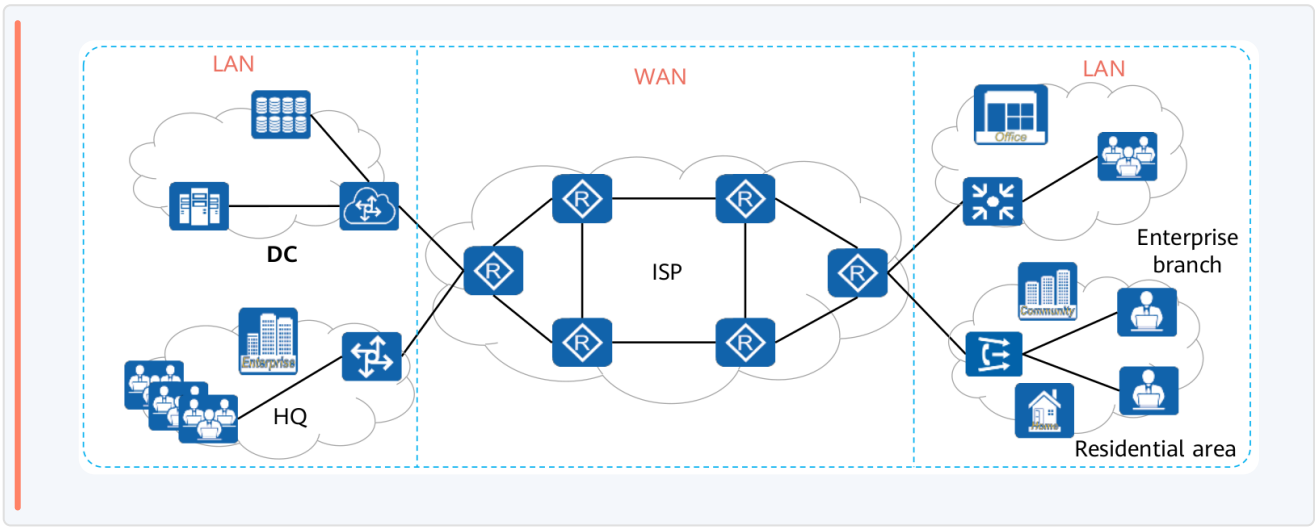
WAN Technologies

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

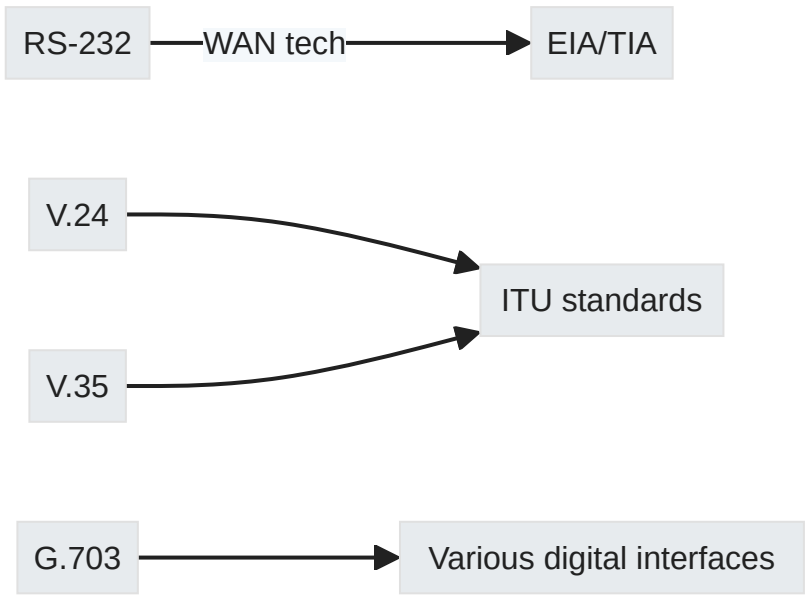
1.1.2.1 TCP/IP reference model layers:

- **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

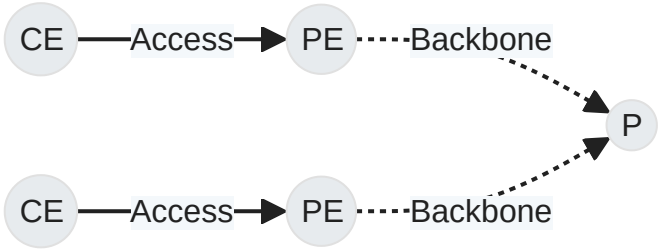
Protocol	Description
HDLC	Data packets encapsulated into frames; high reliability but lower efficiency; do not support IP address negotiation and authentication
PPP	Supports authentication; used on synchronous/asynchronous links
FR	Switched protocol with error-free check mechanism
ATM	Connection-oriented technology; uses 53-byte cells for information transmission

