishing a basic connection between your device and the network, whereas access authentication involves proving your identity and securing communication within that network after you're connected.

3. Association with the wireless network (SSID).

Association

- Occurs after successful link authentication.
- It's a service negotiation process (rate, channel, etc.).



> like agreeing on the rules of conversation before starting to chat

4. Access authentication process (like WPA/WPA2).

Note

- Differentiates users and controls access rights, more secure than link authentication.
- **Modes:** PSK authentication, 802.1X authentication.
- Ensures data security through encryption (e.g., WEP, WPA/WPA2).

5. Obtaining IP address via DHCP.

IP

- STAs need IP addresses to connect properly.
- DHCP servers assign IP addresses.

> AC or aggregation switch can function as a DHCP server

> Previous steps doesn't need ip to communication its need just MAC

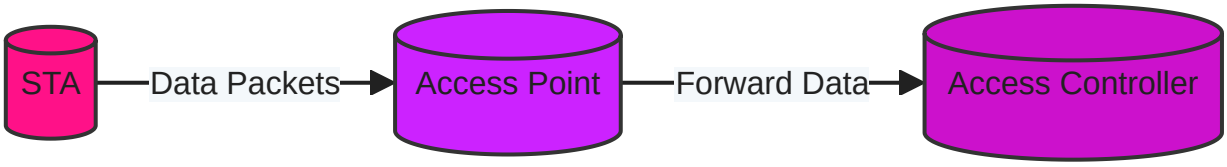
6. User authentication for network access control if applicable.

User Authentication

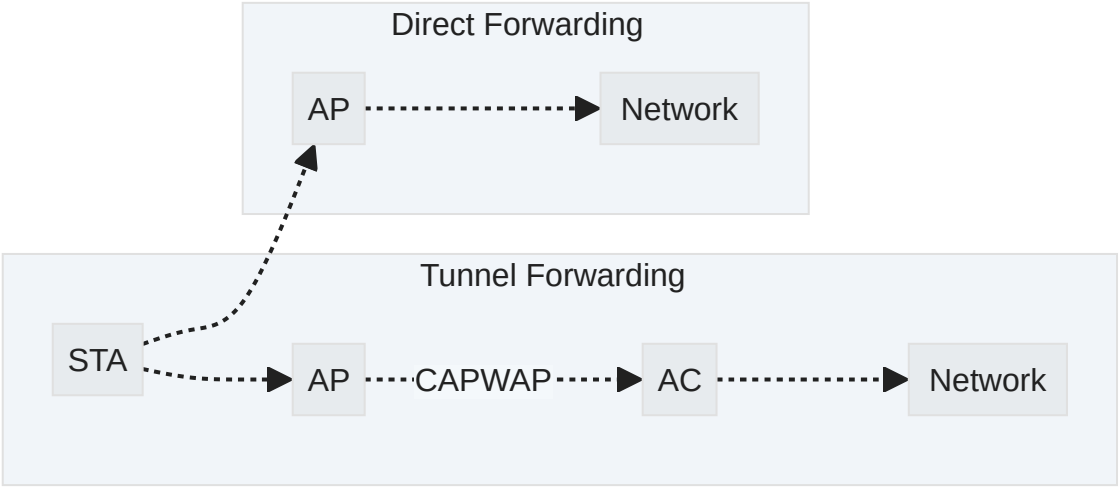
Users must authenticate on web portals before accessing the Internet.

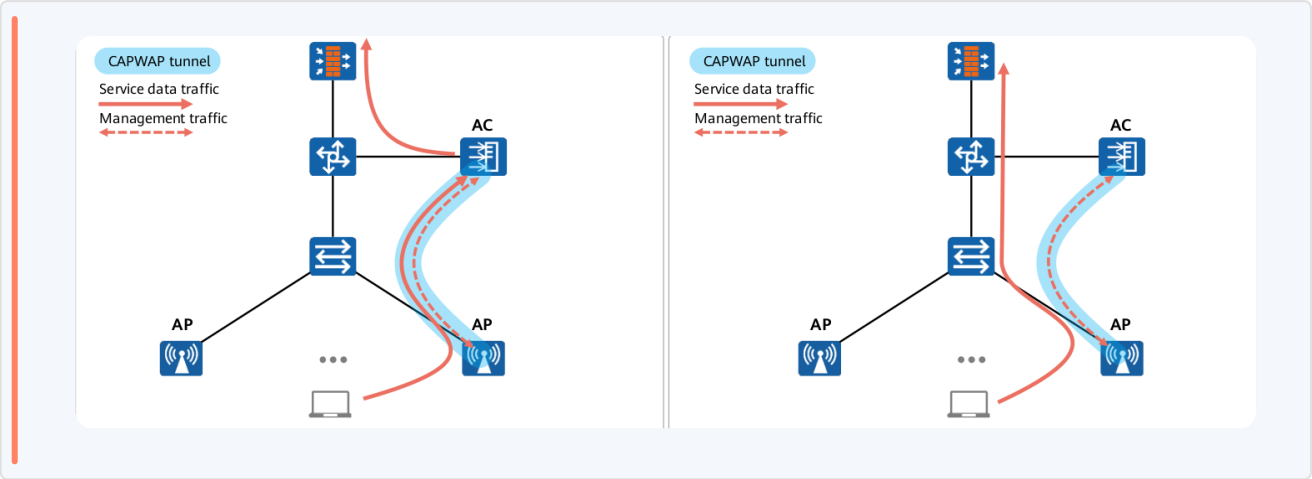
Policy	Link Auth	Access Auth	Data Encryption	Description
WEP	Open system	N/A	No encryption or WEP	Insecure
WEP	Shared-key Authentication	N/A	WEP	Insecure
WPA/WPA2-802.1X	Open system	802.1X (EAP)	TKIP or CCMP	A more secure policy, applicable to large enterprises
WPA/WPA2-PSK	Open system	PSK	TKIP or CCMP	More secure policy, applicable to small- and medium-sized enterprises or household users

1.3.1.4 4. WLAN Service Data Forwarding



1.3.1.4.1 Data Forwarding Modes:





Tunnels Forwarding :

- All data packets are forwarded through an AC.
- More secure but less efficient due to added Load on AC.

Direct Forwarding:

- More efficient as it bypasses the AC for data forwarding since data sent directly upper layer network without encapsulating them over a CAPWAP data tunnel.

1.4 WLAN Configuration Implementation

1.4.1 Basic WLAN Configuration Commands

1.4.1.1 Configuring an AP to Go Online

1.4.1.1.1 AP Onboarding

- Configure the AC as a DHCP server with Option 43.

```markdown
[AC-ip-pool-pool1] option <code> sub-option <sub-code> ascii <ascii-string>||hex <hex-string>||cipher <cipher-string>||ip-address <ip-address>
```

More Details

- `<code>`
  - You're telling the DHCP server (the AC in this case) to include additional configuration information (Option 43) in its responses.
- `<sub-code>`
  - Within this extra information, you can have various pieces each tagged with a different sub-option code.
- `<ascii-string>`
  - The actual content of these pieces can be written out as readable text using ASCII encoding.

- Create a regulatory domain profile and set the country code.

```markdown
[AC-wlan-view] regulatory-domain-profile name <profile-name>
[AC-wlan-regulate-domain-profile-name] country-code <country-code>
```

> Profile name It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

> Country code such as CN (default value): China , AU: Australia ,etc

- Create an AP group and bind regulatory domain profile.

```markdown
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] regulatory-domain-profile <profile-name>
```

> **group name:** It cannot contain question marks (?), slashes (/), or spaces, and cannot start or end with double quotation marks (").

- Configure source interface or address for CAPWAP.

```markdown
[AC] capwap source interface loopback <loopback-number>||vlanif <vlan-id>
```

```markdown
[AC] capwap source ip-address <ip-address>
```

- AP authentication

```markdown
[AC-wlan-view] ap auth-mode mac-auth||sn-auth
```

> AP authentication by default, MAC address authentication is used.

- Add APs in offline mode using MAC or SN authentication.

```markdown
[AC-wlan-view] ap-id <ap-id> type-id <type-id>||ap-type <ap-type> ap-mac <ap-mac>||ap-sn <ap-sn>
[AC-wlan-ap-ap-id] ap-name <ap-name>
```

> **ap-id:** ranges from 0 to 8191.

> **type-id:** ranges from 0 to 255.

> **ap-type:** ranges from 1 to 31 characters.

> **ap-sn:** ranges from 1 to 31 characters, and can contain only letters and digits.

- Add the AP to an AP group.

```markdown
[AC-wlan-view] ap-id 0
[AC-wlan-ap-0] ap-group <ap-group>
```

- Verifying Configuration

```markdown
[AC] display ap all||ap-group <ap-group>
```

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
Extra information:
P  : insufficient power supply
--------------------------------------------------------------------------------------------------------------
ID   MAC               Name      Group      IP              Type        State STA Uptime     ExtraInfo
--------------------------------------------------------------------------------------------------------------
0    60de-4476-e360    area_1    ap-group1  10.23.100.254   AP5030DN    nor   0   10S        -
--------------------------------------------------------------------------------------------------------------
Total: 1
```

AP State

- **State:** AP state.
  - **normal:** An AP has gone online on an AC and is working properly.
  - **commit-failed:** WLAN service configurations fail to be delivered to an AP after it goes online on an AC.
  - **download:** An AP is in upgrade state.
  - **fault:** An AP fails to go online.
  - **idle:** It is the initialization state of an AP before it establishes a link with the AC for the first time.

1.4.1.2 Configuring Radios

- Enter Radio View

```markdown
[AC-wlan-view] ap-id <ap-id>
[AC-wlan-ap-0] radio <radio-id>
```

- Configure Bandwidth and Channel

```
[AC-wlan-radio-0/0] channel <20mhz>||<40mhz-minus>||<40mhz-plus>||<80mhz>||<160mhz> <channel_number>
```

- Set Antenna Gain

```
[AC-wlan-radio-0] antenna-gain <antenna-gain-in-dB>
```

> **antenna-gain:** ranges from 0 to 30, in dB.

- Configure the transmit power for a radio.

```
[AC-wlan-radio-0/0] eirp <eirp>
```

> eirp ranges from 1 to 127, in dBm.

- Configure the radio coverage distance.

```
[AC-wlan-radio-0/0] coverage distance <distance>
```

> distance ranges from 1 to 400, in 100 meters.

- Configure the operating frequency for a radio.

```
[AC-wlan-radio-0/0] frequency 2.4g||5g
```

> By default, radio 0 works on the 2.4 GHz frequency band, and radio 2 works on the 5 GHz frequency band.

- Create a radio profile.

```markdown
[AC-wlan-view] radio-2g-profile name <profile-name>
```

> **profile name:** It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

- Bind the radio profile.

```markdown
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] radio-2g-profile <profile-name> radio <radio-id>||all
```

> **radio-id:** can be 0 or 2.

1.4.1.3 Configuring VAPs (Virtual Access Points)

- Create VAP Profile

```markdown
[AC-wlan-view] vap-profile name <profile-name>
```

- Set Data Forwarding Mode

```markdown
```

```
[AC-wlan-vap-prof-profile-name] forward-mode direct-forward||tunnel
```

- Configure service VLANs

```Markdown
[AC-wlan-vap-prof-profile-name] service-vlan vlan-id <vlan-id>||vlan-pool <pool-name>
```

- Configure a security profile.

```Markdown
[AC-wlan-view] security-profile name <profile-name>
```

> By default, security profiles **default**, **default-wds**, and **default-mesh** are available in the system.

```Markdown
[AC-wlan-view] vap-profile name <profile-name>
[AC-wlan-vap-prof-profile-name] security-profile <profile-name>
```

> Bind the security profile to the VAP profile.

- Configure an SSID profile

```Markdown
[AC-wlan-view] ssid-profile name <profile-name>
```

> By default, the system provides the SSID profile **default**.

```Markdown
[AC-wlan-ssid-prof-profile-name] ssid <ssid>
```

> By default, the SSID **HUAWEI-WLAN** is configured in an SSID profile.

> string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters.

Note

To create a Wi-Fi name that begins with a space, put it in quotes like " hello". Quotes count as two extra symbols. To start with a quote, use a backslash before it, like "hello. The backslash counts as one extra symbol.

Markdown

```
[AC-wlan-view] vap-profile name <profile-name>
[AC-wlan-vap-prof-profile-name] ssid-profile <profile-name>
```

> Bind the SSID profile to the VAP profile.

- Bind the VAP profile

Markdown

```
[AC-wlan-view] ap-group name <group-name>
[AC-wlan-ap-group-group-name] vap-profile <profile-name> wlan <wlan-id> radio <radio-id>||all service-vlan vlan-id <vlan-id>||vlan-pool <pool-name>
```

> Bind the specified VAP profile to radios in an AP group.

- Check VAP information.

Markdown

```
[AC] display vap ap-group <ap-group-name>||{ap-name <ap-name>||ap-id <ap-id>} radio <radio-id> ssid <ssid>
```

```
[AC] display vap all||ssid <ssid>
```

```
[AC-wlan-view] display vap ssid wlan-net
WID : WLAN ID
--------------------------------------------------------------------------------------------------------------
AP ID      AP name    RfID  WID   BSSID              Status  Auth type        STA   SSID
--------------------------------------------------------------------------------------------------------------
0          area_1     0     1     60DE-4476-E360     ON      WPA/WPA2-PSK     0     wlan-net
0          area_1     1     1     60DE-4476-E370     ON      WPA/WPA2-PSK     0     wlan-net
--------------------------------------------------------------------------------------------------------------
Total: 2
```

Display information about service VAPs.

1.5 Next-Generation WLAN Solutions

1.5.1 Huawei WLAN Solutions Overview

1.5.1.1 All-scenario Solutions

- Customized solutions for varied application scenarios.
- Comprehensive deployment and management for campus and branch networks.

1.5.1.2 High Bandwidth

- Support for 802.11ac Wave 2 protocol.
- Dual-5G radio coverage with wireless access bandwidth up to 3.46 Gbps.
- Enhancements to Wi-Fi 6 with single 5 GHz radio rate up to 9.6 Gbps.

- Roaming support and multiple wireless QoS protocols like WMM.

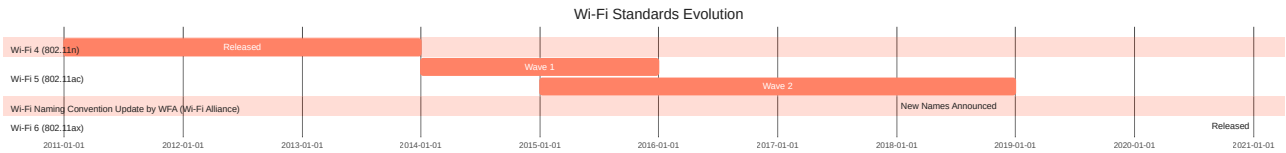
1.5.1.3 High Security

- Mainstream authentication and encryption modes, such as WPA, WPA2, WPA3, and WAPI

1.5.1.4 Easy Deployment

- APs support plug-and-play, automatic upgrade, and dynamic adjustments. Also compatible with IoT integration and offer cloud management capabilities.

1.5.2 Wi-Fi Generations Timeline



1.5.2.1 Application Development & Bandwidth Requirements

Year	Applications	Bandwidth/User	Latency
Pre-2018	HD Video/Social Networking	2-4 Mbps	<50 ms
Pre-2020	Video Surveillance/E-Classroom	4-12 Mbps	<30 ms
Post-	Interactive VR/AR/4K Video	>50 Mbps	<10 ms

Year	Applications	Bandwidth/User	Latency
2020	Conferencing		

1.5.2.2 Comparison: Wi-Fi 6 Vs. Wi-Fi 5

Feature	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)
Maximum Bandwidth	Up to 3.5 Gbps	Up to 9.6 Gbps
Concurrency Rate	Supports up to ~100 devices per access point	Supports up to ~400 devices per access point
Latency	Average latency about 30 ms	Service latency reduced to ~20 ms
Power Consumption	Standard power consumption	Up to 30% reduction in power consumption with TWT
Frequency	Primarily operates on 5 GHz band	Operates on both 2.4 GHz and 5 GHz bands
Modulation	Up to 256-QAM	Up to 1024-QAM
MU-MIMO	Supports MU-MIMO for downlink only	Supports MU-MIMO for both uplink and downlink
OFDMA	Not supported	UL/DL OFDMA supported
Spatial Reuse	Limited	Enhanced with BSS Coloring
Target Wake Time (TWT)	Not supported	Supported

Note

> **Power Consumption**: The introduction of TWT in Wi-Fi 6 helps devices conserve power by scheduling wake times.

> **Modulation**: Higher-QAM allows for denser data transmission in good signal conditions.

MU-MIMO: Multi-user, multiple-input, multiple-output technology enables more efficient data transmission for multiple devices concurrently.

OFDMA: Orthogonal frequency division multiple access allows the splitting of channels into smaller sub-channels, improving efficiency particularly in dense environments.

Spatial Reuse: Techniques like BSS Coloring in Wi-Fi 6 help reduce interference from neighboring networks.

Target Wake Time (TWT): This feature helps manage when clients need to wake up and communicate with the AP, reducing power usage.

1.5.3 Next-generation Campus Networks

1.5.3.1 Small-and-Medium-Sized Intent-driven Campus

1.5.3.1.1 Cloud Management Platform Benefits:

- Using a cloud management platform makes it easier and cheaper to handle all your devices from one place.

1.5.3.1.2 Advantages over AC + Fit AP Architecture:

- Cloud-based Wi-Fi architecture makes setting up and managing networks easier and cheaper by offering simple setup, centralized control, and built-in tools.

1.5.3.2 Medium-and-Large-Sized Intent-driven Campus

1.5.3.2.1 Native AC Architecture Characteristics:

- iMaster NCE Simplifies the management of wireless access points and wired networks using advanced data analysis and artificial intelligence to create easy-to-use, smart, and secure networks for medium to large businesses.

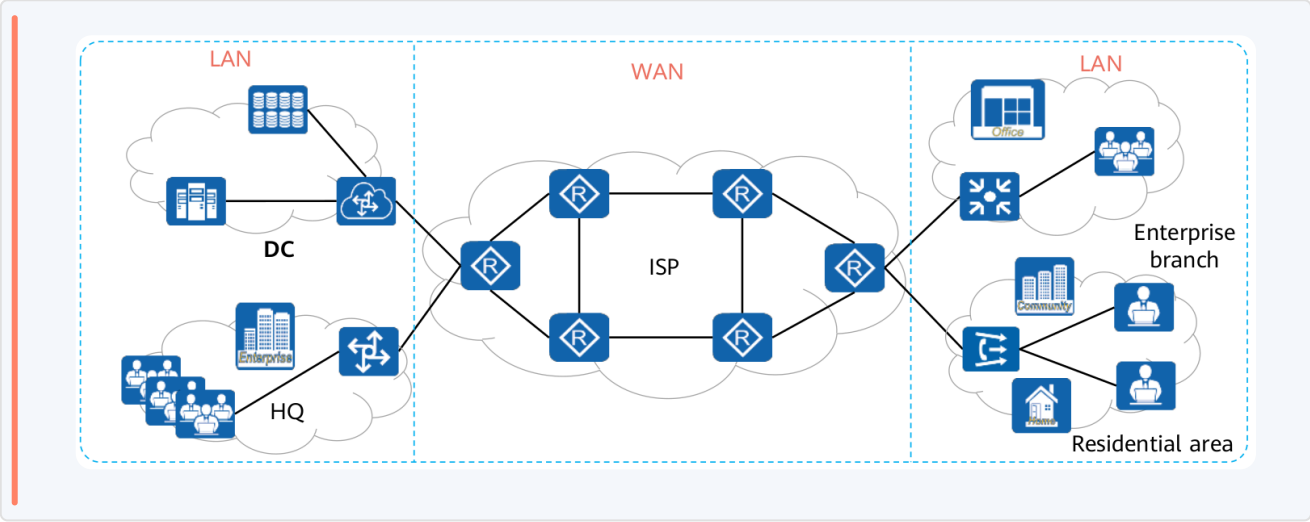
WAN Technologies

1 WAN Technologies

1.1 Overview of Early WAN Technologies

1.1.1 Definition of WAN

- **WAN** stands for Wide Area Network.
- Connects LANs across wide geographical areas (cities, countries, continents).
- Enables long-distance communication and international remote networking.



1.1.1.1 Differences Between WAN and LAN

LAN

- Covers a small geographical area.
- High bandwidth, short transmission distance.
- **Devices used:** mainly switches.
- Belongs to an institute or organization.

WAN

- Covers a wide area (Renting ISP network or building private).
- Lower bandwidth compared to LANs, covers long distances.
- **Devices used:** mostly routers.
- Services often provided by ISPs.

Other Points:

- Different protocols at the physical and data link layers.
- Private networks of banks, governments are also WANs.

> because they connect multiple locations across cities, states, or even countries. These organizations need to share data and resources securely over long distances, so they use WANs to ensure their employees and branches can communicate and access the same information regardless of their physical location.

1.1.2 Overview of Early WAN Technologies

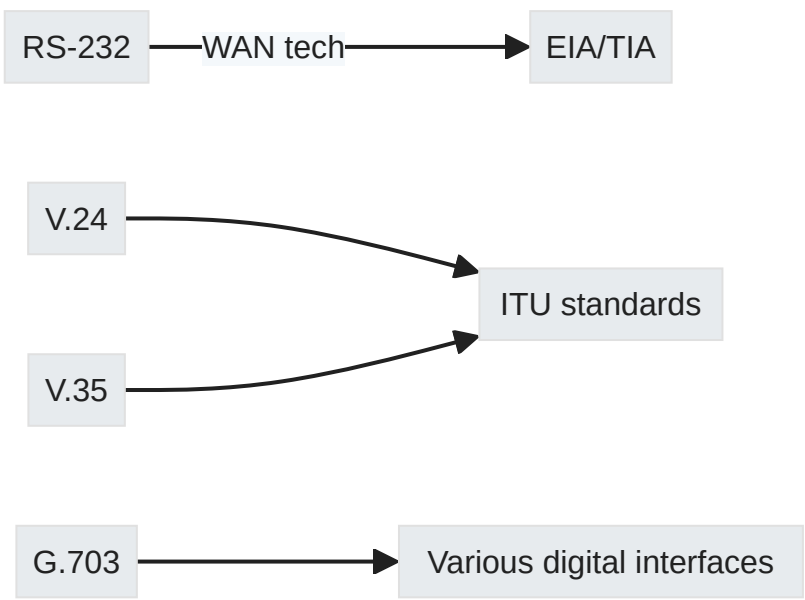
1.1.2.1 TCP/IP reference model layers:

- **LAN technologies**
  - IEEE 802.3/4/5/11

- **WAN technologies**
  - PPP
  - HDLC
  - Frame Relay
  - ATM
  - RS-232
  - V.24
  - V.35
  - G.703

> The early WANs and LANs differ in the data link layer and physical layer and are the same in the other layers in the TCP/IP reference model.

1.1.2.2 Early WAN Physical Layer Standards



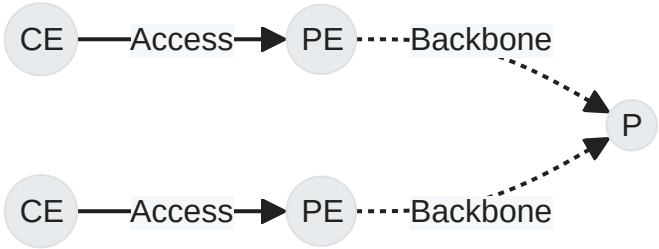
1.1.2.3 Early WAN Data Link Layer Standards

Protocol	Description
HDLC	Data packets encapsulated into frames; high reliability but lower efficiency; do not support IP address negotiation and authentication
PPP	Supports authentication; used on synchronous/asynchronous links
FR	Switched protocol with error-free check mechanism
ATM	Connection-oriented technology; uses 53-byte cells for information transmission

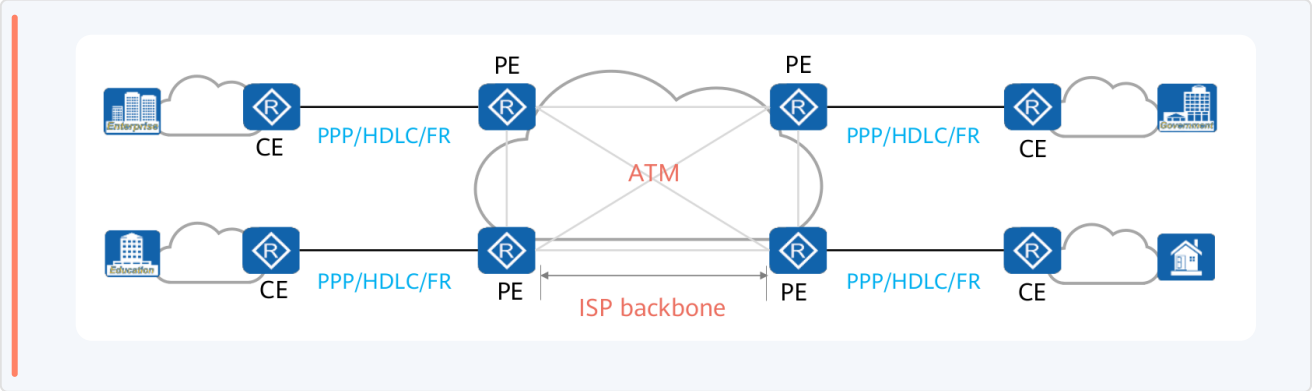
1.1.3 WAN Device Roles

1.1.3.1 Basic Roles:

1. **CE (Customer Edge)**: Located at customer premises; connects to PEs.
2. **PE (Provider Edge)**: Service provider's edge device; connected to CEs and Ps.
3. **P (Provider)**: Part of service provider's network; not connected to any CEs.



1.1.4 Application of Early WAN Technologies



1.1.4.1 Encapsulation Types:

Connection Type	Encapsulation Protocol
CE to PE	PPP/HDLC/FR

1.1.4.2 Usage:

- PPP/HDLC/FR used between CEs and PEs for user packet transmission over a WAN.
- ATM commonly employed on ISP backbone networks for high-speed forwarding.

1.2 PPP Implementation and Configuration

1.2.1 PPP Implementation

1.2.1.1 Key Concepts

PPP (Point-to-Point Protocol) is a widely used protocol for establishing direct connections between two networking nodes. It operates at the data link layer and

provides multiple features such as authentication, encryption, and compression.

PPP Details overview

> When you set up a PPP link between two routers, you're creating a logical direct connection between them, which means that for the purposes of the PPP session, it's as if there's a straight line connecting the two.

> Even though in the real world, your data goes through lots of different equipment like switches and routers to get from one place to another, PPP makes it look like there's just one simple connection.

- Here's how it works in practice:
  - **DTE and DCE Roles**: Your home router serves as a DTE, interfacing with your ISP's DCE equipment, which facilitates the connection to the wider network.
  - **PPP Encapsulation**: PPP wraps data packets in its own frame structure for transmission over the physical network links.
  - **Network Transparency**: Intermediate devices like switches and routers are transparent to PPP, meaning they forward frames without altering PPP data.
    - Switches forward PPP frames based on hardware addresses without decrypting IP payloads, treating them like any other Layer 2 frame.
    - Routers inspect IP headers within PPP frames to route packets based on IP addresses, after which they re-encapsulate them for transmission.
  - **Logical Link Perception**: Despite multiple physical components in the network path, PPP treats this chain as a singular logical link between endpoints.

Advantages of ppp

1. PPP supports encapsulation of various network layer protocols over the same physical link.
2. LCP in PPP establishes, configures, and tests the data-link connection for reliability.
3. PPP provides authentication methods like PAP and CHAP to secure connections.
4. PPP features error detection mechanisms for identifying link issues such as dropped packets.
5. NCPs in PPP negotiate and configure settings for different network layer protocols on the link.
6. PPP is adaptable to multiple physical layers beyond serial connections, including fiber optics and satellite links.

1.2.1.2 PPP Link Setup Process

1.2.1.2.1 LCP (Link Control Protocol) Negotiation

- `LCP` is responsible for establishing, configuring, and testing the data link connection.
- Key parameters negotiated include MRU (Maximum Receive Unit) and authentication mode,magic number.

> The magic number detects loops by exchanging unique values between connected devices; if a device receives a packet with its own magic number since magic number is unique number, it knows the data has looped back. A loop can happen if the physical networking setup Accidentally creates a circular path for data, causing packets to travel in circles rather than reaching their destination.

1.2.1.2.2 Authentication Negotiation

- `PAP` (Password Authentication Protocol) involves a two-way handshake with credentials sent in clear text.
- `CHAP` (Challenge Handshake Authentication Protocol) uses a three-way handshake with encrypted (MD5{ID+random number+password}) credentials.

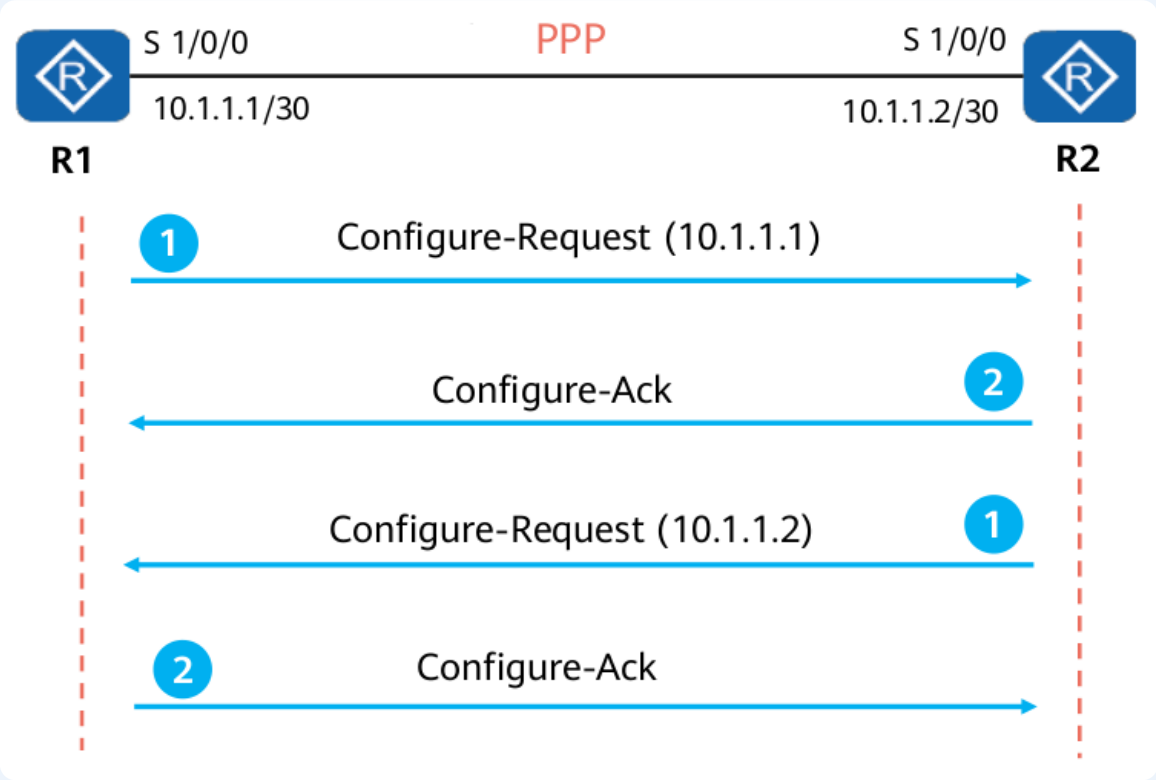
1.2.1.2.3 NCP (Network Control Protocols) Negotiation

- Responsible for selecting and configuring network layer protocols like IP.
- Examples include `IPCP` for IP address configuration.

Note

Static IP Address Negotiation Simplified:

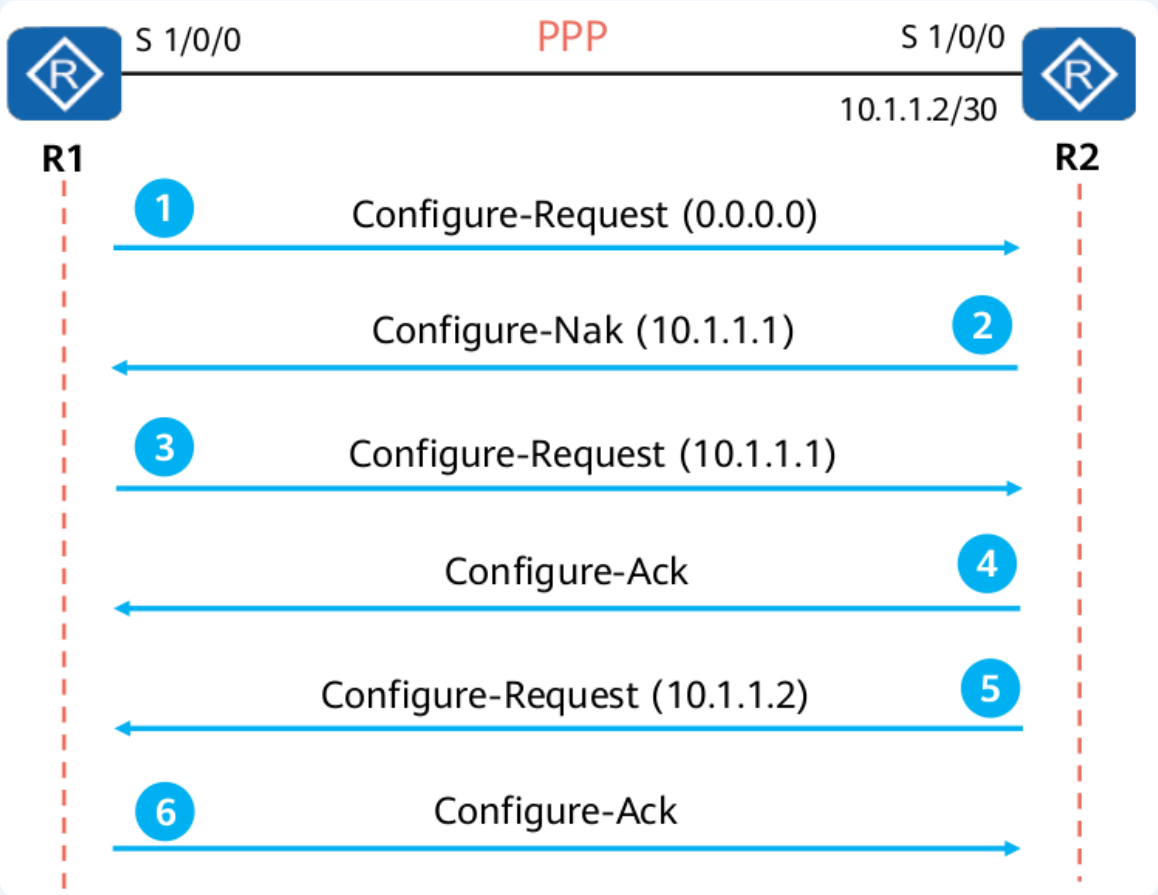
- Both devices manually configure and exchange their own static IP addresses; if there's no conflict, they acknowledge each other's address.



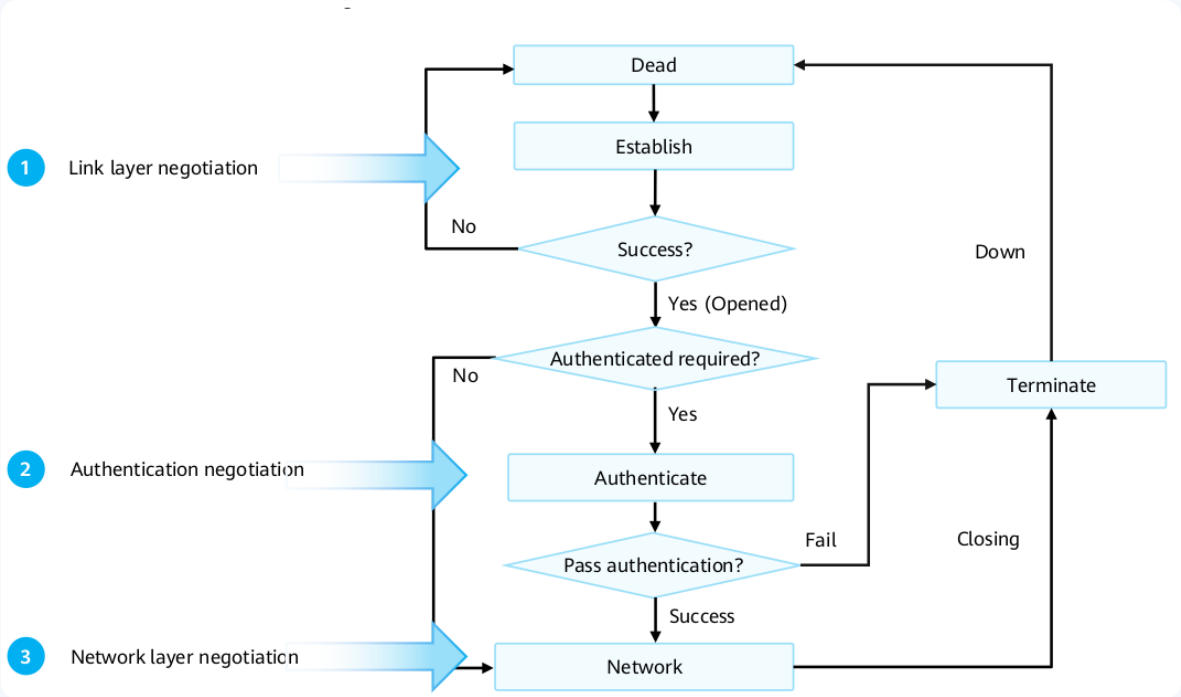
Dynamic IP Address Negotiation Simplified:

- One device requests an IP address by sending a request with no IP (0.0.0.0), the other assigns an available IP, and then both confirm the

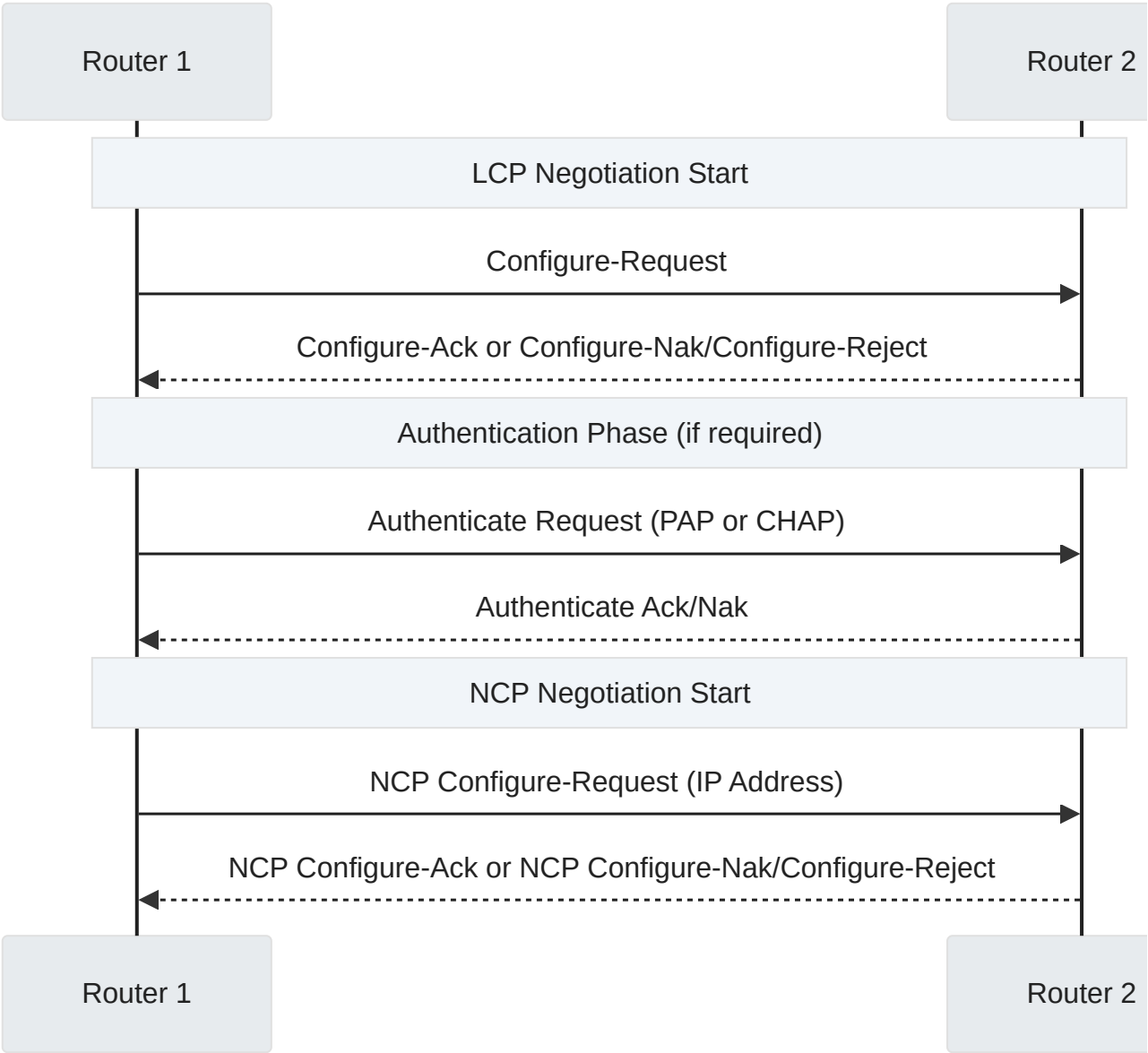
new address is acceptable.



1.2.1.3 State Machine of the PPP Link Interface



1.2.1.4 Configuration Exchange Process



1.2.1.5 Packet Structure

1.2.1.5.1 PPP Frame Format

Field	Description
Flag	Marks start/end of frame (`0x7E`)
Address	Broadcast address (`0xFF`)

Field	Description
Control	Unordered frame indicator (`0x03`)
Protocol	Indicates type of encapsulated packet
Information	Contains actual protocol data
FCS	Frame Check Sequence for error checking

> inside **Protocol**

Packet Type	Hexadecimal Code
IP packet	0x0021
IPCP packet	0x8021
LCP packet	0xC021
PAP packet	0xC023
CHAP packet	0xC223

1.2.1.5.2 LCP Packet Types

Code	Name	Content
0x01	Configure-Request	Request to start negotiation
0x02	Configure-Ack	Acknowledge negotiation success
0x03	Configure-Nak	Suggest alternative parameters
0x04	Configure-Reject	Reject unidentifiable parameters

1.2.1.6 Security Considerations

⚠ Note on Security

While MD5 is used in CHAP authentication, it has known security risks. It's recommended to use stronger algorithms like SHA256 or SHA3 for hashing

purposes. Encryption should be done using secure algorithms such as AES or RSA with key lengths of at least 2048 bits.

1.2.2 PPP Configuration

1.2.2.1 Basic PPP Functions

1.2.2.1.1 Encapsulation with PPP

- Change interface encapsulation protocol to PPP using:

```markdown
[Interface-Serial0/0/0] link-protocol ppp
```

1.2.2.1.2 Negotiation Timeout

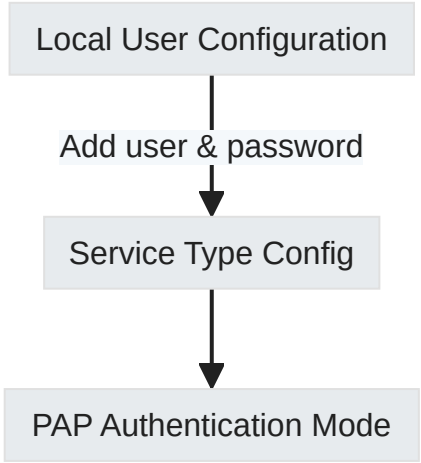
- Configure a negotiation timeout period (in seconds) with:

```markdown
[Interface-Serial0/0/0] ppp timer negotiate <seconds>
```

> **The negotiation timeout determines how long the device waits for a LCP reply before resending.**

1.2.2.2 PAP Authentication Configuration

1.2.2.2.1 Authenticator Setup



1. Add username and password:

```markdown
[AAA] local-user <user-name> password <cipher>|| <irreversible-cipher> <password>
```

- `<cipher>` : A Decipherable encryption method used to encrypt the user's password, allowing for potential decryption if necessary.
- `<irreversible-cipher>` : A one-way encryption method that secures the user's password without the possibility of decryption, enhancing security.

2. Set service type to PPP:

```markdown
[AAA] local-user <user-name> service-type ppp
```

3. Enable PAP authentication mode on interface:

```markdown
[Interface-Serial0/0/0] ppp authentication-mode pap
```

1.2.2.3 Peer Setup

Peer Interface Config —Set PAP credentials→ PAP Local User Config

- Configure peer's PAP credentials:

```markdown
[Interface-Serial0/0/0] ppp pap local-user <user-name> password <cipher>||<simple> <password>
```

- `<cipher>` : This parameter indicates that the `<password>` provided should be in an encrypted format, enhancing security.
- `<simple>` : This parameter signifies that the `<password>` is in plain text, which is simpler but less secure.

1.2.2.4 CHAP Authentication Configuration

1.2.2.4.1 Authenticator Setup (CHAP)

1. Add username and irreversible-ciphered password:

```markdown
[AAA] local-user <user-name> password <cipher>||<irreversible-cipher> <password>
```

- `<cipher>` : A Decipherable encryption method used to encrypt the user's password, allowing for potential decryption if necessary.
- `<irreversible-cipher>` : A one-way encryption method that secures the user's password without the possibility of decryption, enhancing security.

2. Set service type to PPP and enable CHAP on interface:

```markdown
[AAA] local-user <user-name> service-type ppp
[Interface-Serial0/0/0] ppp authentication-mode chap
```

1.2.2.5 Peer Setup (CHAP)

- Configure peer's CHAP username and password:

```markdown
[Interface-Serial0/0/0] ppp chap user <user-name>

[Interface-Serial0/0/0] ppp chap password <simple>||<cipher> <password>
```

- `<cipher>` : This parameter indicates that the `<password>` provided should be in an encrypted format, enhancing security.
- `<simple>` : This parameter signifies that the `<password>` is in plain text, which is simpler but less secure.

1.3 PPPoE Implementation and Configuration

1.3.1 PPPoE Overview

1.3.1.1 Overview

- PPPoE combines Ethernet and PPP (Point-to-Point Protocol).
- Allows multiple users to access the internet through a single physical connection, such as a modem or router.
- Provides user control and accounting features.
- Commonly used in DSL connections for user authentication and connection management.
    - DSL is a fast internet service that works over regular phone lines and lets you use the internet and make phone calls at the same time.

Example

Consider a street where all residents use one mailbox for sending and receiving mail:

- **PPPoE**: It's like each person having a special code on their letters that tells the mail carrier exactly which house it's from and where to deliver any incoming mail. This way, despite using one mailbox, everyone's correspondence is properly sorted and directed.

Purpose

- **Individual Accounts**: Each user gets a unique login for personalized access and usage tracking.
- **Security**: Incorporates encryption and authentication to keep user data protected during transmission.
- **Quality of Service**: Prioritizes data packets for efficient delivery, ensuring important information is transmitted swiftly.

1.3.1.2 Key Advantages

- Flexible networking (Ethernet)
- Authentication and accounting (PPP)

1.3.1.3 Frame Structure

Field	Description
DMAC	Destination MAC Address
SMAC	Source MAC Address
Eth-Type	EtherType (0x8863 or 0x8864)
PPPoE Header	Contains version, type, code, etc.
PPP Packet	Encapsulated PPP frame
FCS	Frame Check Sequence

1.3.1.3.1 Eth-Type code

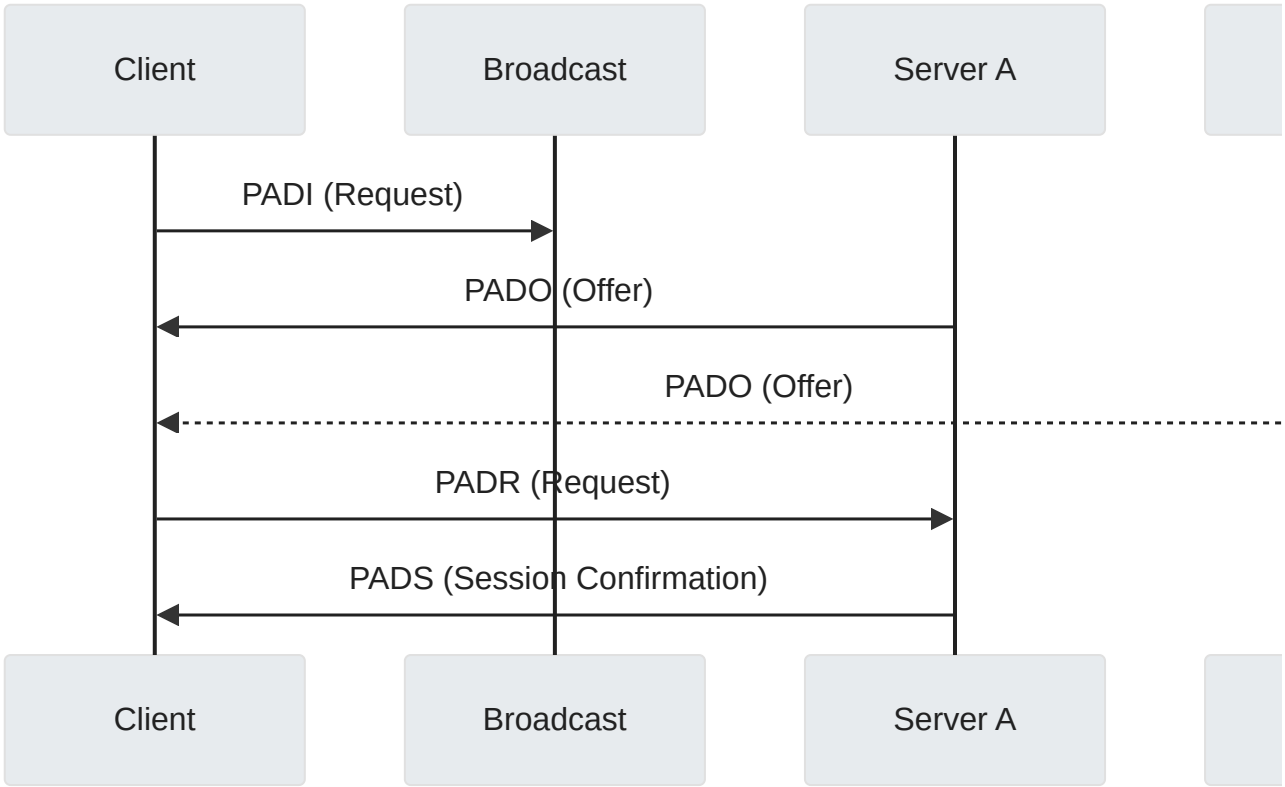
Code	Name	Description
0x09	PADI	PPPoE Active Discovery Initiation packet
0x07	PADO	PPPoE Active Discovery Offer packet
0x19	PADR	PPPoE Active Discovery Request packet
0x65	PADS	PPPoE Active Discovery Session-confirmation packet
0xa7	PADT	PPPoE Active Discovery Terminate packet

1.3.1.4 Session Establishment

> **PPPoE session establishment involves three stages:** PPPoE discovery, session, and termination stages.

1.3.1.4.1 Discovery Stage

> A PPPoE virtual link is created for user access.



1. The PPPoE client sends out a PADI packet to all potential servers asking for a connection.
2. A server that can provide the service responds to the client with a PADO packet.
3. The client picks the first server that replied and sends it a PADR packet to request a session.
4. The server accepts by sending back a PADS packet with a unique session ID to start the connection.

1.3.1.4.2 Session Stage

> PPP negotiation includes LCP negotiation, PAP/CHAP authentication, and NCP negotiation.

1. **LCP Negotiation:** Establish/configure link and verify the data link status.

2. **Authentication:** Usually via PAP or CHAP.
3. **NCP Negotiation:** Configures network layer protocols like IP addresses.

> After PPP negotiation succeeds, PPP data packets can be forwarded over the established PPP link. The data packets transmitted in this phase must contain the session ID determined in the discovery stage, and the session ID must remain unchanged.

1.3.1.4.3 Termination Process

- Either client or server can send a PADT packet to terminate the session.
- PADT carries the session ID to identify which session to terminate.

1.3.1.5 Application Scenarios

1.3.1.5.1 For Home Users:

Home devices installed with PPPoE client software dial up to access Internet services using unique account credentials provided by ISPs.

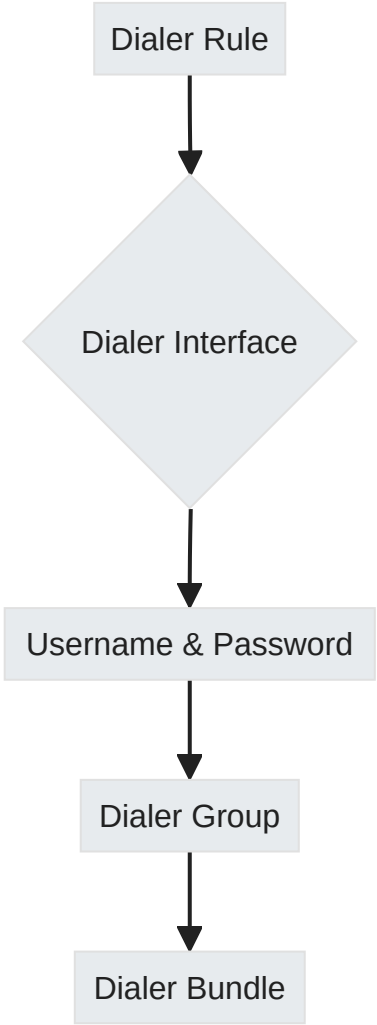
1.3.1.5.2 For Enterprises:

Multiple hosts use PPPoE connections managed by centralized server for secure access control and accounting.

1.3.2 Basic PPPoE Configuration

1.3.2.1 Configuration Steps

1.3.2.1.1 Step 1: Configure a Dialer Interface



Markdown

```
[Huawei] dialer-rule
[Huawei-Dialer1]dialer user <username>
[Huawei-Dialer1]dialer-group <group-number>
[Huawei-Dialer1]dialer-bundle <number>
[Huawei-Ethernet0/0/0]pppoe-client dial-bundle-number <number>
```

- `dialer-rule` command sets conditions for initiating a PPPoE session.
- `interface dialer number` creates a dialer interface.

- `dialer user username` configures the username for peer authentication.
- `dialer-group group-number` associates the interface with a dialer group.
- `dialer-bundle number` specifies a bundle associated with the physical interface.

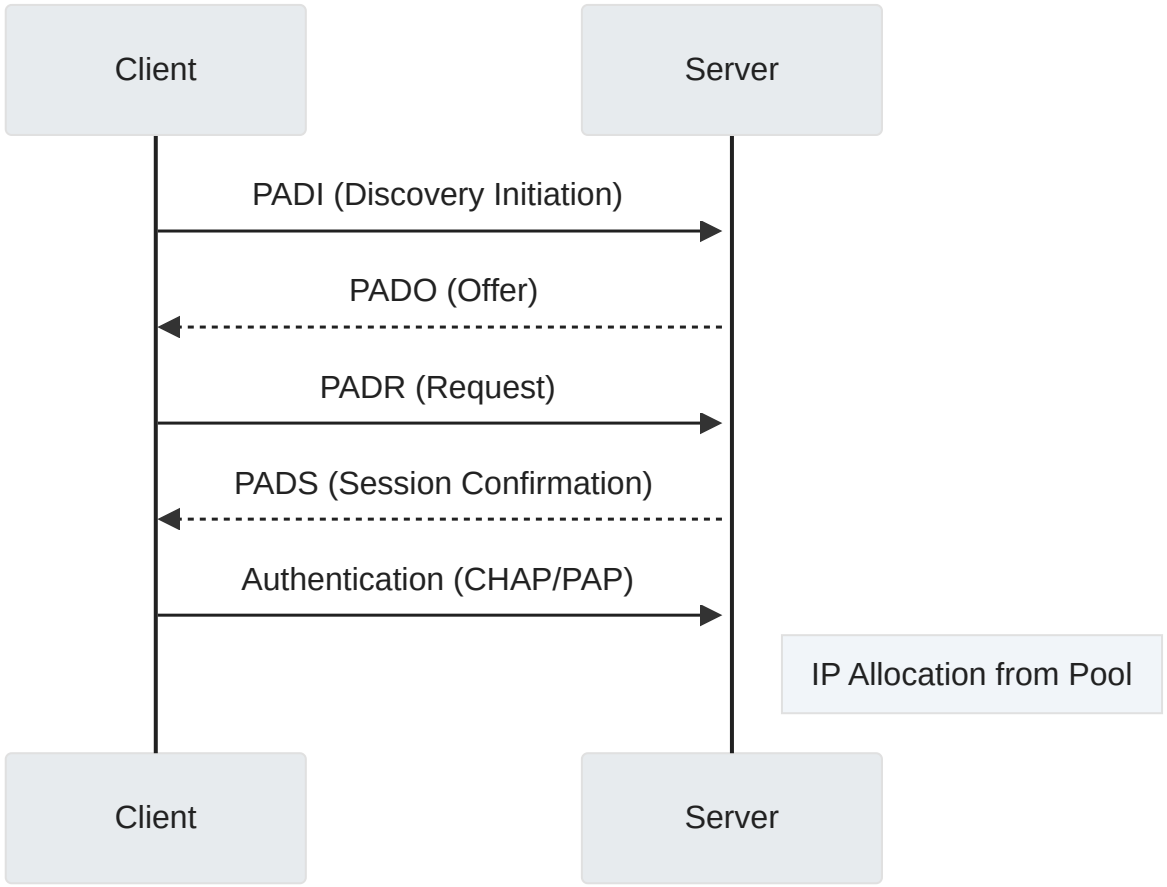
1.3.2.1.2 Verifying Configuration

Command	Description
`display interface Dialler number`	Shows configuration details of the Dialler interface
`display pppoe-client session summary`	Provides summary of current PPPoE client sessions

```
<R1>display interface Dialer 1
Dialer1 current state: UP
Line protocol current state: UP (spoofing)
Description: HUAWEI, AR Series, Dialer1 Interface
Route Port, The Maximum Transmit Unit is 1500, Hold timer
is 10(sec)
Internet Address is negotiated, 192.168.10.254/32
Link layer protocol is PPP
LCP initial
Physical is Dialer
Bound to Dialer1:0:
Dialer1:0 current state : UP
Line protocol current state : UP
Link layer protocol is PPP
LCP opened, IPCP opened
```

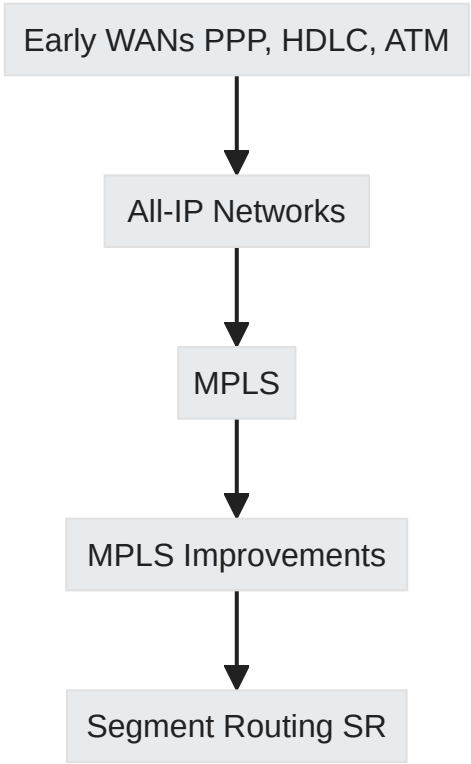
```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf      Client-MAC      Server-MAC     State
0      1       1    GE0/0/1  54899876830c  000000000000  IDLE
```

1.3.2.2 Client Connection Process



1.4 Development of WAN Technologies

1.4.1 Overview



Early WAN Protocols: PPP, HDLC, ATM were used in early WANs for data link layer communication.

Bottleneck: Traditional IP routing became a bottleneck due to software-based longest match rule leading to low forwarding performance.

1. **Computational Complexity**: Routers must search through numerous entries to find the longest IP address match, which is computationally demanding.
2. **Software-Based Processing**: Slower software processing on general-purpose CPUs handles the lookup instead of faster dedicated hardware.
3. **Scaling Issues**: Larger routing tables from network growth increase lookup times due to more potential matches.
4. **Lack of Optimization**: Traditional routing prioritizes flexibility and update ease over fast packet forwarding optimization.

MPLS Introduction: MPLS improved forwarding speed by parsing IP headers only at the edge and using labels for transit node forwarding.

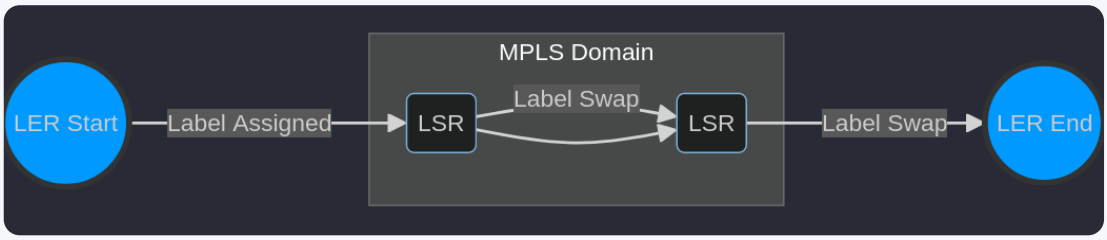
1. **Label Assignment and Switching**: Packets are assigned a label at the network edge that directs their path through routers without IP header analysis.
2. **Fixed-Length Labels**: Routers swiftly process packets based on fixed-length labels, avoiding the need for complex IP routing table lookups.
3. **Label Switched Paths**: Predefined paths, determined by network policies, direct labeled packets through the MPLS network efficiently.
4. **Efficient Use of Resources**: Core routers Speed up packet forwarding by using label information instead of deep packet inspection, conserving processing power.
5. **Fast Reroute Capabilities**: MPLS quickly reroutes traffic along alternate paths during failures without waiting for IP protocol convergence.

- MPLS speeds up the movement of data through a network by using labels instead of constantly checking where each data packet needs to go. This means that packets are moved along a predetermined path without the usual delay caused by each router figuring out the packet's route.
- This predetermined label-switched path allows for faster packet forwarding because each intermediate router does not need to perform a complex route lookup in its IP routing table; it merely looks up a simple label-to-label mapping in its MPLS table which takes less time and therefore speeds up packet forwarding through the network.

Extra

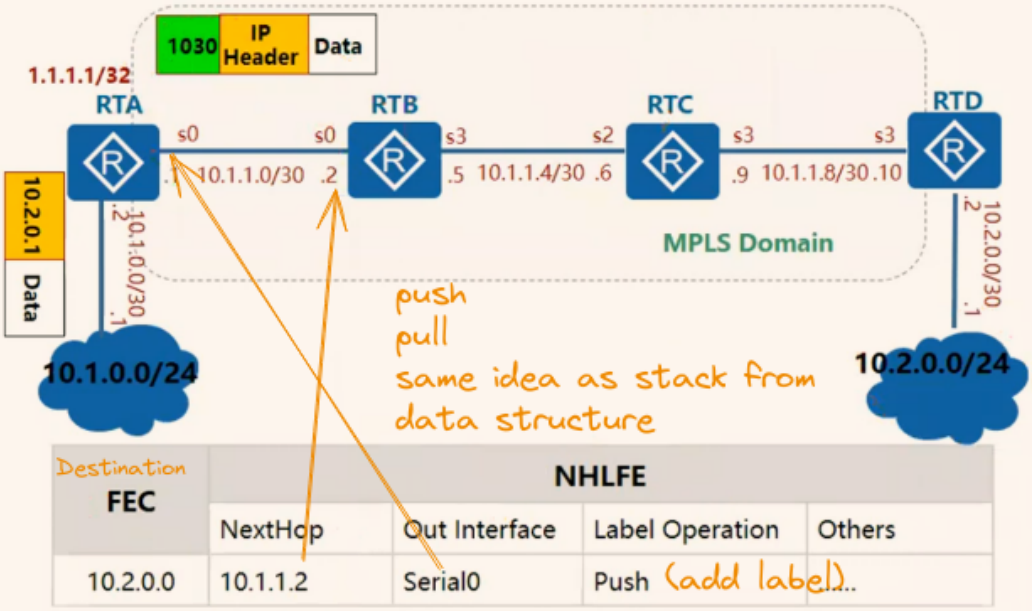
1. **LER (Label Edge Router)**: This is the router at the edge of an MPLS domain that makes decisions about which labels to assign to incoming packets based on their destination. It's where the MPLS paths begin and end.
2. **LSR (Label Switch Router)**: These are routers within the MPLS domain that route data based on the labels attached to packets, not the IP headers. They swap labels on the incoming packets with new labels before forwarding them towards their destination.

3. **LSP (Label Switched Path)**: This is essentially the path that a packet takes through an MPLS network, from one LER to another, traversing LSRs in between depend of IGP protocols.
4. **Label Distribution Protocol**: This protocol is used by routers in an MPLS network to share label mapping information with each other so they know how to properly forward labeled packets.
5. **Label Forwarding Table**: Each LSR maintains this table, which dictates how incoming labeled packets should be forwarded—by looking up the incoming label, determining what new label should replace it if necessary, and deciding which interface to send it out on.
6. **MPLS Header**: A 4-byte header
   - **Label Field**: A 20-bit field containing the label value.
   - **EXP (Experimental)**: A formerly experimental use field now often used for QoS priority marking; it's three bits in size.
   - **S (Bottom of Stack)**: A single bit indicating if this label is the last in the stack; S=1 means this is the bottom label.
7. **FEC (Forward Equivalence Class)**: This term describes a group of IP packets that are forwarded in the same manner, over the same path, and with the same forwarding treatment.
8. **NHLFE (Next Hop Label Forwarding Entry)**: This contains information necessary for forwarding labeled packets, including next hop IP address and operation on labels such as push, pop or swap.

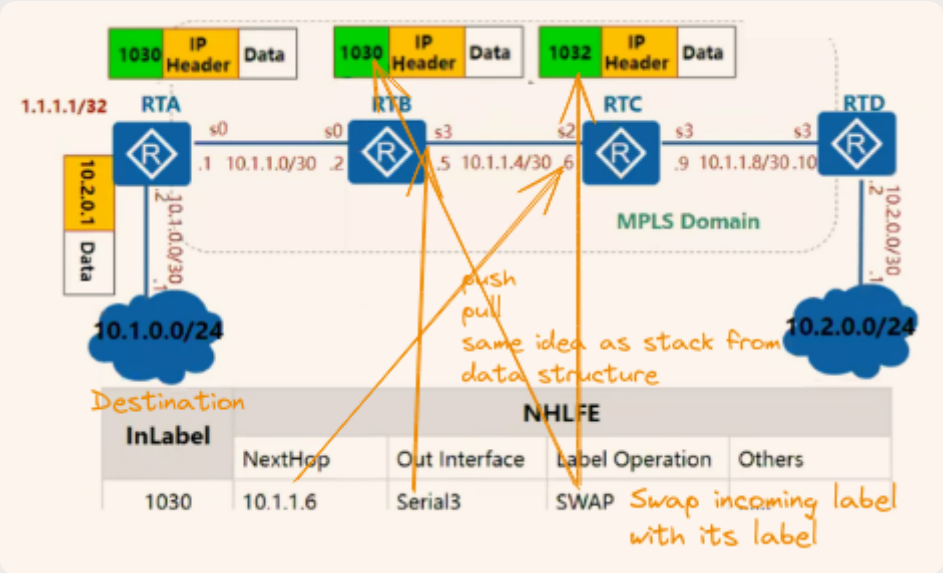


Example Forwarding process

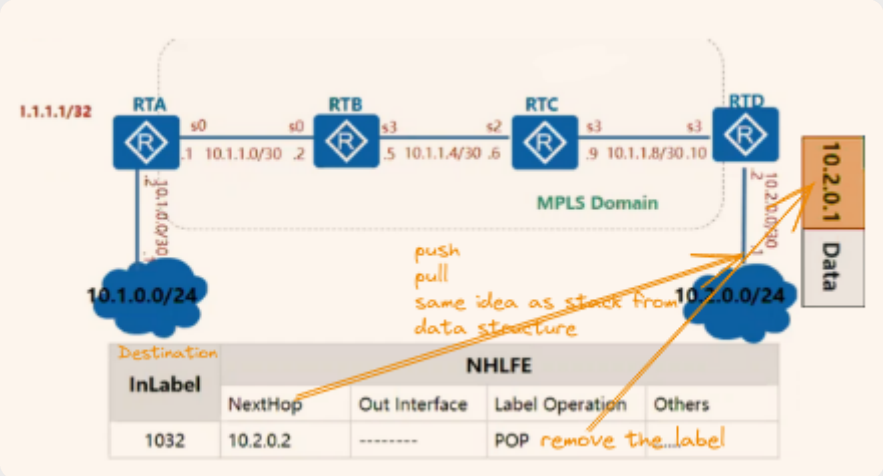
- Step1


1030
IP Header
Data
1.1.1.1/32
RTA
RTB
RTC
RTD
s0
s0
s3
s2
s3
s3
.1 10.1.1.0/30 .2
.5 10.1.1.4/30 .6
.9 10.1.1.8/30 .10
10.2.0.1
Data
.2 10.1.0.0/30 .1
MPLS Domain
.2 10.2.0.0/30 .1
push
pull
same idea as stack from
data structure
10.1.0.0/24
10.2.0.0/24
Destination FEC
NHLFE
NextHop
Out Interface
Label Operation
Others
10.2.0.0
10.1.1.2
Serial0
Push (add label)

- step2


1030
IP Header
Data
1030
IP Header
Data
1032
IP Header
Data
1.1.1.1/32
RTA
RTB
RTC
RTD
s0
s0
s3
s2
s3
s3
.1 10.1.1.0/30 .2
.5 10.1.1.4/30 .6
.9 10.1.1.8/30 .10
10.2.0.1
Data
.2 10.1.0.0/30 .1
MPLS Domain
.2 10.2.0.0/30 .1
push
pull
same idea as stack from
data structure
10.1.0.0/24
10.2.0.0/24
Destination InLabel
NHLFE
NextHop
Out Interface
Label Operation
Others
1030
10.1.1.6
Serial3
SWAP
Swap incoming label
with its label

- step3


1.1.1.1/32
RTA
RTB
RTC
RTD
s0
s0
s3
s2
s3
s3
.1 10.1.1.0/30 .2
.5 10.1.1.4/30 .6
.9 10.1.1.8/30 .10
MPLS Domain
10.2.0.1
Data
push
pull
same idea as stack from
data structure
10.1.0.0/24
10.2.0.0/24
Destination InLabel
NHLFE
NextHop
Out Interface
Label Operation
Others
1032
10.2.0.2

POP
remove the label

1.4.2 MPLS vs Traditional IP Routing

1.4.2.1 Traditional IP Routing

- Connectionless-oriented

> **Connectionless-oriented communication:** is like sending a letter without expecting a response: the message is sent without establishing a dedicated connection between sender and receiver.

- No end-to-end QoS guarantee

> **No end-to-end QoS (Quality of Service) guarantee:** means that a network cannot Guarantee Stable performance levels or data delivery from the source all the way to the destination.

- Hop-by-hop packet processing (low performance)

1.4.2.2 MPLS Advantages

- Fast label-based packet forwarding
- Supports multi-layer labels for VPNs, TE, QoS

> ⚠ **Warning**
>
> - Static MPLS label distribution involves setting up paths manually, which is not practical for large, changing networks.
> - Some dynamic MPLS protocols can't create routes by themselves and rely on other protocols (IGP), making their control processes complex

and resource-intensive.

- Despite enabling traffic engineering, certain dynamic protocols are complicated to set up and don't handle traffic load balancing well, leading to excessive network signaling and resource use.

Criterion	Traditional IP	MPLS
Forwarding Method	Hop-by-hop	Label-based
Performance	Lower	Higher
QoS Support	Poor	Better
Complexity	Higher	Simplified

1.4.3 Segment Routing (SR)

1.4.3.1 Key Improvements with SR

---

1. Extends the existing protocols.

> Segment Routing Simplifies network operations by enhancing IGPs and BGP for greater efficiency and eliminating the need for additional label distribution protocols like MPLS or RSVP.

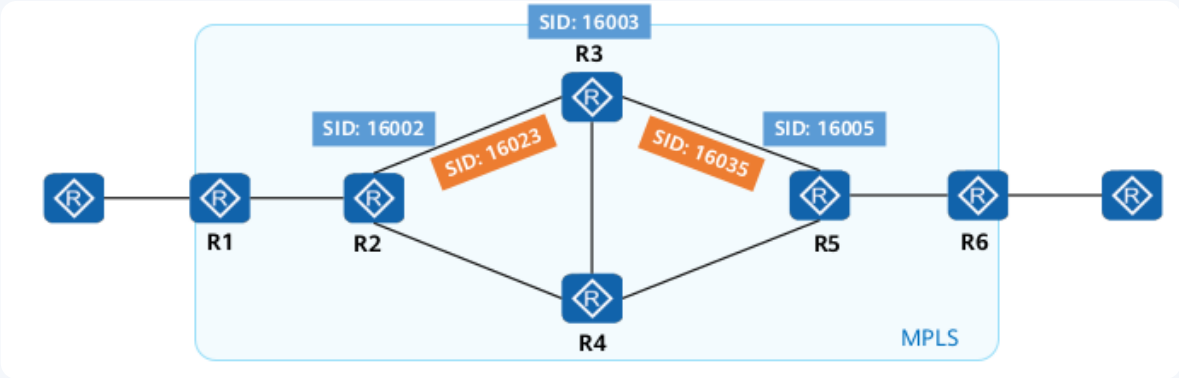
2. Introduces the source routing mechanism.

> Sender of a packet can define the entire path that the packet will take through the network.Instead of each router in the network calculating paths on its own, Segment Routing can work with centralized controllers. These controllers have a full view of the network and can calculate optimal paths for data packets to follow using IGP.

3. Allows networks to be defined by services.

> Segment Routing enables dynamic path computation specific needs for service requirements, such as higher bandwidth or enhanced security, allowing networks to adapt explicitly for optimal service delivery.

1.4.3.2 SR Forwarding Implementation



1. SR (Segment Routing) breaks down a network path into segments, each with a unique Segment ID (SID).
2. In SR, SIDs serve as labels for segments and can be in various formats like MPLS labels or IPv6 addresses; SR-MPLS uses MPLS labels, while SRv6 utilizes IPv6.
3. Nodes and links SIDs are put together in a segment list to define a specific route, which is included in the packet's header by the source node.
4. When a packet arrives at a node, that node checks the segment list; if the top SID matches its own, it removes that SID and continues processing; otherwise, it sends the packet towards the next node on the path in equal cost multiple path (ECMP) mode.

1.4.3.3 Deployment Modes of SR

> In a controller-based deployment, a central controller gathers information about the network, plans and reserves the best routes for data to travel,

and then tells the starting point of the data where to send it. This method helps manage traffic efficiently by using one main system to direct all the data paths.

Without a controller, each network device independently determines the best path for data, leading to a more decentralized and potentially less coordinated approach to traffic management.

1.4.3.4 Applications of SR

Different paths can be defined for various services such as data download (high-bandwidth), video (low-latency), and voice (low packet loss rate).

Extra

SR Overview

- **Segments**: Steps taken by network devices to handle data packets, such as sending them to the right place.
- **Segment ID (SID)**: Unique codes that represent routes or destinations in a network.
- **SR Domain**: A group of network devices that can use Segment Routing technology.

LDP vs. RSVP Problems

LDP, which stands for Label Distribution Protocol, is used in MPLS (Multiprotocol Label Switching) networks to assign labels to network

> paths.

> RSVP (Resource Reservation Protocol) issues related to setting up LSPs (Label Switched Paths)

LDP Issues

---

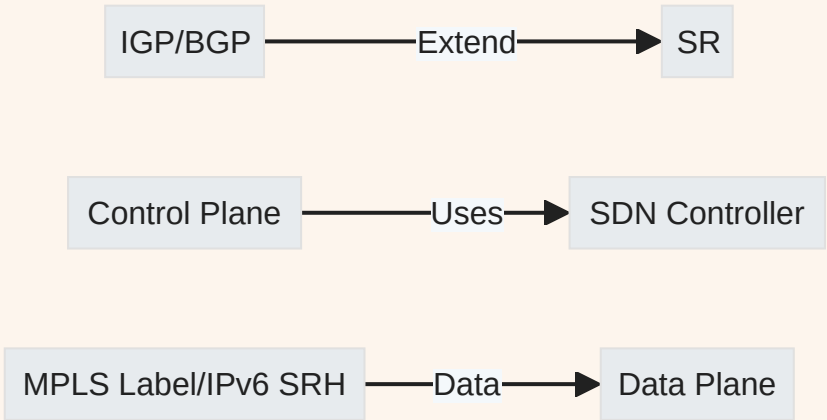
1. LDP determines paths based on the shortest IGP routes and does not support in Traffic Engineering, which could lead to non-optimal data flow that doesn't account for network load or bandwidth.
2. The protocol uses 11 Different packet types for various operations, introducing complexity in packet management and increasing the potential for configuration errors.
3. Frequent label exchanges in LDP can lead to higher bandwidth usage and Increased CPU processing on network devices, potentially affecting performance if resources are limited.

RSVP Issues

---

1. Setting up end-to-end LSPs in an MPLS network requires configuring each node sequentially, a process that is intricate and can be slow.
2. Nodes within the MPLS network need to track active LSPs, increasing operational complexity due to the additional state information required.
3. Implementing ECMP with RSVP is challenging as it complicates routing decisions when multiple paths have similar metrics for data traffic.

SR Technical Framework



Control Plane Components

---

1. Path Selection & Computation via SPT.

> An SPT, or Shortest Path Tree, uses algorithms like Dijkstra's to find the most efficient data travel routes in networks, akin to choosing the quickest drive to work.

2. Routing Protocol Extension (ISIS/OSPF/BGP).
3. SDN Controller Interaction.

> SDN controllers centrally manage network traffic by directing hardware through protocols/APIs, enabling dynamic and automated adjustments to network flow.

Data Plane Components

---

1. **MPLS Label Forwarding:**
    - MPLS streamlines packet forwarding through networks by attaching labels for quick routing decisions, avoiding repetitive IP address inspections.

- IPv6 SRH enhances routing by embedding a sequence of waypoints in the packet header, directing its path across routers.

2. **Source node dictates forwarding path based on segment list:**
    - The originator of a packet specifies its route using segment routing by including an ordered list of segments in the packet's header.
    - Routers simply follow this predefined route, which optimizes network efficiency and allows traffic management for congestion avoidance or performance enhancement.

Basic Concepts of SR

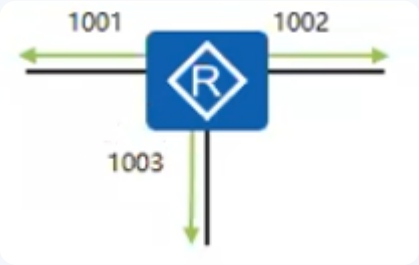
> Segment Routing is a networking technique where data packets follow a pre-determined path with specific stops, simplifying and streamlining the route they take.

Segments

Node Segment

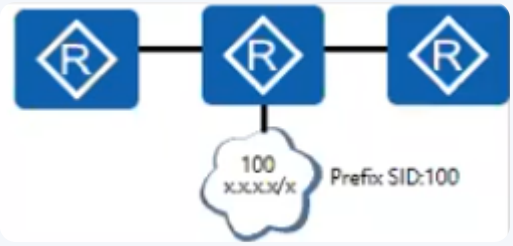
- Identifies a specific node; typically mapped to the loopback address prefix SID.

Adjacency Segment



- Identifies an adjacency between two nodes; dynamically allocated and local to the node.

Prefix Segment



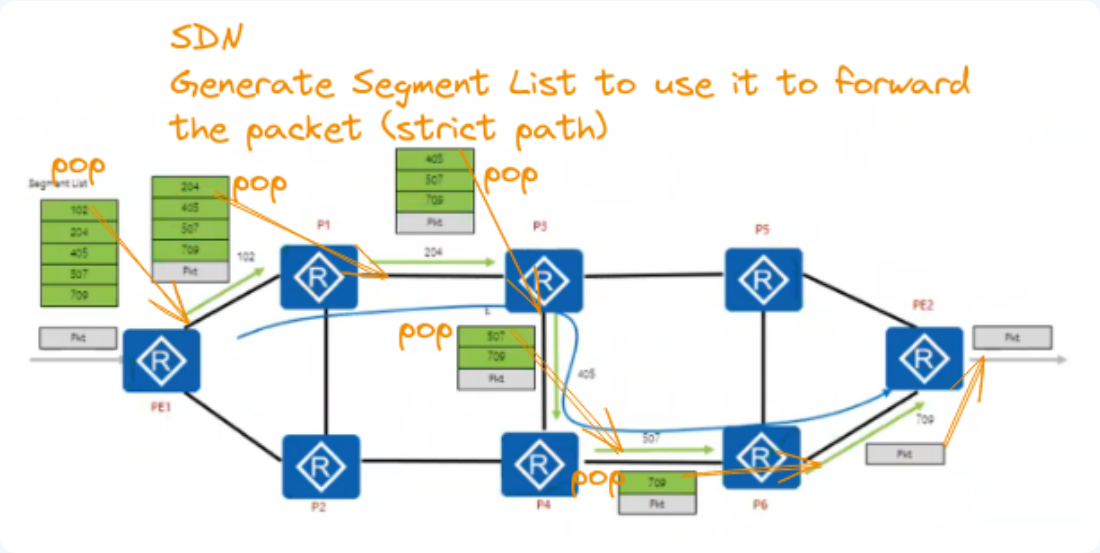
- Identifies the prefix of a destination address; globally valid and advertised via IGP.

SRGB (Segment Routing Global Block)

> The Segment Routing Global Block (SRGB) is like a set of special codes that help guide internet traffic to the right place, kind of like unique addresses for data to follow. Each code is a direction that helps data move efficiently through the network, like a map for letters in the postal system.

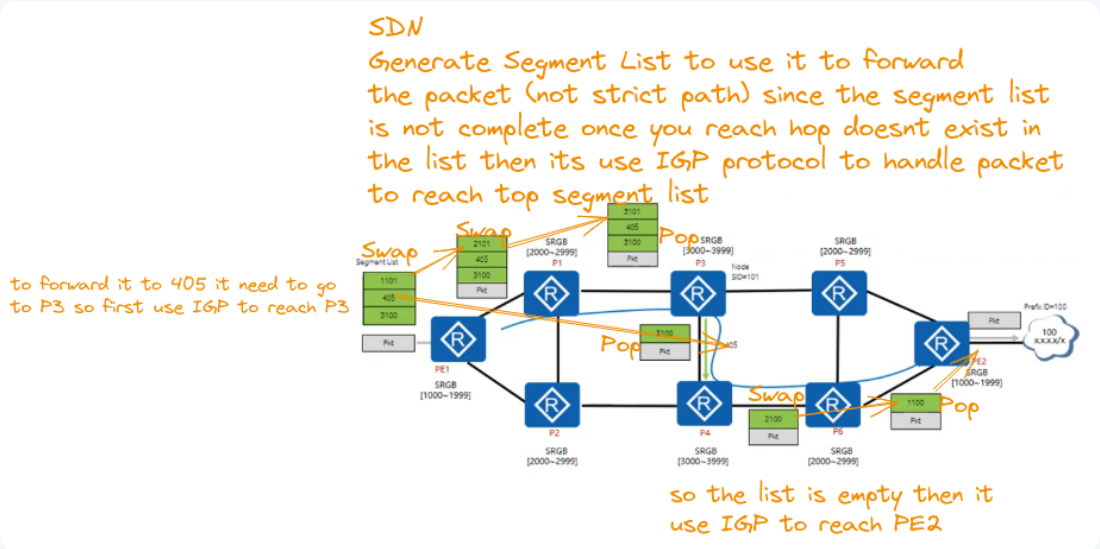
Working Principles

Strict explicit path



Used In SR-TE

Loose Explicit



Used In SR-TE

1.5 Extra

1.5.1 GRE

Extra

Overview of GRE

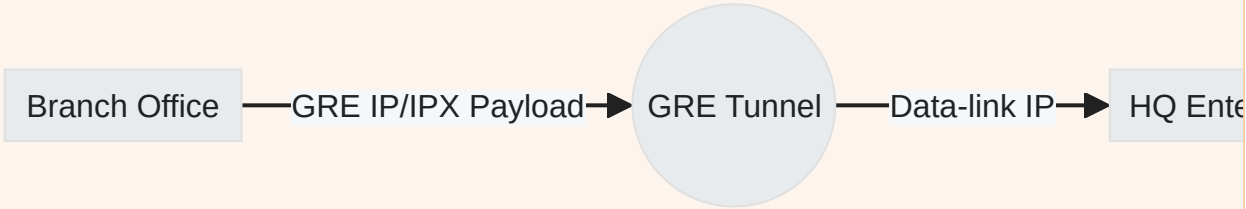
GRE Tunnel Concept

- Encapsulates protocols over other protocols

> Like encapsulate IPX over IP since the public Network works with IP

- Enables routing between remote networks

GRE Tunneling Mechanics



- A **GRE header** is inserted into the packet to create a tunnel.
- This virtual network layer is built over the physical network.

GRE Scaling Solution for IGP

GRE IGP Scaling

- Increases scalability of IGP networks by building tunnels.
- Resolves hop count limitations.

IPSec Support for GRE Tunnels

IPSec GRE Support

> While GRE does not provide confidentiality, IPSec can be used to ensure it.

GRE Keepalive Mechanism

> Use keepalives to monitor tunnel status. Unacknowledged keepalives lead to tunnel teardown.

Configuring a GRE Tunnel

Basic Configuration Steps on Router RTA:

Markdown

```
[RTA] interface <interface-type> <interface-number>
```

```
[RTA-Tunnel0/0/1] ip address <tunnel-ip-address> <mask>
[RTA-Tunnel0/0/1] tunnel-protocol gre
[RTA-Tunnel0/0/1] source <public-ip-address>
[RTA-Tunnel0/0/1] destination <public-ip-address>
[RTA-Tunnel0/0/1] quit
[RTA] ip route-static <destination-ip-address> <mask> <interface-type> <interface-number>
```

Continue

- `<tunnel-ip-address>` : The ip address assigned for tunnel the ip seeable and goes over internet
- `<public-ip-address>` : The ip address obtained by ISP

Configuration Validation:

Markdown

```
[RTA] display interface <interface-type> <interface-number>
```

Continue

> Validates the state (UP/DOWN), encapsulation type, and source & destination of the tunnel.

Routing Table Validation

Route	Flags	NextHop	Interface
`10.1.2.0/24`	RD	`40.1.1.2`	`Tunnel 0/0/1`

Continue

> Ensure the routing table has an entry that corresponds to the established tunnel.

Enabling Keepalive Function

Steps to Enable Keepalive:

Markdown

```
[RTA] interface <interface-type> <interface-number>
[RTA-Tunnel0/0/1] keepalive period <number> retry-times [number_of_retries]
[RTA-Tunnel0/0/1] quit
```

Continue

> Keepalive settings (interval & retries) should be configured on one end of the tunnel only.

1.5.2 IPSEC

Extra

IPSec VPN Overview

> IPSec VPN facilitates the establishment of private network communication over a public network infrastructure like the Internet.

IPSec VPN Architecture

Authentication Protocols

- `MD5`
- `SHA-1`
- `SHA-2`
- Authentication Header (`AH`)

> Ensure authentication

Encryption Protocols

- `DES`
- `3DES`
- `AES`
- Encapsulating Security Payload (`ESP`)

> Ensure authentication and encryption

> Confidentiality and integrity of services are supported through authentication and encryption-based protocols.

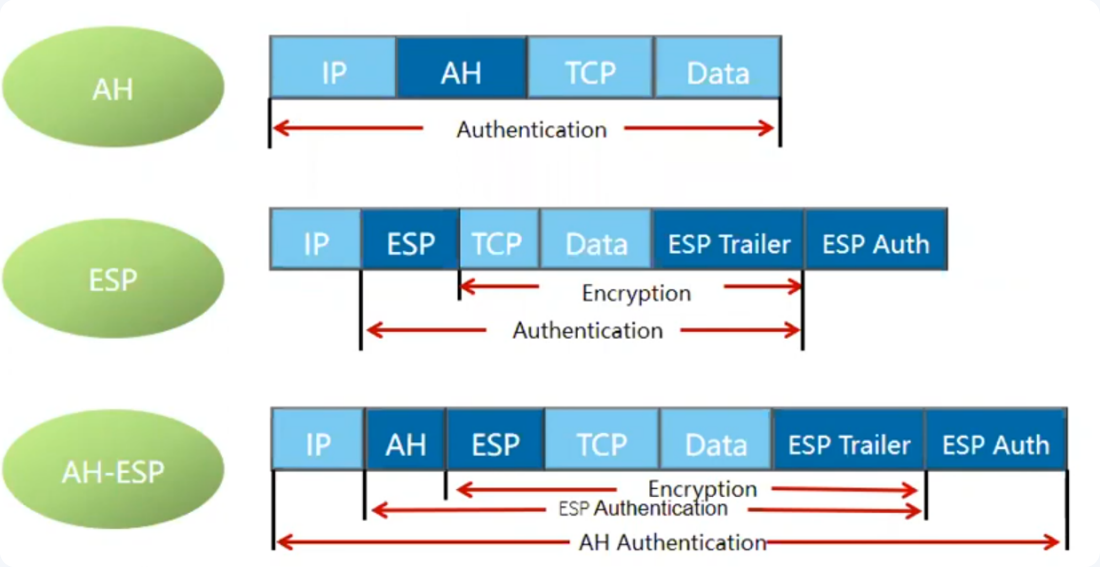
Security Association (SA)

> Specifies parameters for connection establishment. An SA defines parameters in only one direction.

SA Parameters

- **Local Address:** Address of the local interface.
- **Remote Address:** Address of the remote interface.
- **SPI (Security Parameter Index):** Unique identifier for SA like shared key for authentication for Router A and Router B.
  - Inbound SPI
  - Outbound SPI
- **Key:** Secret key used for encryption/decryption.
- **Transform (Proposal):** Encryption and authentication algorithms proposed.

IPSec Transport Mode



IPSec VPN Establishment Process

1. Ensure Reachability between devices.
2. Identify Interesting Traffic that needs to be encrypted.
3. Establish IPSec Proposal with desired encryption and authentication methods.
4. Create IPSec Policy that encapsulates proposal details and associates them with traffic selectors.
5. Apply Policy To Interface to enable traffic encryption across it.

Example Configuration Steps

Static Route Configuration (RTA)

Markdown

```
[RTA] ip route-static <destination-ip-address> <mask> <next-hop>
```

Continue

Access Control List (ACL) Configuration (RTA)

Markdown

```
[RTA] acl number <number>
[RTA-acl-adv-3001] rule <number> permit ip source <ip-address> <wildcard-mask> destination <ip-address> <wildcard-mask>
```

Continue

IPSec Proposal Configuration (RTA)

Markdown

```
[RTA] ipsec proposal <proposal-name>
[RTA-ipsec-proposal-tranl] esp authentication-algorithm
<algorithm-name>
```

Continue

- `<algorithm-name>` : MD5,Sha1,Sha1,DES,3DES,AES

Applying Policy to Interface (RTA)

Markdown

```
[RTA]interface <interface-type> <interface-number>
[RTA-GigabitEthernet0/0/1]ipsec policy <policy-name>
```

Continue

> Remember to configure both endpoints with matching policy parameters.

Verification Commands

To verify IPSec proposal:

Markdown

```
[RTA] display ipsec proposal
```

Continue

To verify IPSec policy:

Markdown

```
[RTA] display ipsec policy
```

1.5.3 SRv6

Extra

Introduction to SRv6

- SRv6 stands for Segment Routing over IPv6.
- Popular in SDN (Software-Defined Networking) and service-driven networks.
- MPLS complexity and resource consumption make it less suitable for large-scale deployment.
- Emergence of NFV (Network Functions Virtualization) brings new network changes.

Benefits of SRv6

Smart Network Paths → Programmable Services → Simple Implementa

- **Smart:** Bridges gap between applications and networks.

- **Simple:** Based on IGP and BGP extensions, no MPLS labels needed.
- **IP-based:** Uses native IPv6 for forwarding, integrates into existing networks.

SRv6 Packet Forwarding

Key Fields in SRH (Segment Routing Header)

---

1. `Segment List` : List of segments forming an explicit path.
2. `Segment Left` : Points to the current active segment.

> A segment in this context is typically a portion or section of a path

Processing at Capable Node

- Updates IPv6 DA field based on Segment List.
- Forwards packet based on longest match routing.

> 1. The node changes the packet's destination if it has a Segment List, which is a set of directions for the packet's journey through the network.
> 2. The node looks at its routing table and sends the packet to the address that best matches the packet's destination address, similar to finding the closest match in a list.

Programmable Behaviors

Instructions vary by seed type:

- **Ingress Node:** Processes SRH, updates DA field.

> This is like a gatekeeper for a network. When data packets come in, it checks if they have a special set of instructions called SRH (Segment Routing Header). The Ingress Node uses these instructions to decide where to send the packet next and changes the packet's "DA" field (Destination Address) accordingly.

- **Egress Node:** Processes packet without SRH if final destination reached.

> This is like the exit door of the network. If a data packet arrives here and it's meant to leave the network because it has reached its final destination, the Egress Node will process it without worrying about any SRH instructions because they're not needed anymore.

Service Applications of SRv6

L3 VPN Services

Route Advertisement Phase

---

1. Configure public network with IGP/BGP.
2. Configure VPN instances on PEs connecting customer edges (CEs).

Data Forwarding Process

---

1. Encapsulate SID representing VPN instance into packets from CE1 to CE2.

> When data needs to travel from one customer site (CE1) to another (CE2), it will be tagged with a Segment Identifier (SID) specific to that VPN instance. This tag ensures that when the data enters the provider network, it stays on its own unique path and is only accessible within that particular VPN as it moves towards its destination at CE2.

EVPN VPWS Services

Similar to L3 VPN but uses layer 2 encapsulation.

> two offices in different cities, and you want computers in one office to connect directly to computers in the other office as if they were in the same room. EVPN VPWS creates a virtual "wire" that connects these offices over a long distance, allowing devices to communicate as though they're physically connected by an Ethernet cable. This service encapsulates the traffic so that it can travel through public or shared networks without being mixed with other traffic or compromised by outside sources.

Inter-AS SRv6 Deployment

Key Points for Inter-AS Deployment

---

1. Locator route advertisement across AS boundaries.

> In Segment Routing with IPv6, we share information about certain network paths, called locators, with other networks so everyone knows how to send data to the right place.

2. Multi-hop MP-BGP peer relationship for VPN routes.

> Using a special version of BGP that works with different network types, we can connect and exchange routes for VPNs even between networks that aren't directly linked together.

Data Forwarding with SRv6 PE Mode

Use ASBRs as ingress/egress points with support for SRv6 encapsulation/decapsulation.

> ASBRs are special routers that connect different networks and help guide data into or out of a network. With SRv6, they wrap data in a special cover when it comes in (like putting a letter in an envelope) and take the cover off when the data goes out (like removing the letter from the envelope).

> When data travels across networks using SRv6, the ASBRs stick on a label with instructions for how to get through the network. Once the data reaches its exit point or another network, these routers peel off this label so that the data can continue on its journey without any extra baggage.

Reliability Features in SRv6

Supports TI-LFA (Topology Independent Loop-Free Alternate) fast reroute mechanism similar to MPLS TI-LFA.

> TI-LFA is a quick fix for network problems that helps avoid traffic jams and keeps data moving even if there's a hiccup in the network.

> It works with the new internet protocol, SRv6, just like it does in older MPLS networks, and doesn't care about how the network cables are arranged.

Network Evolution with SRv6

Stages:

1. Upgrade ingress/egress nodes first; other nodes require only IPv6 forwarding initially.

> The first step is to update the network's entry (ingress) and exit (egress) points so they understand SRv6 commands. Initially, other nodes in the network just need to be capable of handling basic IPv6 traffic.

2. Eventually upgrade remaining nodes to support native SRv6 deployment.

Applicability:
4G/5G MBH, Metro Access, DCI, Tactile Cloud scenarios that require service chaining can benefit from inherent support provided by SRv6 SIDs orchestration.

Words

- **4G/5G MBH:** Networks that connect mobile base stations to the core.
- **Metro Access:** Networks that connect subscribers in metropolitan areas.
- **DCI:** Networks connecting different data centers.
- **Tactile Cloud:** Environments needing fast communication between computing resources.

Conclusion: Comparison with MPLS-SR

Advantages of IPv6-SR over MPLS-SR:

SR Feature	MPLS-SR	IPv6-SR
Programmability	Limited	Enhanced
Legacy Network Integration	Complex	Simpler
Service Chaining Support	Basic	Advanced

Network Management and O&M

1 Network Management and O&M

1.1 Basic Concepts of Network Management and O&M(Operation and Maintenance)

1.1.1 Overview

- **Purpose:** Ensure devices work properly & network runs efficiently, reliably, and securely.
- **Role:** Managed by a network administrator for stable operation.

1.1.2 Classification of Network Management

- **Software Management:**
  - Management of network applications.
  - User accounts management.
  - Permissions for file access.
- **Hardware Management:**

- Involves managing network elements (NEs) like firewalls, switches, routers.

> **Note**
>
> NEs are both hardware devices and the software running on them with at least one main control board.

1.1.3 Basic Network Management Functions (OSI Model) (FCAPS)

1.1.3.1 Configuration Management

- Monitors configurations.
- Manages hardware/software parameters and conditions.
- Configures services.

1.1.3.2 Performance Management

- Manages network performance for reliable communication with minimal resources.

1.1.3.3 Fault Management

- Maintains network availability.
- Repairs faults Quickly.

1.1.3.4 Security Management

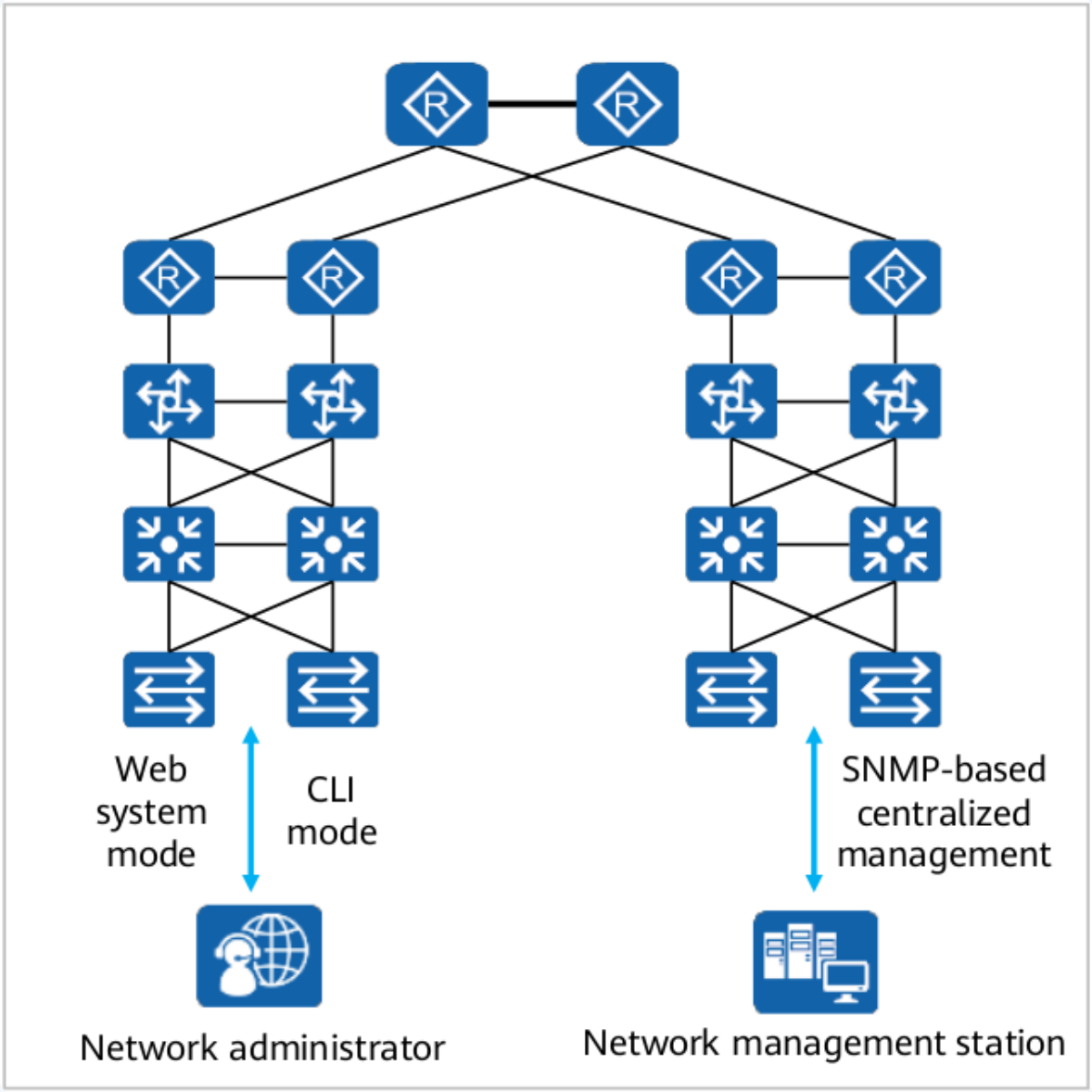
- Protects against unauthorized access and attacks.

1.1.3.5 Accounting Management

- Records user resource usage.
- Charges users based on usage.

1.1.4 Network Management Modes

1.1.4.1 Traditional Network Management



Mode	Description
Web System	GUI via built-in web server (HTTPS).
CLI Mode	Command line management via console port, Telnet, or SSH.
SNMP-based Centralized	Manages NEs using SNMP from a central management station.

CLI mode: provides Enhanced device management but requires that users be familiar with command lines.

SNMP-based centralized management: provides centralized and unified management of devices on the entire network, greatly improving

management efficiency.

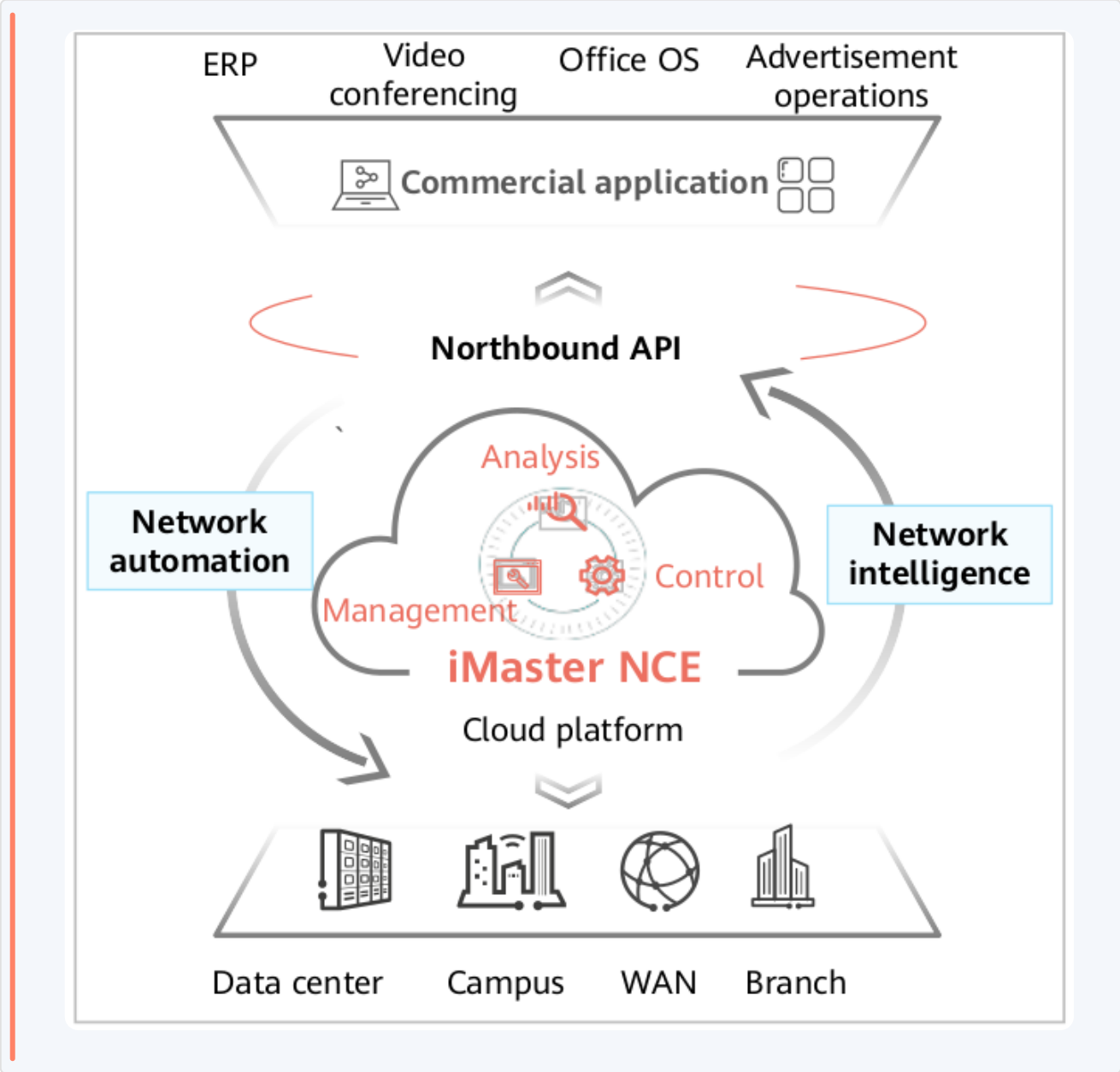
SNMP unified managment

- Without SNMP, manual login and command execution (`show ip ospf` on Cisco, `show ospf neighbor` on Juniper) are necessary for OSPF status.
- With SNMP, an SNMP manager queries OSPF data using standardized OIDs in the routers' MIBs via SNMP protocol operations without direct CLI commands.

Here's an example of what some OID requests might look like:

- To get OSPF version number: `SNMP GET 1.3.6.1.2.1.14.1.2`
- To get OSPF area ID: `SNMP GET 1.3.6.1.2.1.14.2`

1.1.4.2 iMaster NCE-based Network Management



Feature	Description
Automation & Intelligence Platform	Integrates management, control, analysis, AI.
Full-lifecycle Automation	Simplifies operations through automation.
Intelligent Closed-loop Mgmt.	Utilizes big data & AI for decision-making.
Open Programmability	Supports scenario-specific applications ecosystem.
All-cloud Platform Capacity	Manages networks on a large scale efficiently.

Protocols Used:

- NETCONF & RESTCONF for configuration delivery.
- Telemetry for traffic monitoring.

1.2 SNMP Fundamentals and Configuration

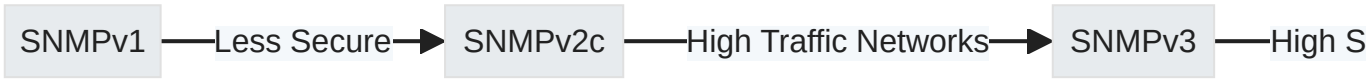
1.2.1 Key Concepts

1.2.1.1 SNMP Basic Understanding

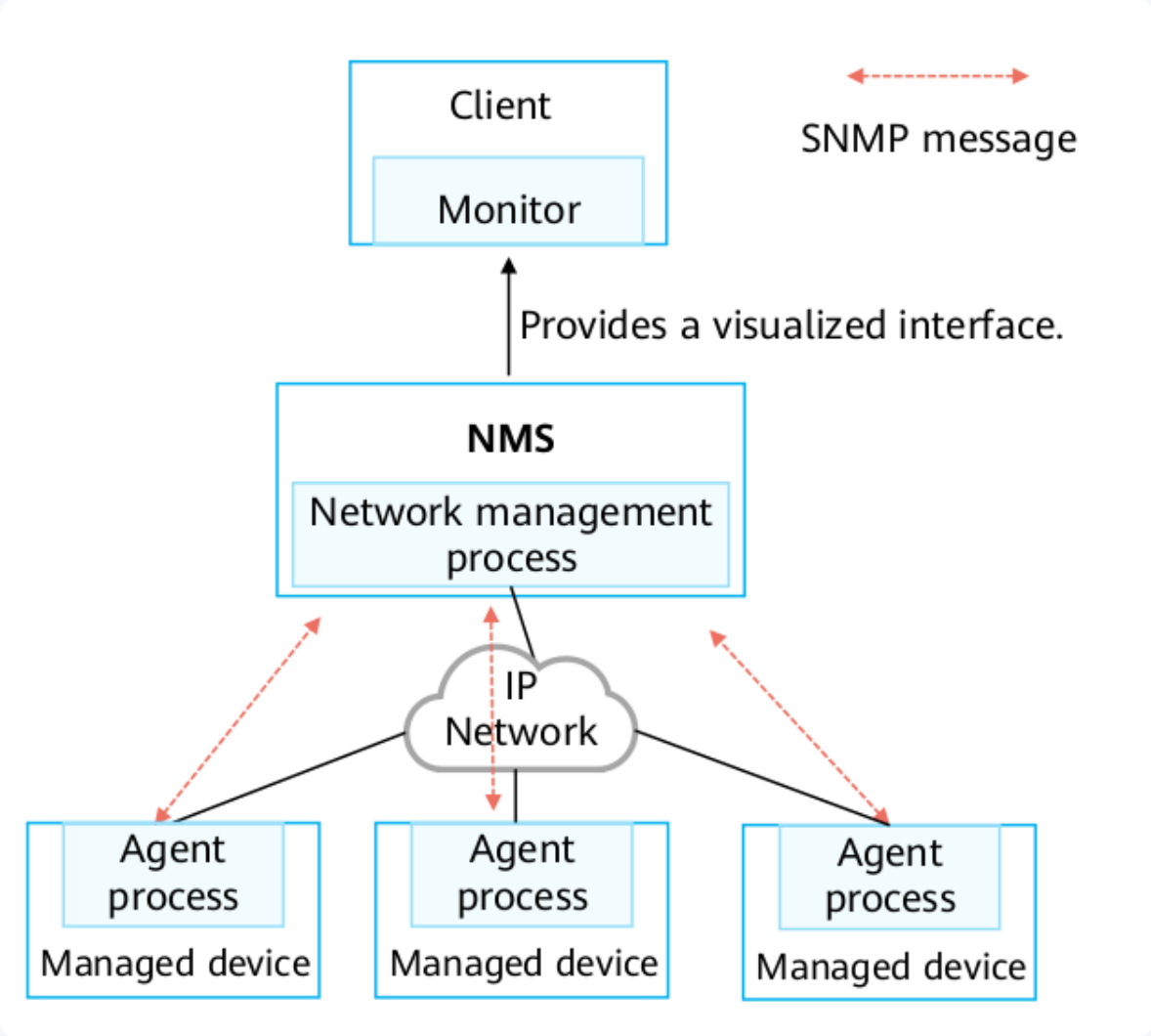
> **Note:** SNMP is crucial for network management, especially in large-scale networks with diverse device types.

- **Simplicity**: Uses UDP and polling mechanism.
- **Convenience**: Enables management across different devices.

1.2.1.2 SNMP Versions



- `SNMPv1` : Basic functionality, low security.
- `SNMPv2c` : Enhanced error codes and bulk operations.
- `SNMPv3` : Authentication and encryption support.



1.2.1.3 MIB (Management Information Base)

> A MIB is a structured database of variables for network devices, containing OIDs, statuses, access permissions, and data types.

1.2.1.3.1 Public vs. Private MIBs

- **Public:** Defined by RFCs for standardization.
- **Private:** For enterprise-specific functions or protocols.

1.2.1.3.2 Common MIB Objects Access Permissions

OID	Object Name	Data Type	Access Level	Description
`1.3.6.1.2.1.2.1`	ifNumber	Integer	read-only	Number of interfaces
`1.3.6.1...`	hwIpAdEntNetMask	IpAddress	read-create	Subnet mask

1.2.1.4 SNMP Message Types

1.2.1.4.1 Operations and Traps in Different Versions

- **`Get`, `Set`, `GetNext`, `Response`, `Trap`:** Basic operations in SNMPv1.
  - `Get`: Asks for the value of a specific variable from an SNMP agent.
  - `Set`: Tells an SNMP agent to change the value of a specific variable.
  - `GetNext`: Requests the next variable in the MIB (Management Information Base) hierarchy from an SNMP agent.
  - `Response`: The reply from an SNMP agent delivering the requested information or confirmation of a set action.
  - `Trap`: An unasked or unrequested message from an SNMP agent to the management system indicating an event or change in status.
- **Added in SNMPv2c:** `GetBulk` (multiple GetNext), `Inform` (requires acknowledgment).
  - `GetBulk`: A request to efficiently retrieve large volumes of data by requesting multiple `GetNext` operations in a single command.
  - `Inform`: A message sent between SNMP managers to share alerts or notifications, with a confirmation required to acknowledge receipt.
- **SNMPv3:** Same as v2c but with security enhancements (authentication & encryption).

1.2.1.5 Configuration Basics

1.2.1.5.1 Enabling SNMP on a Device

```markdown
[R1]snmp-agent
[R1]snmp-agent sys-info version <version>
```

- `<version>` : is v1,v2c,v3 for snmp.

> **Warning**
>
> Ensure that the protocol version matches between device and NMS.

1.2.1.5.2 Create or update MIB view information.

```markdown
[Huawei] snmp-agent mib-view view-name < exclude | include > subtree-name {mask <mask>}
```

1.2.1.5.3 Add a new SNMP group and map users in this group to the SNMP view.

```markdown
[Huawei] snmp-agent group v3 <group-name> <authentication||noauth||privacy> { read-view <view-name> | write-view <view-name> | notify-view <view-name> }
```

1.2.1.5.4 Add a user to the SNMP group.

```markdown
[Huawei] snmp-agent usm-user v3 <user-name> group <group-name>
```

1.2.1.5.5 Configure an authentication password for an SNMPv3 user.

```markdown
[Huawei] snmp-agent usm-user v3 <user-name> authentication-mode < md5 | sha | sha2-256 >
```

1.2.1.5.6 Configure the SNMPv3 user encryption password.

```markdown
[Huawei] snmp-agent usm-user v3 <user-name> privacy-mode < aes128 | des56 >
```

1.2.1.5.7 Set parameters for the device to send traps.

```markdown
[Huawei] snmp-agent target-host trap-paramsname <paramsname> v3 securityname <securityname> <authentication | noauthnopriv | privacy >
```

1.2.1.5.8 Configure the target host of traps.

```
[Huawei] snmp-agent target-host trap-hostname <hostname> address <ipv4-address> trap-paramsname <paramsname>
```

1.2.1.5.9 Enable all trap functions.

```
[Huawei] snmp-agent trap enable
```

1.2.1.5.10 Configure the source interface that sends traps.

```
[Huawei] snmp-agent trap source <interface-type> <interface-number>
```

1.3 Network Management Based on Huawei iMaster NCE

1.3.1 Huawei iMaster NCE Platform

> Constructing automated and intelligent network systems centered on user experience is important to address the explosive increase in traffic and service complexity.

1.3.1.1 Overview

- Integrates management, control, analysis, AI functions.
- Manages both traditional devices and SDN-capable networks.

1.3.1.2 Key Capabilities

1.3.1.2.1 Full-lifecycle Automation

- Device plug-and-play.
- On-demand service provisioning.
- Fault self-healing.

1.3.1.2.2 Intelligent Closed-loop Management

- Intent engine and automation engine for real-time network status determination.
- AI algorithms provide automated analysis and decision-making.

1.3.1.2.3 Open Programmability

> Ecosystem for scenario-based applications:
>
> - Southbound programmability with Design Studio.
> - Northbound cloud-based AI training platforms.

> - **South side:** Manages network hardware and infrastructure

> - **North side:** Interfaces with applications using network data for higher-level tasks.

1.3.1.2.4 Large-capacity Cloud Platform

- Supports on-premises and cloud-based deployment.
- Elastic scalability for numerous access users.

1.3.1.3 NETCONF Protocol

1.3.1.3.1 NETCONF Overview

> NETCONF is a network management protocol that allows for the installation, manipulation, and deletion of the configuration of network devices using XML.

- **NETCONF has three objects:**
  - NETCONF client
  - NETCONF server
  - NETCONF message

1.3.1.3.2 Advantages of NETCONF vs SNMP vs CLI

Function	NETCONF	SNMP	CLI
Interface	Machine-machi	Machine-man interface	Man-machine

Function	NETCONF	SNMP	CLI
Operation	High efficie	Medium efficiency	Low
Scalability	Extens	Weak	Moderate
Transactio Strong support like rollback like	Not supported	Partially	
Secure Trans.	Multiple pro cols	Only SNMPv3	SSH only

1.3.1.4 YANG Modeling Language

1.3.1.4.1 YANG Overview

YAML

```yaml
// YANG file example snippet:
module example-module {
namespace "http://example.com/ns/example-module";
prefix "ex";

container server {
    list server {
      key "name";
      unique "ip port";
      leaf name { type string; }
      leaf ip { type inet:ip-address; }
      leaf port { type inet:port-number; }
    }
}
}
```

> The YANG file is used to convert data into XML-format NETCONF messages before they are sent to the device.

> The YANG file is used to convert received XML-format NETCONF messages into data for subsequent processing.

1.3.1.4.2 Characteristics of YANG Models

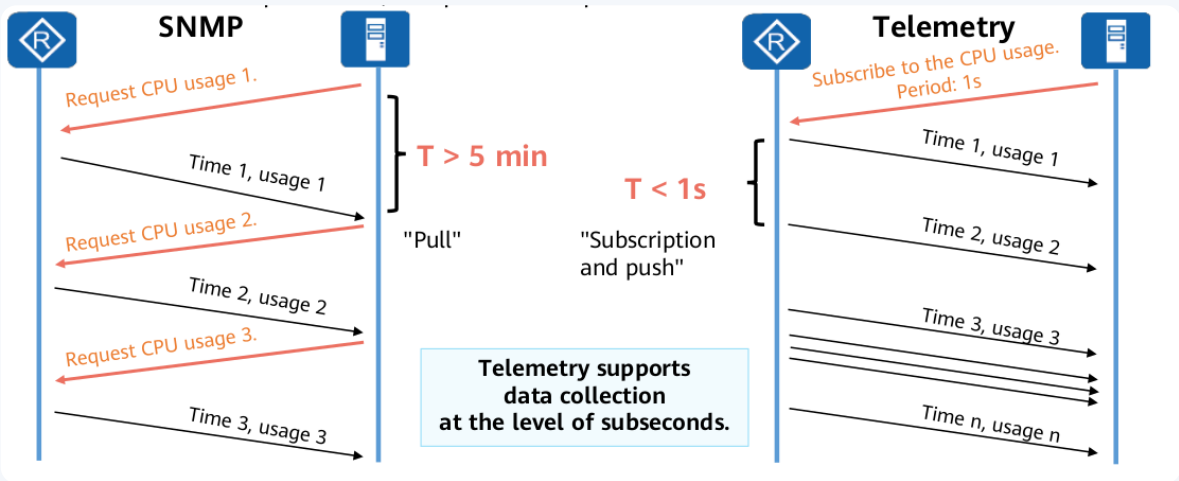
- Hierarchical tree-like structure modeling.
- Modules and sub-modules presentation.
- Conversion to XML-syntax YIN model without loss.

1.3.1.5 Telemetry Technology

1.3.1.5.1 Telemetry vs SNMP

SNMP - Pull Mode → T > 5 min

Telemetry - Push Mode → T < 1s



- **Pull mode (SNMP):** The monitoring system periodically requests information from devices.
- **Push mode (Telemetry):** Devices automatically send information to the monitoring system in real-time or at configured intervals.

1.3.1.5.2 Benefits of Telemetry

- Sub-second level data collection for real-time insights.
- Improved transmission efficiency through data packaging.

IPv6 Basics

1 IPv6 Basics

1.1.1 Overview of IPv6

1.1.1.1 Need for IPv6

- Exhausted public IP addresses in IPv4 vs. nearly infinite address space in IPv6.

> The 128-bit address length creates an extremely large number of unique addresses, which is more than enough for the growing needs of things like the Internet of Things and allows for easy growth and development of new services.

- Improved packet header design.

Why ipv6 packet header better

1. **Simplified Header:** IPv6 has a fixed 40-byte header with fewer fields, making it quicker for routers to process.
2. **No Router Fragmentation:** IPv6 leaves packet fragmentation to the sender, simplifying router operations.
3. **Fixed Header Length:** The consistent length of the IPv6 header allows for predictable processing by network devices.
4. **Extension Headers:** IPv6 uses optional extension headers for special functions, which are skipped by routers if not needed, speeding up processing.
5. **Larger Address Space:** IPv6 has 128-bit addresses, vastly increasing the number of available IP addresses and solving exhaustion issues.

- In essence, IPv6 Simplifies packet processing and offers an expanded addressing scheme, leading to more efficient networking.

- Plug-and-play

> Plug-and-play networking allows devices to connect to a network with minimal setup by automatically obtaining an IP address. They can receive an IP address manually from an administrator, automatically from a DHCP server, or through self-configuration using SLAAC with IPv6. This simplifies device connection and network configuration.

- Hierarchical address allocation.

Note

- IPv4 can indeed use route aggregation to reduce the number of routing table entries, similar to IPv6. Both protocols allow networks to be summarized with a single prefix when announcing routes. For example, if an ISP owns the blocks 203.0.113.0/24 and 203.0.114.0/24, it can aggregate them and announce a single route to cover both blocks using the prefix 203.0.112.0/23.
- However, IPv6's larger address space (128-bit vs IPv4's 32-bit) allows for a much more detailed and hierarchical structure in address

allocation, which enhances the ability to aggregate routes even more efficiently than IPv4 due to its vast address space and flexible subnetting options.

- High scalability

> IPv6 extension headers, inserted between the basic header and payload as needed, enhance encryption, mobility, optimal path selection, and QoS without Overloading the main data packet, thus improving packet forwarding efficiency.

- Enhanced security features.

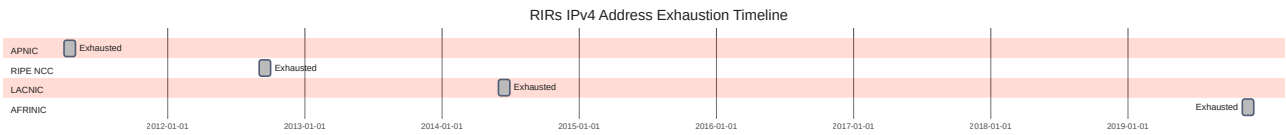
> IPsec, source address authentication, and other security features ensure E2E security, preventing NAT from damaging the integrity of E2E communication.

- Support for mobility and QoS.

> mobile devices can switch between network areas more efficiently without unnecessary extra paths, making the network faster and more reliable.

> A Flow Label field is additionally defined and can be used to allocate a specific resource for a special service and data flow.

1.1.1.2 Regional Internet Registries (RIRs) Status



Note

- **IANA (Internet Assigned Numbers Authority):** is an organization responsible for coordinating global IP address allocation and managing the DNS root zone.
- **RIR (Regional Internet Registry):** is an entity that oversees the allocation and registration of Internet number resources within a specific region of the world.

1.1.1.3 IPv6 Header

Field	Description
Version	Indicates the IP protocol version, set to 6 for IPv6.
Traffic Class	Specifies packet priority for Quality of Service (QoS).
Flow Label (NEW)	Identifies data flows for special handling.
Payload Length	Length of data following the header, in bytes.
Next Header	Type of the next header or upper-layer protocol.
Hop Limit	Decrements by 1 at each hop; packet discarded if zero.
Source Address	The 128-bit address of the sender of the packet.
Destination Address	The 128-bit address where the packet is being sent to.

Extension Header Field	Description in Simple Terms
Hop-by-Hop Options Header	Provides instructions for each router the packet passes through on the network, such as how to process the packet.
Destination Options Header	Carries additional information for the final destination of the packet, and is checked after any Routing or Fragment headers have been processed.
Routing Header	Lists one or more routers the packet should visit before reaching its final destination.

Extension Header Field	Description in Simple Terms
Fragment Header	Used for splitting large packets into smaller pieces that can travel across networks with smaller MTU limits.
Authentication Header (AH)	Provides a way to check if the packet is from a trusted sender and hasn't been tampered with (part of IPsec).
Encapsulating Security Payload	Helps keep data in the packet secret and secure from eavesdroppers, also part of IPsec (ESP header).

Extension headers are optional and variable in length. Only one `::` allowed per address to represent consecutive zeros.

1.1.1.4 Abbreviating IPv6 Addresses

Note

> An IPv6 address is 128 bits long, typically divided into eight 16-bit blocks in hexadecimal form separated by colons. For example, an IPv6 address can look like this: 2001:0DB8:0000:0000:0008:0800:200C:417A.

> IPv6 addresses can be shortened by removing leading zeroes within each block, and in a row blocks of zeroes can be replaced by a double colon (::), but only once in an address. For instance:

- **Full IPv6 Address:**
  - 2001:0DB8:0000:0000:0008:0800:200C:417A
- **Abbreviated:**
  - 2001:DB8::8:800:200C:417A

> **Tip**
>
> Also, the case of letters doesn't matter.

1.1.1.5 Classification of IPv6 Addresses

1.1.1.5.1 Unicast Addresses

- **Global Unicast Address** (`GUA`): `2000::/3`
- **Unique Local Address** (`ULA`): `FD00::/8`
- **Link-local Address** (`LLA`): `FE80::/10`
- **Special IPv6 address**
  - Unspecified address (::/128): Used as a source address for packets such as Neighbor Solicitation messages during Duplicate Address Detection (DAD) or DHCPv6 client requests.
  - Loopback address (::1/128): Functions like IPv4's 127.0.0.1 for local loopback, where packets sent to it are directed back to the sending host for testing.

1.1.1.5.2 Multicast Addresses

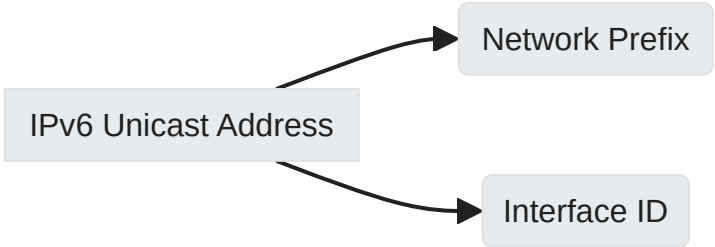
Identify multiple interfaces; packets sent to all group members.

1.1.1.5.3 Anycast Addresses

Identify a group of interfaces; packets sent to nearest member.

> 1. Anycast addresses offer service redundancy.
> 2. They enable efficient service delivery by selecting the optimal path.

1.1.1.6 Unicast Address Format



- **Network Prefix:** n bits (similar to IPv4's network ID)
- **Interface ID:** 128-n bits (similar to IPv4's host ID)

> Commonly, both the network prefix and interface ID are 64 bits long.

1.1.1.6.1 Interface ID Generation Methods

- Manual configuration
- Automatic system generation

> An automatic system generation for creating a unique identifier automatically assigns a distinct code to each user without human input.

- EUI-64 standard

> The EUI-64 standard extends a 48-bit MAC address to create a unique 64-bit interface identifier for IPv6 addresses by inserting 'FFFE' in the

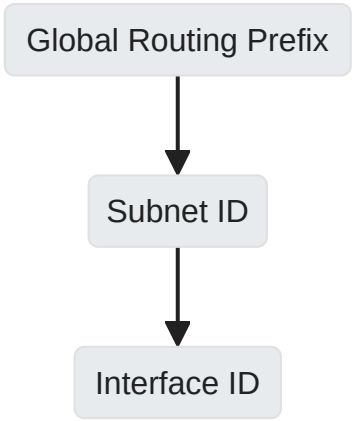
> middle and flipping the seventh bit. EUI Create unique identifier 64 bit is paired with a network prefix to form a complete IPv6 address.

1.1.1.6.1.1 EUI-64 Example Conversion

---

1. Convert MAC `3C-52-82-49-7E-9D` to binary.
2. Invert bit 7.
3. Insert `FFFE` in the middle.
4. **Result:** `3E-52-82-FF-FE-49-7E-9D`

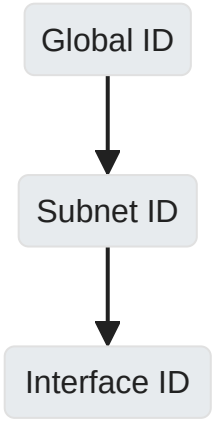
1.1.1.6.2 Global Unicast Addresses (GUAs)



> Network address is 64 bit and host address is 64 bit

> GUAs start with `2000::/3`. They are globally unique and used for Internet access.

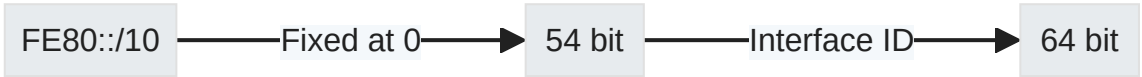
1.1.1.6.3 Unique Local Addresses (ULAs)



> It has 40 bit for random id(global id) Generated using a pseudo-random algorithm

> ULAs start with `FC00::/7` or more specifically `FD00::/8` for local communication.

1.1.1.6.4 Link-Local Addresses (LLAs)



> prefix of FE80::/10.

> LLAs are used within a single link and cannot be routed externally.

> Each IPv6 interface must have an LLA.

1.1.1.6.5 Multicast Address Format

---

8 bits	4 bits	4 bits	80 bits	32 bits
11111111	Flags	Scope	Reserved (must be 0)	Group ID

Field	Bits	Description
Flags	4	Indicates permanent/transient group
Scope	4	Specifies multicast group scope
GroupID	32	Multicast group identifier

Note

- **All nodes:** FF01::1, FF02::1
- **All routers:** FF01::2, FF02::2

1.1.1.6.5.1 Scopes:

---

1. Interface-local scope: span only a single interface.
2. Link-local scope: limited to the local network segment.
3. Site-local scope: confined to the local site.
4. Organization-local scope: spans across organizational boundaries.
5. Global scope: encompasses the entire IPv6 internet.

1.1.1.6.5.2 Solicited-Node Multicast Address

---

a solicited-node multicast address is a special type of address used in IPv6 networks to help devices find each other on the same local network. When a device has an IPv6 address, it automatically gets a corresponding solicited-node multicast address. This special address is used for two main purposes:

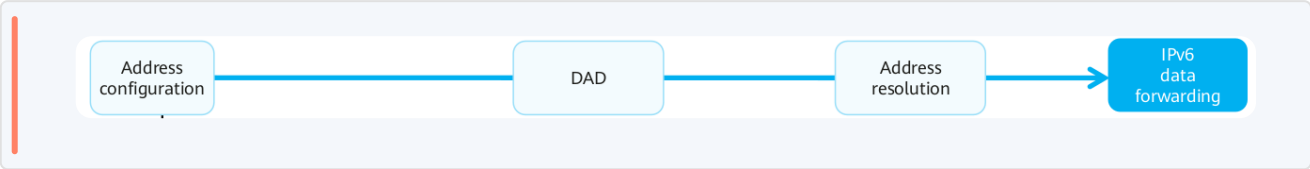
1. **Neighbor Discovery**: It helps devices on the same local network segment to identify who their neighbors are.

2. **Duplicate Address Detection (DAD)**: It ensures that no two devices try to use the same IP address on the network.

> **Note**
>
> This solicited-node multicast address is only relevant and used within the local network (it doesn't work over the internet). When one device wants to communicate with another, instead of sending a message to everyone, it sends a message just to this special multicast address. Only the intended recipient, which 'listens' for messages sent to this address, will receive and process the message. This makes things more efficient because it avoids bothering all other devices on the network with unnecessary traffic.

1.2 IPv6 Overview

1.2.1 Address Configuration Process



1.2.1.1 Global Unicast Address (GUA)

- Manual Configuration or SLAAC/DHCPv6.

1.2.2 Neighbor Discovery Protocol (NDP)

> NDP stands for Neighbor Discovery Protocol, and it's used by devices on an IPv6 network to discover each other and to determine each other's link-layer addresses, find routers, and maintain reachability information about the paths to other active neighbor nodes.

> - Defined in RFC 4861.

ICMPv6 Messages:

- **RS (Router Solicitation):** A device sends this message asking for routing information.
- **RA (Router Advertisement):** A router sends this message in response, providing routing information.
- **NS (Neighbor Solicitation):** A device sends this message either looking for another device's physical address or doing DAD.
- **NA (Neighbor Advertisement):** A device replies with this message, providing its physical address or responding to DAD.

1. **SLAAC (Stateless Address Autoconfiguration):** Devices automatically configure their IP addresses using Router Advertisements from NDP to obtain network prefixes.

> Routers send Router Advertisements (RA) with prefix information, and devices use this information to generate an IP address.

2. **DAD (Duplicate Address Detection):** Devices use NDP to send a Neighbor Solicitation message for their proposed IP to ensure its uniqueness on the network.

> sending a Neighbor Solicitation (NS) message with its proposed IP address as the target address. If another device is already using that

> address, it will respond with a Neighbor Advertisement (NA), indicating there's a conflict.

3. **Address Resolution:** NDP facilitates discovery of a device's link-layer address by exchanging Neighbor Solicitation and Advertisement messages.

> A device sends an NS message asking "Who has this IPv6 address?" and the owner of that IP sends back an NA message with its link-layer address.

4. **Prefix Advertisement:** Routers broadcast IPv6 prefix information via NDP in Router Advertisements for address configuration on the local network.

> This is done through Router Advertisement messages which include prefix information options.

1.2.3 Dynamic IPv6 Address Configuration

1.2.3.1 Stateless Address Autoconfiguration (SLAAC)

- Uses ICMPv6 RA and RS messages.
- Host generates an address using the prefix from RA and its own interface ID.

> Only IPv6 addresses can be obtained

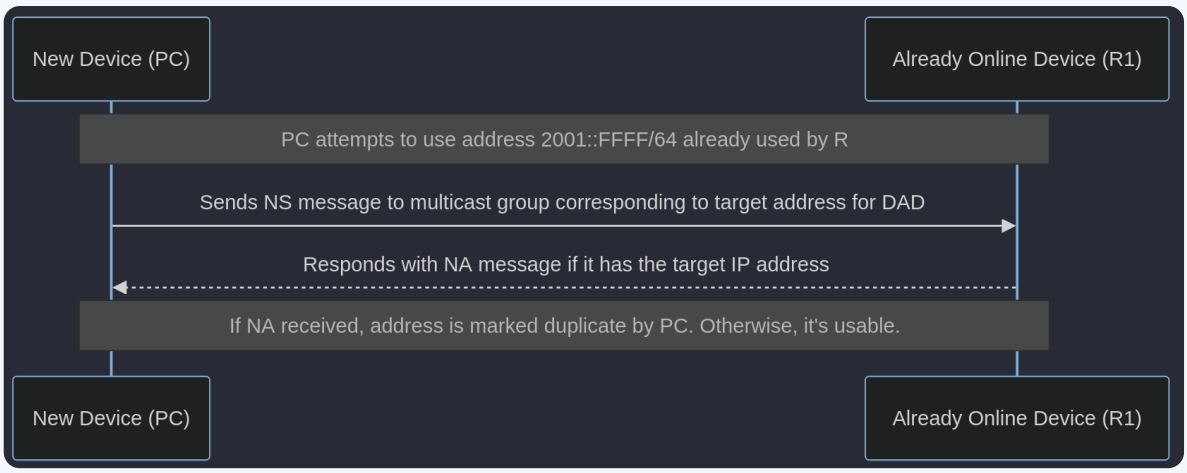
1.2.3.2 Stateful Address Autoconfiguration (DHCPv6)

- Managed by DHCPv6 server.
- Provides full IPv6 addresses and other network parameters.

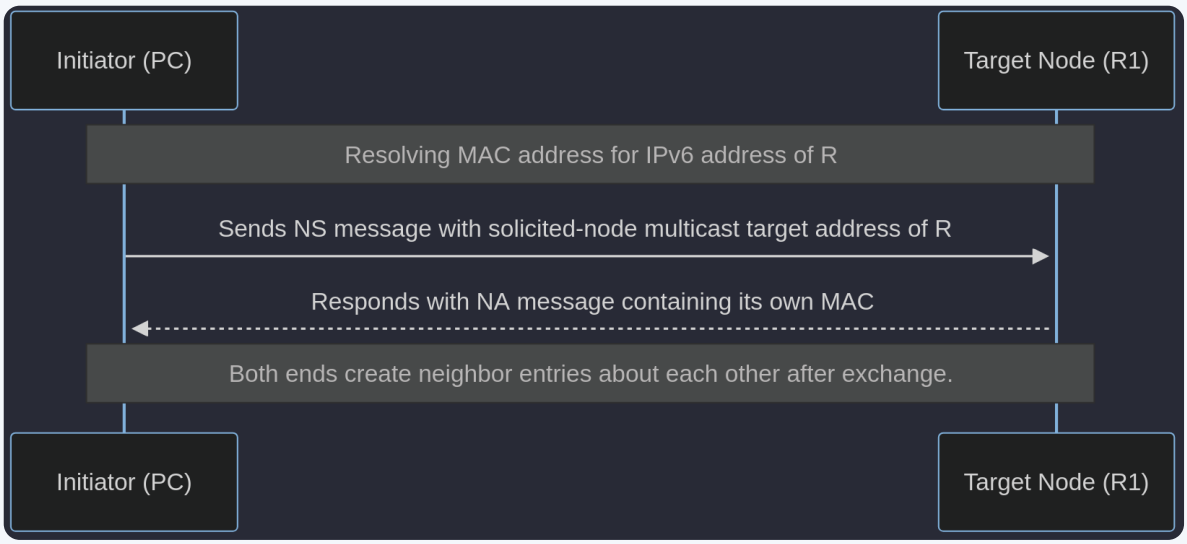
Flag	Purpose
M Flag	Managed address configuration
O Flag	Other stateful configurations

> M flag = 1 and O flag = 1 indicates stateful configuration via DHCPv6.

1.2.4 DAD Mechanism Example



1.2.4.1 Address Resolution with NDP Example



1.3 Typical IPv6 Configuration Examples

1.3.1 General Commands

1.3.1.1 Enabling IPv6 Globally

Markdown

```
[Huawei] ipv6
```

> Enable IPv6 on the device globally.

1.3.1.2 Enabling IPv6 on an Interface

Markdown

```
[Huawei-GigabitEthernet0/0/0] ipv6 enable
```

> Activate IPv6 on a specific interface.

1.3.1.3 Link Local Address (LLA)

1.3.1.3.1 Configuring LLA Manually/Automatically

Markdown

```
[Huawei-GigabitEthernet0/0/0] ipv6 address <ipv6-address> link-local
```

> Set LLA manually

Markdown

```
[Huawei-GigabitEthernet0/0/0] ipv6 address auto link-local
```

> Configure LLA automatically.

1.3.1.4 Global Unicast Address (GUA)

1.3.1.4.1 Configuring GUA Manually/Automatically

Markdown

```
[Huawei-GigabitEthernet0/0/0] ipv6 address {<ipv6-address> prefix-length | <ipv6-address>/prefix-length}
```

> Assign GUA manually.

Markdown

```
[Huawei-GigabitEthernet0/0/0] ipv6 address auto {global | dhcp}
```

> Obtain GUA via DHCPv6/stateless autoconfig.

1.3.1.5 Static Routing

1.3.1.6 Adding a Static Route

Markdown

```
[Huawei] ipv6 route-static <dest-ipv6-address> <prefix-length> {<interface-type> <interface-number> [<nexthop-ipv6-address>] | <nexthop-ipv6-address>} [preference <preference>]
```

> Define static routes.

1.3.1.7 Display Commands

Command	Description
`display ipv6 interface [<interface-type> <interface-number> | brief]`	Show IPv6 details of interfaces.
`display ipv6 neighbors`	List neighbor entries (similar to ARP in IPv4).

1.3.1.8 Router Advertisement (RA) Messages

1.3.1.8.1 Enabling RA Messages on an Interface

Note

By default, Huawei routers do not send ICMPv6 RA messages necessary for SLAAC. To enable this function:

- `[Huawei-GigabitEthernet0/0/0] undo ipv6 nd ra halt` : Allow the interface to send RA messages.

SDN and NFV Overview

1 SDN and NFV Overview

1.1 SDN Overview

1.1.1 Evolution of the Computer Era

1.1.1.1 Mainframe to PC Transition

- `IBM System/360` : Beginning of mainframes with centralized architecture.

> Mainframes are powerful, large-capacity computers designed for handling and processing vast amounts of data for numerous users simultaneously in a centralized manner.

IBM

It's like having one really big brain that many smaller computers or users can tap into to get their various jobs done, from processing bank transactions to handling airline reservations.

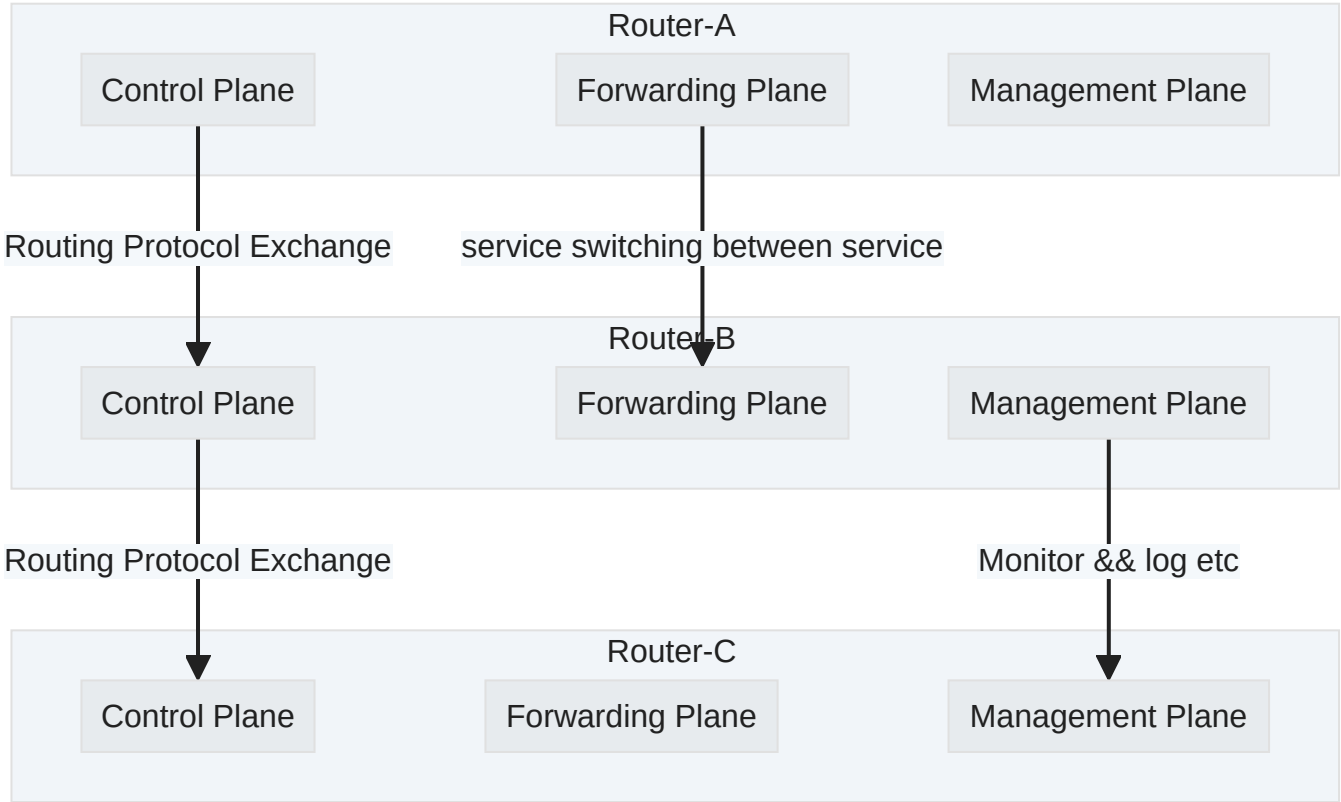
- PCs introduced hardware innovations, OS development, and application changes.
- Three factors contributed to PC ecosystem rapid innovation:
  - Hardware substrate (x86 instruction set)
  - Software-defined upper-layer applications
  - Open-source model (Linux)

1.1.1.2 Network Industry Development

> Reflecting on IT industry transformations, the network industry proposes SDN and aims for more open, flexible networks.

1.1.1.3 Current Situation in Network Industry

1.1.1.3.1 Typical IP Network Structure



- Distributed network with peer-to-peer control.

> A distributed network with peer-to-peer control is a type of computer network where each participant (peer) can communicate directly with others and share resources without needing a central server.

- **Benefit:** Different suppliers' products work together and are reliable.

1.1.1.3.2 Challenges in Typical Networks

1.1.1.3.2.1 Frequent Network Congestion

Problem with Solution's

1. **Problem**: In networks, the shortest path routing often neglects bandwidth availability, leading to congested routes and packet loss. For

instance, router C's direct route to D may be the shortest but could lack sufficient bandwidth for traffic demands.

- **Solution**: To optimize network efficiency, routing algorithms should factor in link bandwidth usage. This approach would balance the load by potentially rerouting traffic through underutilized paths with adequate bandwidth, such as going from C to A, then A to D, ensuring a smoother data flow.

2. **Problem**: Tunnel creation in networks can fail if it's based on a fixed sequence that does not account for live bandwidth conditions. For example, when Tunnel 3 from C-H is set up without considering current network load, it might encounter a bottleneck.
   - **Solution**: Tunnels should be established using a dynamic selection process that evaluates real-time bandwidth. If the preferred path for Tunnel 3 lacks capacity when needed, the system should identify alternative routes or postpone tunnel establishment until the network can accommodate the additional traffic.

1.1.1.3.2.2 Complex Technologies

- Increasing complexity with many protocols and commands to learn.

1.1.1.3.2.3 Difficult O&M (Operations & Maintenance)

> Too dependent on manual fault identification leads to delayed responses. Preventive analysis is lacking.

1.1.1.3.2.4 Slow Service Deployment

Traditional Method

- Traditional network policy changes are complex and not user-friendly.
- Adding a new network service is slow and requires widespread manual adjustments.
- Physical networks lack automatic setup, demanding hands-on configuration for every device.

The improved process aims for:

- Devices can move around the network without problems if they follow the rules.
- New services can be launched rapidly with minimal manual setup.
- Zero Touch Provisioning enables new devices to self-configure upon connection to the network.

1.1.2 SDN (Software-Defined Networking) Overview

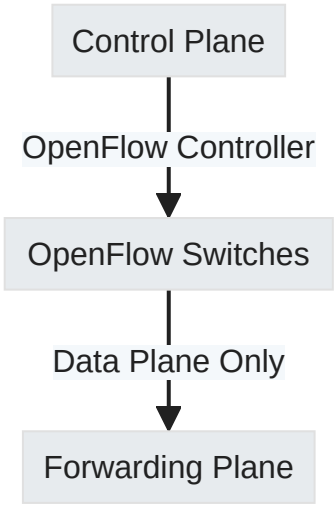
1.1.2.1 Origin

- Developed by Clean Slate Program at Stanford University.
- Aims to separate control and data planes for centralized control.

1.1.2.2 Characteristics

- Forwarding-control separation.
- Centralized control.
- Open programmable interfaces.

1.1.2.3 Core Concept



1.1.2.4 SDN Applications

1.1.2.4.1 Control Plane Functions

- Provided by the controller (e.g., OpenFlow controller).

1.1.2.4.2 OpenFlow Protocol

1.1.2.4.2.1 Message Types

---

1. **Controller-to-Switch:** Manage/query switch info.

> Like modify Configuration ,Modify-State etc

2. **Asynchronous:** Initiated by switch upon status change.

3. **Symmetric:** Can be initiated by both switch and controller (e.g., Hello, Echo, Error messages).

Packet details

- **Hello:** A greeting message to establish communication between devices.
- **Echo:** A request and response to confirm connectivity.
- **Error:** Notification of problems encountered during communication or processing.

1.1.2.4.3 Flow Table Overview

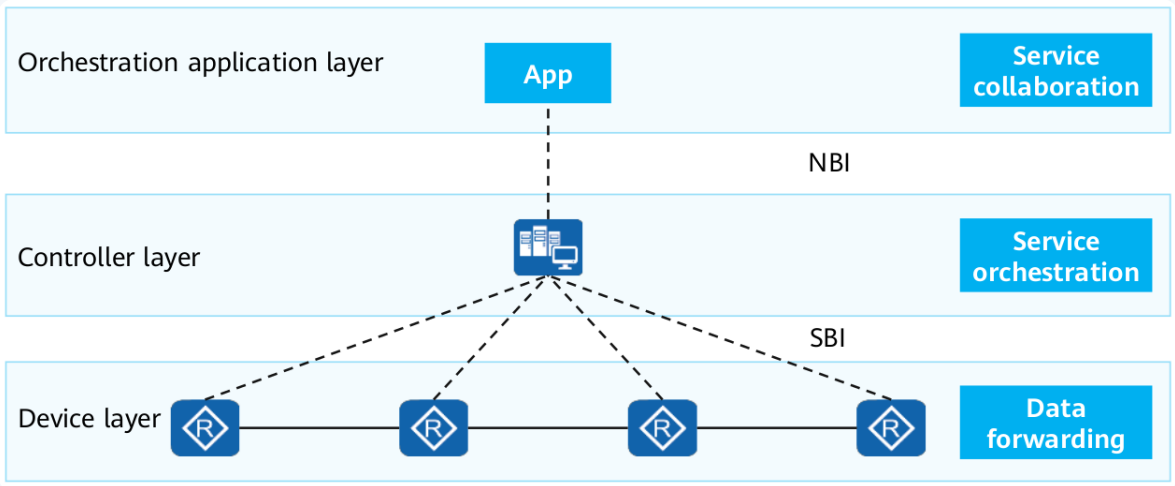
	Field
Match Fields	Criteria used to match incoming packets (e.g., source IP, destination IP, TCP/UDP ports).
Priority	Determines the order in which flow entries are considered. Higher priority entries are checked first.
Counters	Track how many packets and bytes have hit a particular flow entry.
Instructions	Actions to take when a packet matches the entry (e.g., forward, modify, drop).
Timeouts	Determine how long a flow entry remains active in the absence of matching packets (Idle) or unconditionally (Hard).
Cookie	A unique identifier for the flow entry set by the controller.
Flags	Additional settings that control various aspects of flow entry behavior (e.g., overwrite protection).

> OpenFlow switches forward packets based on flow tables.

Difference Routing table VS Flow table

- A routing table guides a router on where to send packets next based only on their destination IP address, Routing table entries are derived from routing protocols among devices, with packets routed using the longest match rule, and a device maintains a single routing table.
- A flow table in an OpenFlow switch allows for multifaceted packet handling, directing actions based on diverse criteria including multiple packet fields(like source IP, destination IP, TCP/UDP ports, etc.), Flow tables, created by an OpenFlow controller, are dynamic in length and detail match-forward criteria, with a network device hosting multiple flow tables.

1.1.2.5 Huawei SDN Network Architecture



1.1.2.5.1 Layers

1. **Orchestration Application Layer:** Higher-level services like OSS and OpenStack.

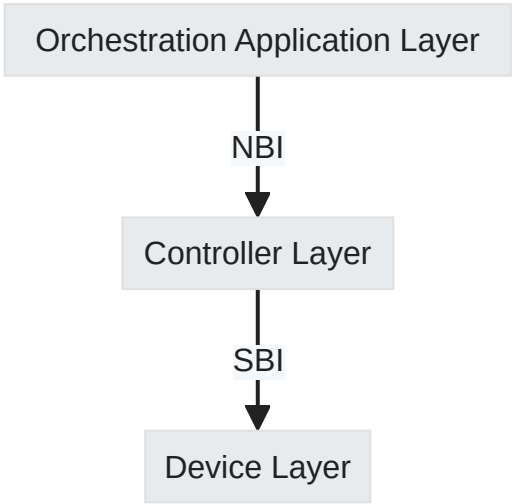
- **OSS (Operational Support System):** refers to software used by telecommunications service providers to manage their networks and

services
- **OpenStack:** is an open-source cloud computing platform for creating and managing large groups of virtual private servers in a data center.

2. **Controller Layer:** Brain of the SDN system; implements network service orchestration , decision-maker that manages and directs network traffic by telling network devices how to handle data packets.
3. **Device Layer:** Performs forwarding based on controller instructions.

1.1.2.5.2 Interfaces

- **NBIs (Northbound Interfaces):** RESTful, used between orchestration(app) layer and controller layer.
- **SBIs (Southbound Interfaces):** Protocols like NETCONF, SNMP, OpenFlow used between device layer and controller layer.



1.1.2.6 Huawei SDN Solution

> Huawei's approach integrates Management, Control, and Analysis to build Intent-Driven Networks across various domains such as DC Fabric,

> Campus Networks, and Branch Interconnection (SD-WAN).

TIP

- **Cloud platform:** A system that controls networking, processing power, and data storage in a data center, with OpenStack being a popular open-source option.
- **Element Management System (EMS):** A software that handles operations for specific types of telecom equipment.
- **Orchestration (container orchestration):** Software like Kubernetes that manages and organizes containers, which are lightweight virtual environments for running applications.

> A container bundles an application with all its necessary components to ensure it works consistently across different computing environments.

- **MTOSI/CORBA:** Standards used to integrate with Business Support Systems (BSS) or Operational Support Systems (OSS) in telecommunications.
- **Kafka/SFTP:** Technologies used to transfer data securely to big data platforms; Kafka is for real-time data streaming, while SFTP is for secure file transfer.

1.1.2.7 iMaster NCE (Network Cloud Engine)

A platform that integrates management, control, analysis, and AI capabilities.

Features:

1. AI-based analysis for prediction/troubleshooting.
2. Unified database with full lifecycle management capabilities.
3. Autonomous Driving Network System integrating NMS (Network Management System), controllers, analyzers.

Applications:

1. Data Center Networks - iMaster NCE-Fabric
2. Enterprise Campus - iMaster NCE-Campus
3. WAN & Transmission - iMaster NCE-WAN/T/IP

1.1.2.7.1 Simplified Deployment

- Service intent self-understanding and conversion.
- Network change simulation eliminates human errors.

1.1.2.7.2 Intelligent Operations & Maintenance (O&M)

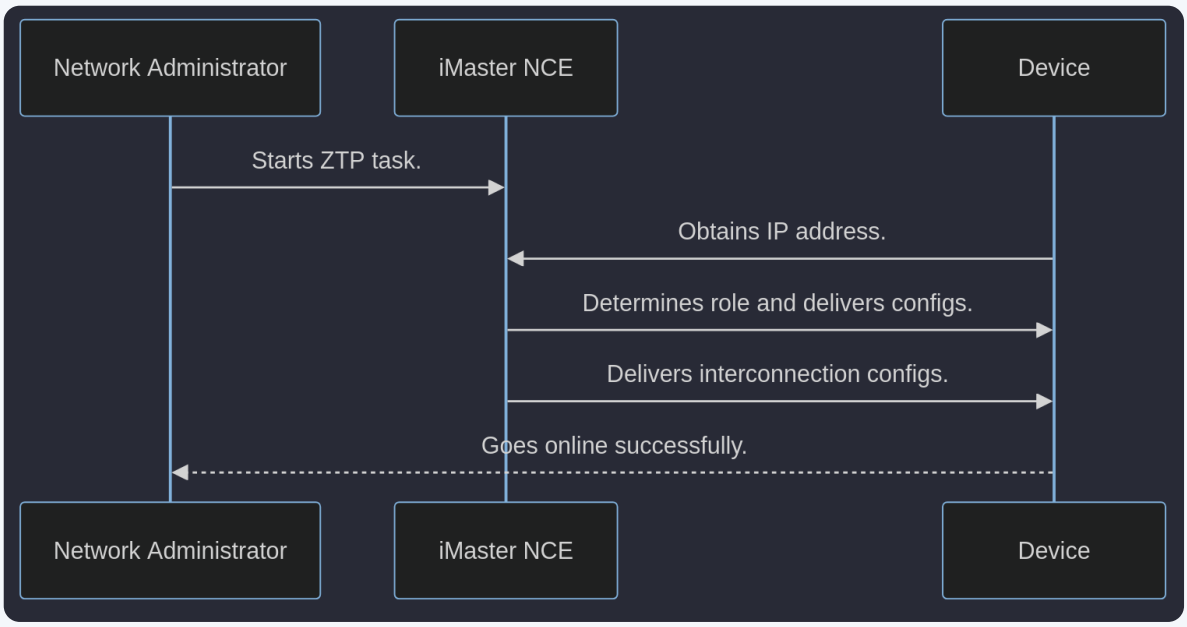
- **Rapid Fault Detection**: Knowledge graph and expert experience.
- **Fast Fault Rectification**: Expertise and simulation analysis.

1.1.2.7.3 Real-time Optimization

> Real-time AI-Fabric-oriented local traffic inference and model optimization.

1.1.2.7.4 Simplified ZTP (Zero Touch Provisioning) Deployment Process

---



1.1.2.7.5 Fast Service Deployment with iMaster NCE-Fabric

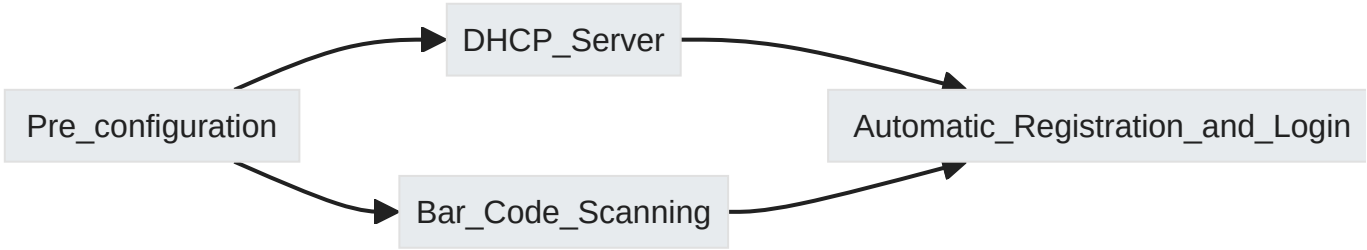
1.1.2.7.5.1 Workflow for Service Deployment

1. Determine the specific requirements and settings for the service deployment.
2. Configuration Delivery through NETCONF

1.1.2.7.5.2 Network Change Simulation and Risk Prediction

- **Resources Sufficiency**: Validates live network resources during changes.
- **Access Connectivity**: Ensures network integrity post-change.

1.1.2.7.5.3 Plug-and-Play Device Deployment Techniques



> Different ways that new devices can be quickly added to networks with minimal effort required from people setting them up – plug them in

1.1.2.7.5.4 Security Group Policies for Free Mobility

> Free mobility ensures consistent network rights regardless of user location or IP address`

1.1.2.7.5.5 Converged Wired and Wireless Management (Native AC)

---

construction modes

Standalone AC Mode:

- A single device manages the Wi-Fi network but can get overwhelmed, leading to potential network issues.

Independent AC Mode:

- A card is added to a switch for Wi-Fi control, with separate management for wired and wireless networks.

Wired and Wireless Convergence (Native AC):

- The switch itself can handle both wired and Wi-Fi networks, reducing bottlenecks and simplifying management.

1.1.2.7.6 AI-Powered Intelligent O&M of Campus Networks

> Shifting from focusing on the machines themselves to prioritizing the user's experience, by using advanced data collection methods (elemetry-based second-level data collection.) like remote sensors to gather more detailed information about how systems are functioning.

1.1.2.7.7 AI-Powered Intelligent Radio Calibration

> AI-powered radio calibration helps wireless networks work better by continuously adjusting settings in real-time for optimum performance without needing a human to manually intervene.

1.2 NFV Overview

1.2.1 Origin of NFV

> - Initiated by top carriers in October 2012 with the release of an NFV White Paper.
> - ETSI NFV ISG founded to define network virtualization requirements and system architecture.

1.2.1.1 Standard Organizations

- `ETSI NFV ISG` : Formulates requirements and functional frameworks.
- `3GPP SA5` : Focuses on virtualization management (MANO-related).
- `OPNFV` : Provides an open-source platform to accelerate market adoption.

1.2.2 NFV Value Proposition

1.2.2.1 Benefits for Carriers:

> - **Shortened service rollout time**: Carriers can introduce new services to customers faster.
> - **Reduced network construction cost**: Carriers can build networks more cheaply.
> - **Improved network O&M (Operations & Maintenance) efficiency**: Carriers can manage and fix their networks more easily and quickly.
> - **Open ecosystem**: Carriers can work with a variety of equipment and software providers, leading to more choices and flexibility.

1.2.3 Key Technologies

1.2.3.1 Virtualization

> **NFV (Network Function Virtualization)**, allows network services that used to require dedicated hardware to run as virtual machines on general-purpose servers.

- **Features:**

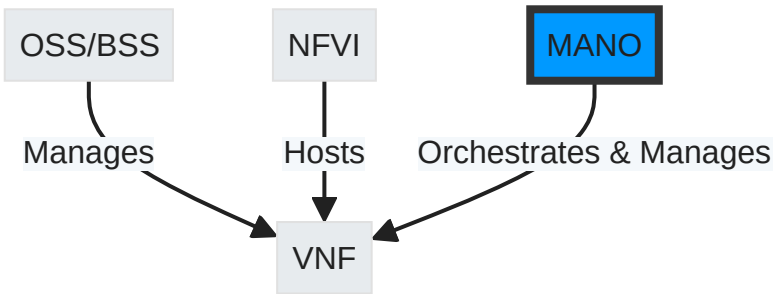
- **Partitioning:** Dividing a physical server into multiple virtual machines that can operate independently.
- **Isolation:** Each virtual machine is kept separate so that the activities in one do not affect others.
- **Encapsulation:** Wrapping up a network function within a virtual machine so that it contains all necessary components and can be easily moved or managed.
- **Hardware Independence:** NFV allows these network functions to run on different types of physical servers, not tied to any specific hardware brand or configuration.

1.2.3.2 Cloudification

Characteristics as defined by NIST:

1. On-demand self-service.
2. Broad network access.
3. Resource pooling.
4. Rapid elasticity.
5. Measured service:a pay-per-use or charge-per-use model.

1.2.4 Introduction to NFV Architecture



1.2.4.1 Layers of Architecture:

1. `OSS/BSS` : These are systems used by telecom companies to support various processes such as managing the network (OSS for Operational Support Systems) and handling billing, customer relations, and business processes (BSS for Business Support Systems).
2. `NFVI` : The Network Functions Virtualization Infrastructure is like a virtual foundation in cloud computing that provides basic resources such as computing power, storage, and networking capabilities. It uses standard servers and cloud management software (CloudOS) to create these resources.
3. `VNF` : A Virtual Network Function is a way to run network services that traditionally required dedicated hardware (like routers or firewalls) as software applications on top of NFVI like VM.
4. `MANO` : This stands for Management and Orchestration. It's an overarching framework in charge of organizing, setting up, and maintaining various components in NFV environments:
    - NFVO: Network Functions Virtualization Orchestrator manages the overall functioning and deployment of network services.
    - VNFM: VNF Manager handles the lifecycle management of VNF instances.
    - VIM: Virtualized Infrastructure Manager manages the interaction with the infrastructure resources like compute, storage, and network.

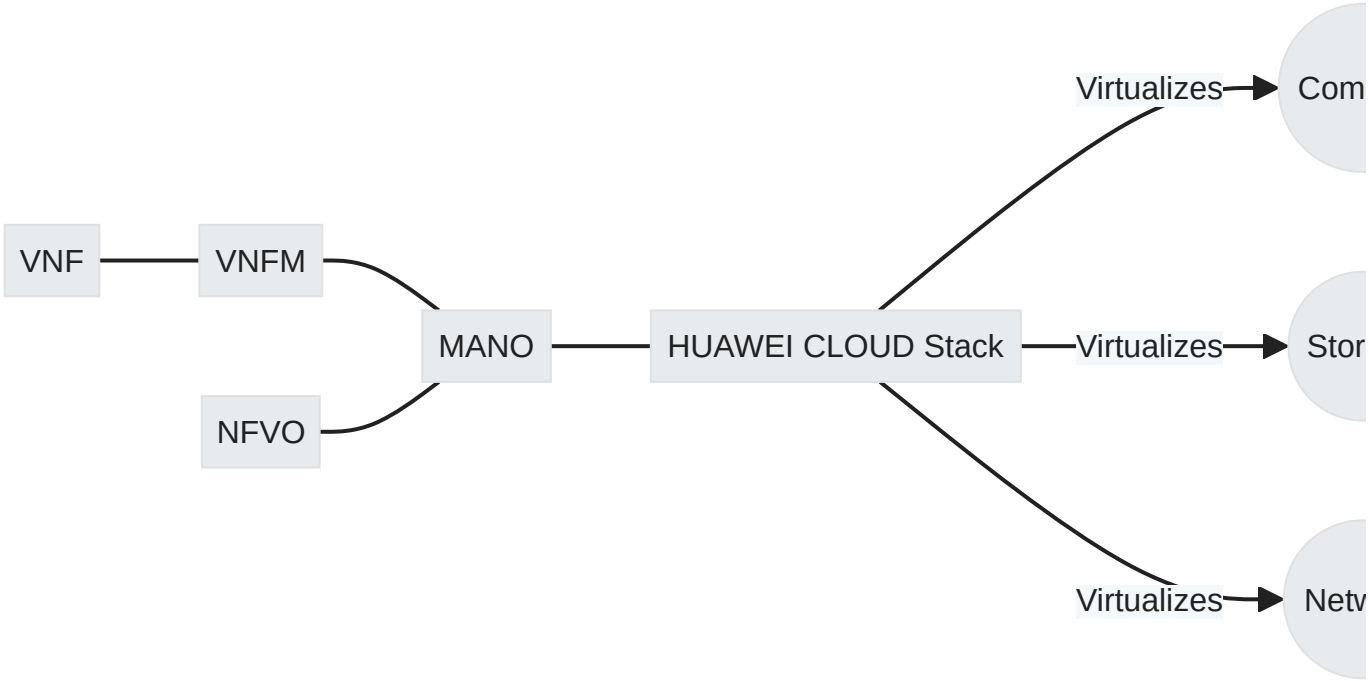
1.2.5 Standard NFV Architecture by ETSI

1.2.5.1 Reference Points:

- `Vi-Ha` , `Nf-Vi` , `Ve-Vnfm` , etc.: Interfaces between different components like VIM, VNFM, VNFs, and hardware.

Reference Point	Description
Vi-Ha	VMs deployment compatibility with NFVI
Nf-Vi	Management of virtual systems within NFVI
Ve-Vnfm	Lifecycle management interface between VNFM and VNF

1.2.6 Huawei's Approach to NFV Solution



- HUAWEI CLOUD Stack implements functions of virtualization layer and VIM.
- Offers solutions for various carriers' networks like wireless, transport, core networks.

Network Programmability and Automation

1 Network Programmability and Automation

1.1 Introduction to Network Programmability and Automation

1.1.1 Typical O&M Scenarios

1.1.1.1 Device Upgrade

- Perform periodic batch upgrades on thousands of live network devices.

1.1.1.2 Configuration Audit

- Annual audits to ensure compliance (e.g., STelnet enabled, spanning tree security configured).

1.1.1.3 Configuration Change

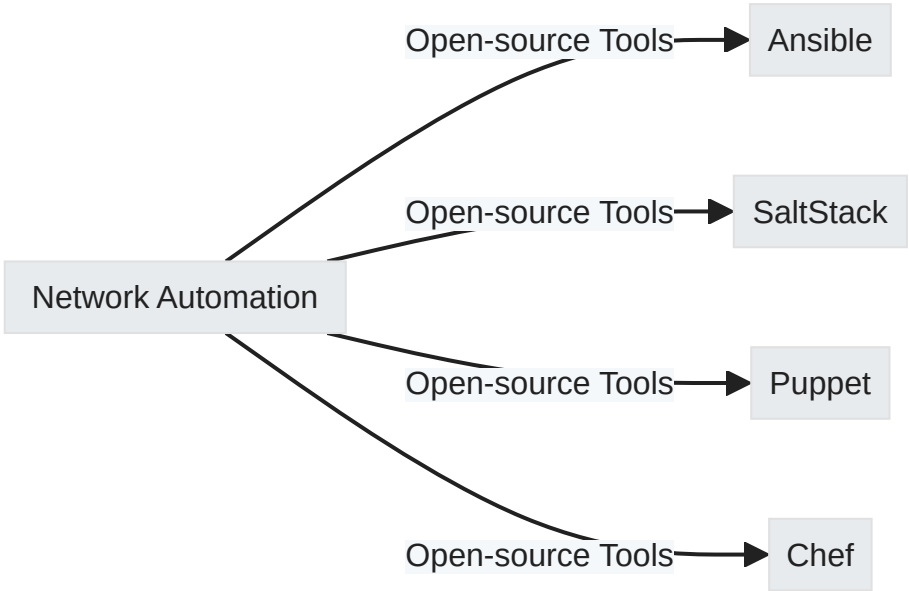
- Regularly update device accounts and passwords due to security requirements.

1.1.2 Network Automation

1.1.2.1 Introduction

> Network automation reduces human dependency by using tools for automated deployment, operations and O&M.

1.1.2.2 Tools for Automation



- Recommended to acquire **coding skills** for network engineering capability construction.

1.1.3 Programming-based Network Automation

1.1.3.1 Python as a Skill Requirement

- Python is essential for writing automation scripts that handle repetitive and rule-based tasks.

1.1.3.2 Automated Device Configuration Example

---

1. **Write Configuration File**

```yaml
Sysname SW1
Vlan 10 description A
Vlan 20 description B
VLAN 30 description C
```

2. **Push Configuration with Python**
   - Establish SSH/Telnet connection.
   - Upload configuration script to the network device.

1.1.3.3 Python Scripting Basics

```python
# Python pseudo-code example for pushing configuration:
import some_ssh_library

def push_config(device_ip, config_file):
    # Establish SSH connection to the device using the library's functions.
    # Open the config file and read the commands.
```

```
    # Iterate over commands and execute them on the device via SSH.
    pass  # Implementation details here.
```

1.1.3.4 Benefits of Network Automation

> With network automation, configurations can be deployed more efficiently and consistently across multiple devices.

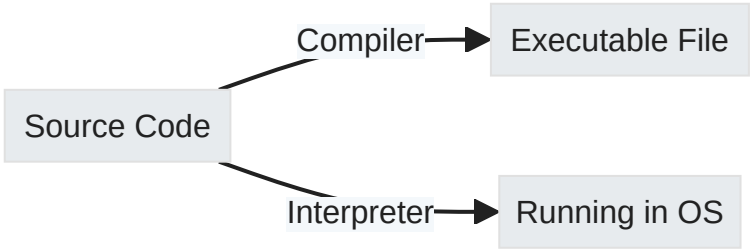
1.2 Overview of Programming Language and Python

1.2.1 Overview

- Programming languages control computer behavior.
- Classified into **compiled** and **interpreted** languages.
- **Based on language levels:** machine language, assembly language, high-level language.

1.2.2 Compiled vs. Interpreted

- **Compiled:** Translated into machine code before execution (e.g., C/C++).
- **Interpreted:** Translated at runtime, line by line (e.g., Python).



1.2.3 Language Level Classification

1.2.3.1 Machine Language

- Consists of `0` and `1` instructions.

1.2.3.2 Assembly Language

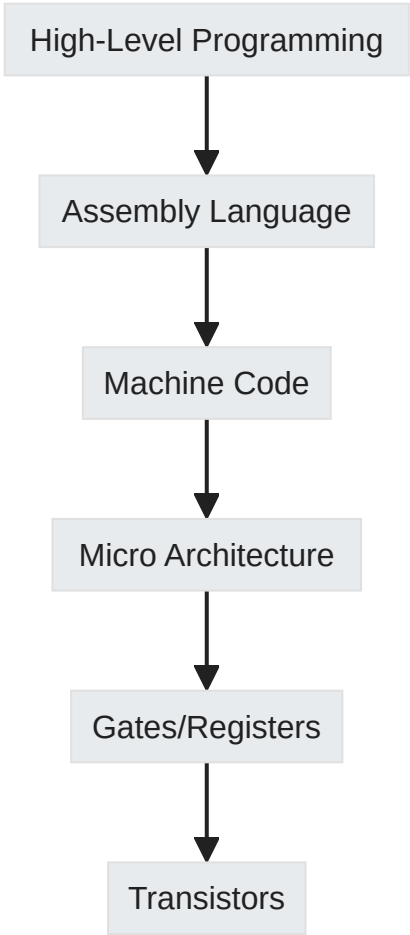
- Encapsulates hardware instructions for readability (e.g., `MOV`, `ADD`).

1.2.3.3 High-Level Language

- Includes languages like Java, Python.
- Requires translation to machine code.

> - **JVM:** Java virtual machine
> - **PVM:** Python VM

1.2.4 Computing Stack & Program Execution



1.2.5 Python Overview

> Python is a high-level interpreted language created by Guido Van Rossum.

1.2.5.1 Advantages & Disadvantages of Python

Advantages & Disadvantages

- **Advantages:**
  - Python is written clearly and is easy to read.
  - It can be used in different ways, both simple and complex.
  - There are lots of extra tools you can get to do more things.

- **Disadvantages:**
  - It can run slowly because it processes one instruction at a time.

1.2.6 Python Execution Process

---

1. Install the Python environment on the operating system.
2. Write the source code `.py`.
3. Compiler generates bytecode `.pyc`.
4. Python VM executes bytecode.

Python

```python
# Example Code Block:
temp = v[k]
v[k] = v[k+1]
v[k+1] = temp
```

1.2.7 Getting Started with Python

1.2.7.1 Interactive Mode

Enter commands directly into the interpreter:

Python

```python
>>> print("hello world")
hello world
>>> a = 1; b = 2; print(a + b)
3
```

1.2.7.2 Script Mode

Write scripts and execute them:

```shell
$ python demo.py # Executes script demo.py containing python code.
```

demo.py:

```python
print("hello world")
a = 1; b = 2; print(a + b)
```

1.2.8 Code Style Guide for Python

1.2.8.1 Indentation & Comments

- Use four spaces per indentation level.
- Single-line comments start with `#`.
- Multi-line comments use triple quotes `"""`.

1.2.8.2 Identifier Naming Rules

Identifiers should start with a letter or underscore:

Correct	Incorrect
user_id	4user_id

1.2.9 Python Functions & Modules

Functions improve modularity; modules contain reusable definitions:

Function Example:

```python
def greet():
    print("Hello World")
greet() # Outputs "Hello World"
```

Module Example:

demo.py:

```python
def sit():
    print('A dog is now sitting')
```

test.py:

```python
import demo
demo.sit() # Calls function from demo module.
```

1.2.10 Introduction to telnetlib

The `telnetlib` module in Python allows you to work with Telnet, a protocol used to establish a command-line interface connection to remote computers over the internet or local networks.

```python
from telnetlib import Telnet
tn = Telnet(host=None, port=0[, timeout])
tn.read_all()
```

Methods:

- `read_until(expected, timeout=None)` : Keep reading data until you find a specific text or until a certain amount of time has passed.
- `read_all()` : Keep reading data until there is no more coming (End Of File - EOF).
- `read_very_eager()` : Read any available data right away without waiting, but don't wait around for more data if there isn't any immediately available.
- `write(buffer)` : Send your own commands or data to the server.
- `close()` : End your Telnet session and close the connection.

1.3 Cases

1.3.1 Telnet Login Using telnetlib

1.3.1.1 Overview

- **Objective**: Log into a network device functioning as a Telnet server using Python's `telnetlib` .

1.3.1.2 Manual Verification

> Use terminal Telnet client for manual login verification.

1. Run command: `telnet 192.168.10.10`
2. Enter password when prompted.

Shell

```
C:\Users\Richard>telnet 192.168.10.10
```

```
Password:
Info: The max number of VTY users is 5...
<Huawei>
```

1.3.1.3 Python Code Example

```python
import telnetlib

host = '192.168.10.10'
password = 'Huawei@123'

tn = telnetlib.Telnet(host)
tn.read_until(b'Password:')
tn.write(password.encode('ascii') + b"\n")

print(tn.read_until(b'<Huawei>').decode('ascii'))
tn.close()
```

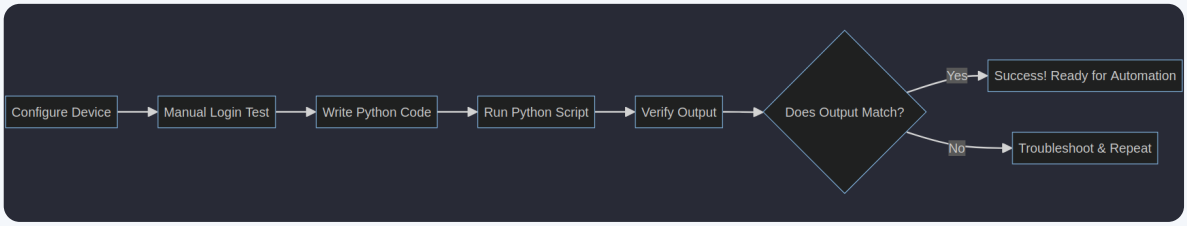
> In Python, use `.encode()` to convert strings to ASCII format required by telentlib; prefix byte strings with `b` (e.g., b'Password:') to denote bytes objects as per official requirements.

1.3.1.4 Code Explanation

- Importing module.
- Setting host IP and password.
- Creating a Telnet connection.
- Reading output until 'Password:' prompt.
- Sending encoded password followed by newline.
- Reading output until `<Huawei>` prompt appears.

- Closing the connection.

1.3.1.5 Mermaid Flowchart



Typical Campus Network Architectures and Practices

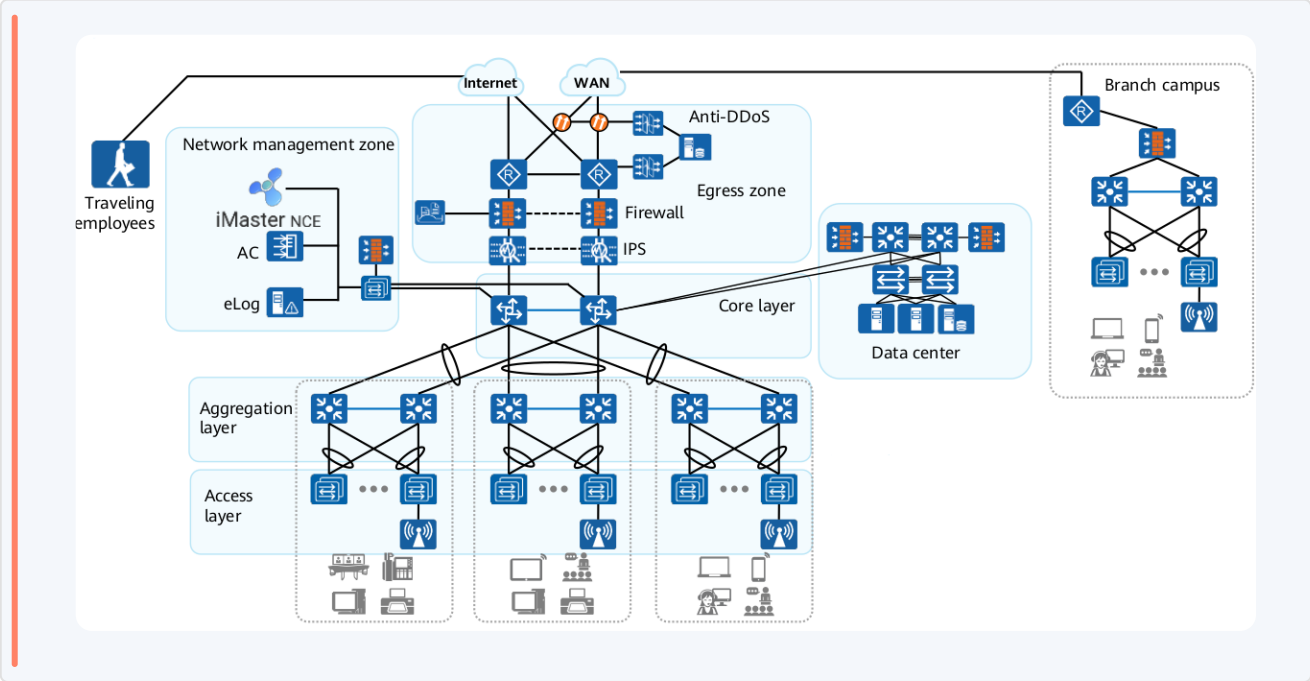
1 Typical Campus Network Architectures and Practices

1.1 Basic Concepts of Campus Networks

1.1.1 Definitions

- **Campus Network**: A collection of interconnected local area networks (LAN) within a limited geographic area, such as a university campus, corporate site, or industrial complex.
- **LAN**: Local Area Network designed to connect computers and other devices within a confined area.
- **MAN**: Metropolitan Area Network connecting multiple LANs over a city-wide geography.

1.1.2 Hierarchical Structure



1.1.2.1 Core Layer

- Backbone of the network.
- High-speed switching.
- Interconnects data centers, management centers, and campus egress points.

1.1.2.2 Aggregation Layer

- Middle layer for data aggregation.
- Provides routing, Quality of Service (QoS), and security functions.

1.1.2.3 Access Layer

- Connects end-users to the network.
- Handles direct communication with devices.

1.1.2.4 Egress Area

- Interface between campus network and external networks.
- Equipped with security devices like IPS and firewalls.

1.1.2.5 Data Center Area

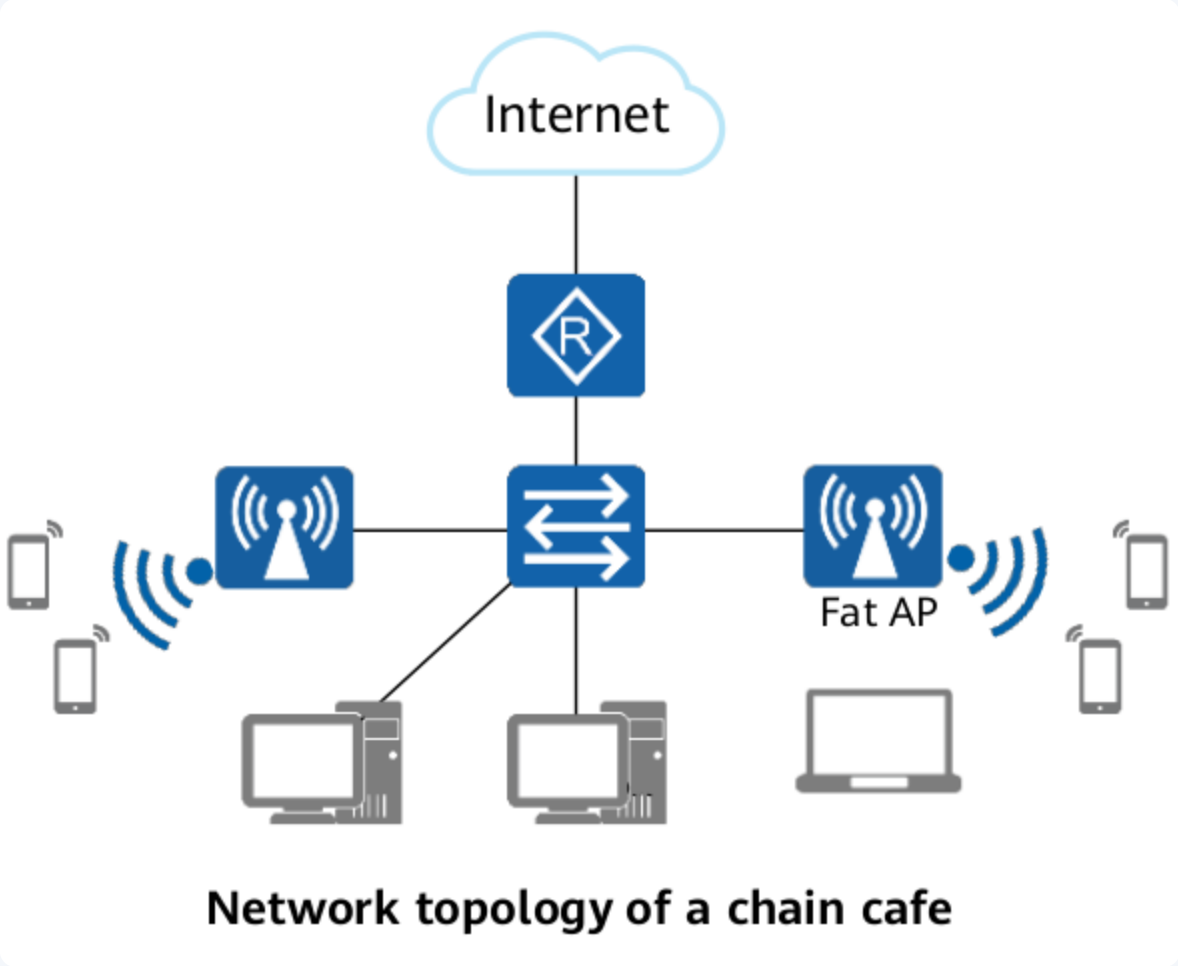
- Hosts servers and applications.
- Provides resources and services to users.

1.1.2.6 Network Management Area

- Contains systems for network oversight (SDN controller, WAC).

1.1.3 Scale Categories

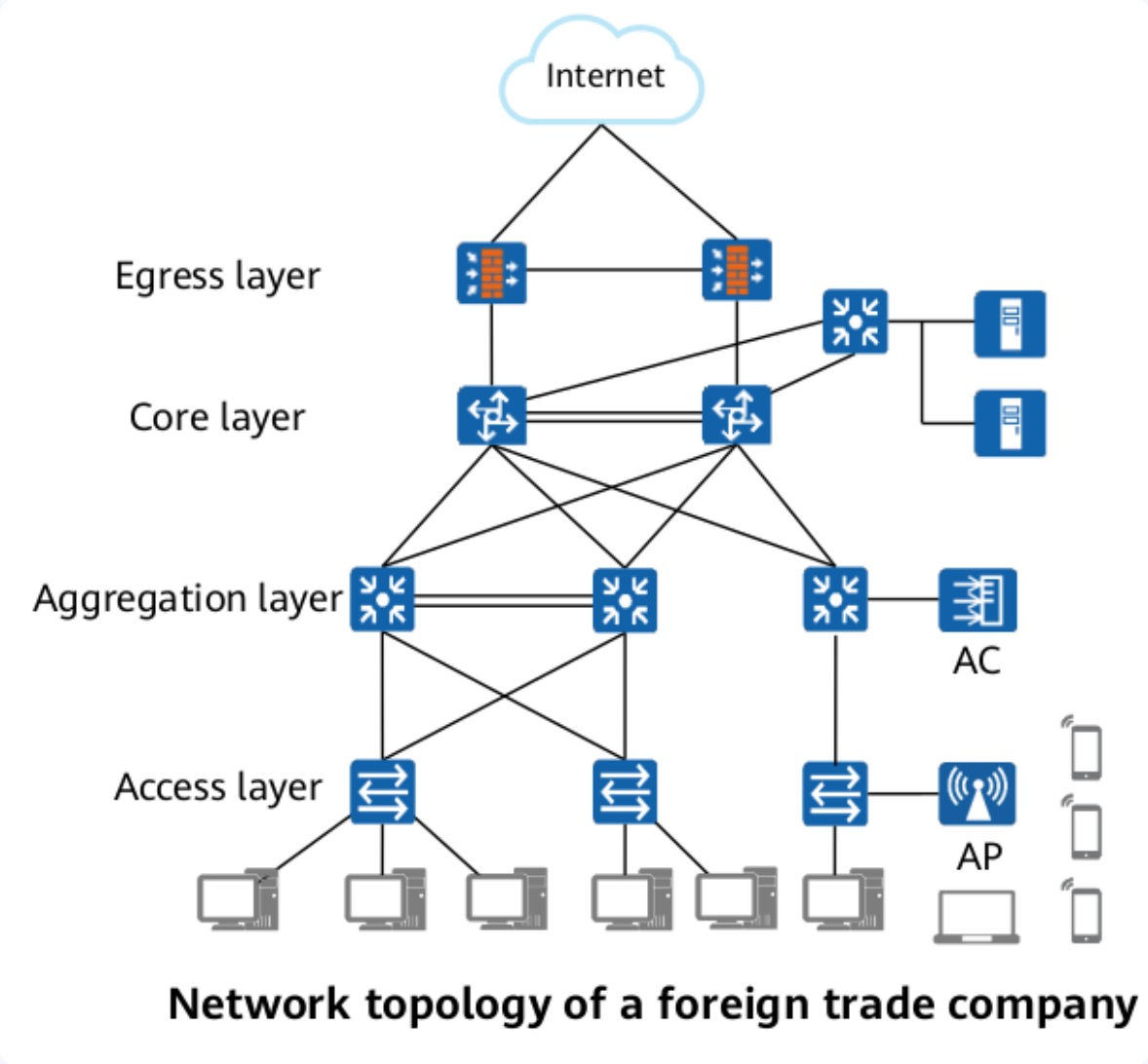
1.1.3.1 Small Campus Networks



Characteristics:

- Fewer users (several or dozens).
- Single location.
- Simple architecture.

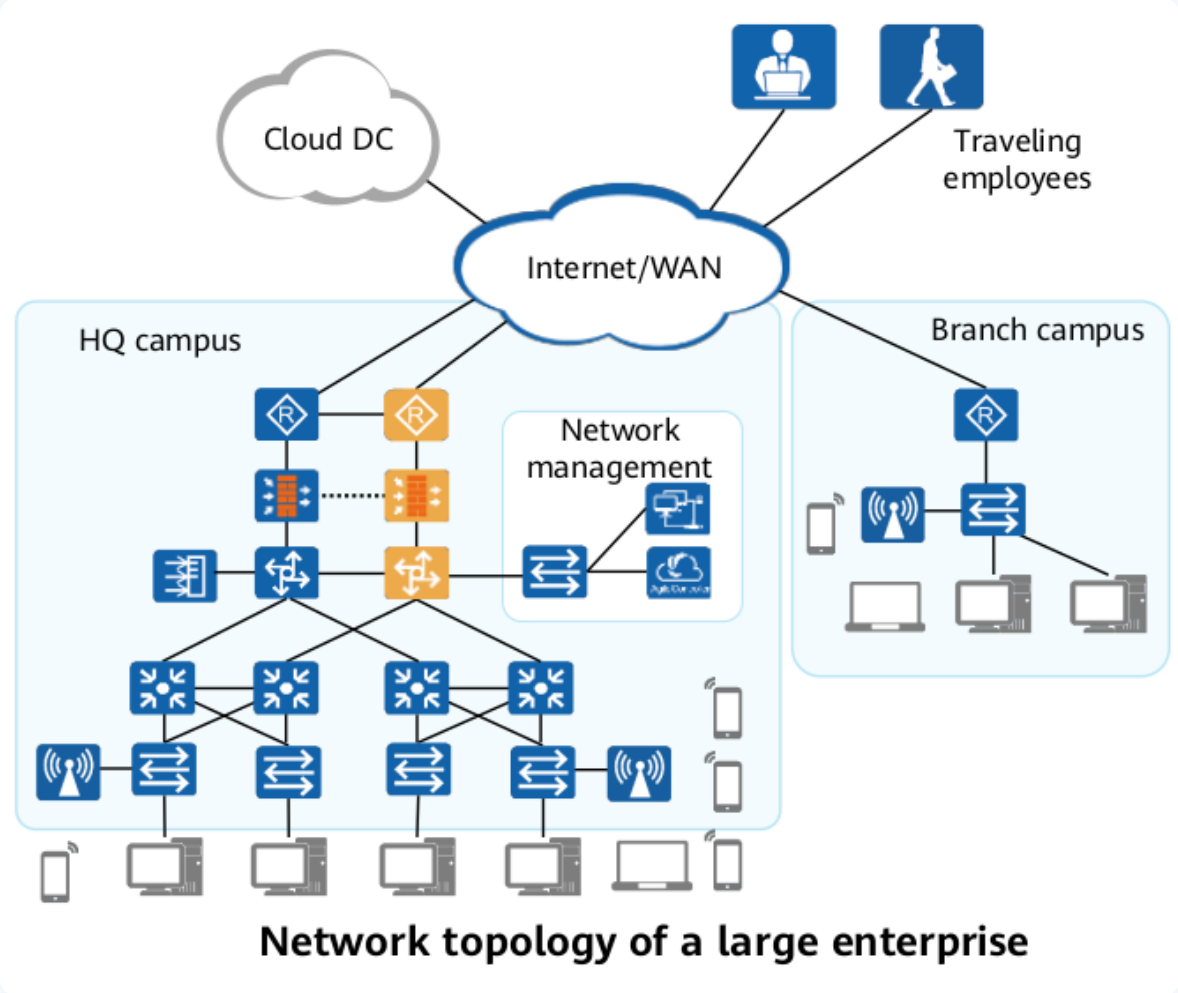
1.1.3.2 Midsize Campus Networks



Characteristics:

- Hundreds to thousands of users.
- Modular design with limited function partitions.
- **Three-layer architecture:** core, aggregation, access.

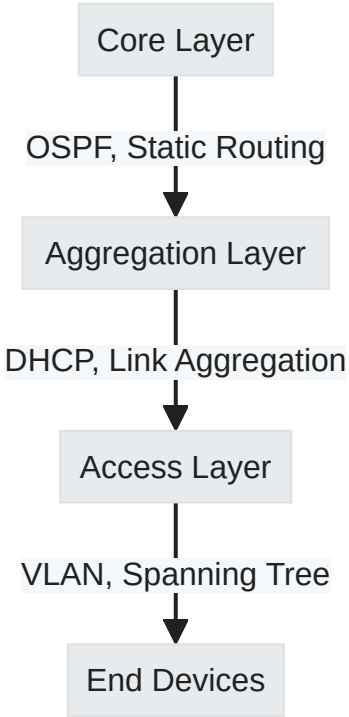
1.1.3.3 Large Campus Networks



Characteristics:

- Multiple buildings or campuses linked by WANs.
- Supports VPN access for traveling employees.

1.1.4 Key Protocols & Technologies



1.2 Campus Network Project Practice