1.1.3 WAN Device Roles

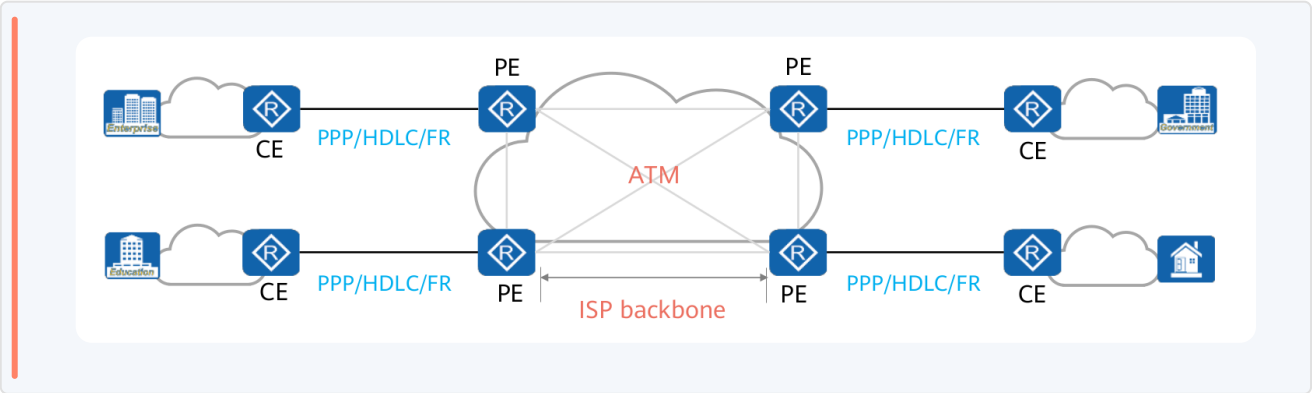
1.1.3.1 Basic Roles:

---

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.

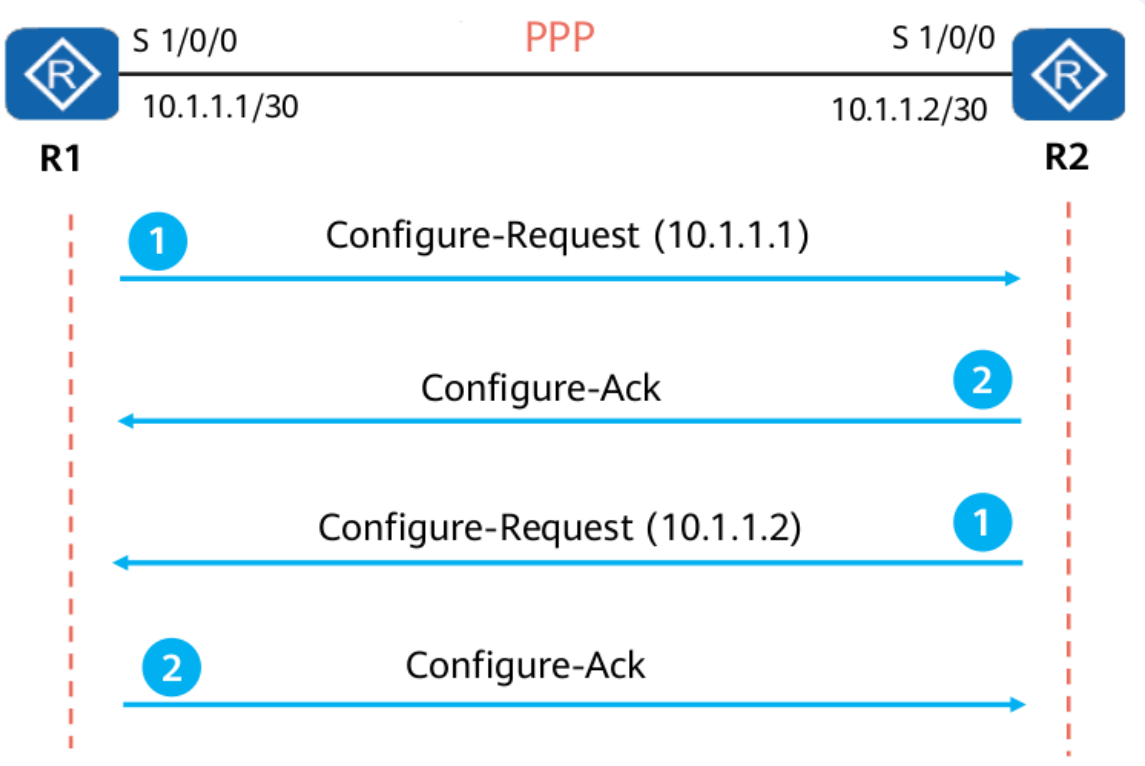
> The magic number detects loops by exchanging unique values between connected devices; if a device receives a packet with its own magic number since magic number is unique number, it knows the data has looped back. A loop can happen if the physical networking setup Accidentally creates a circular path for data, causing packets to travel in circles rather than reaching their destination.

1.2.1.2.2 Authentication Negotiation

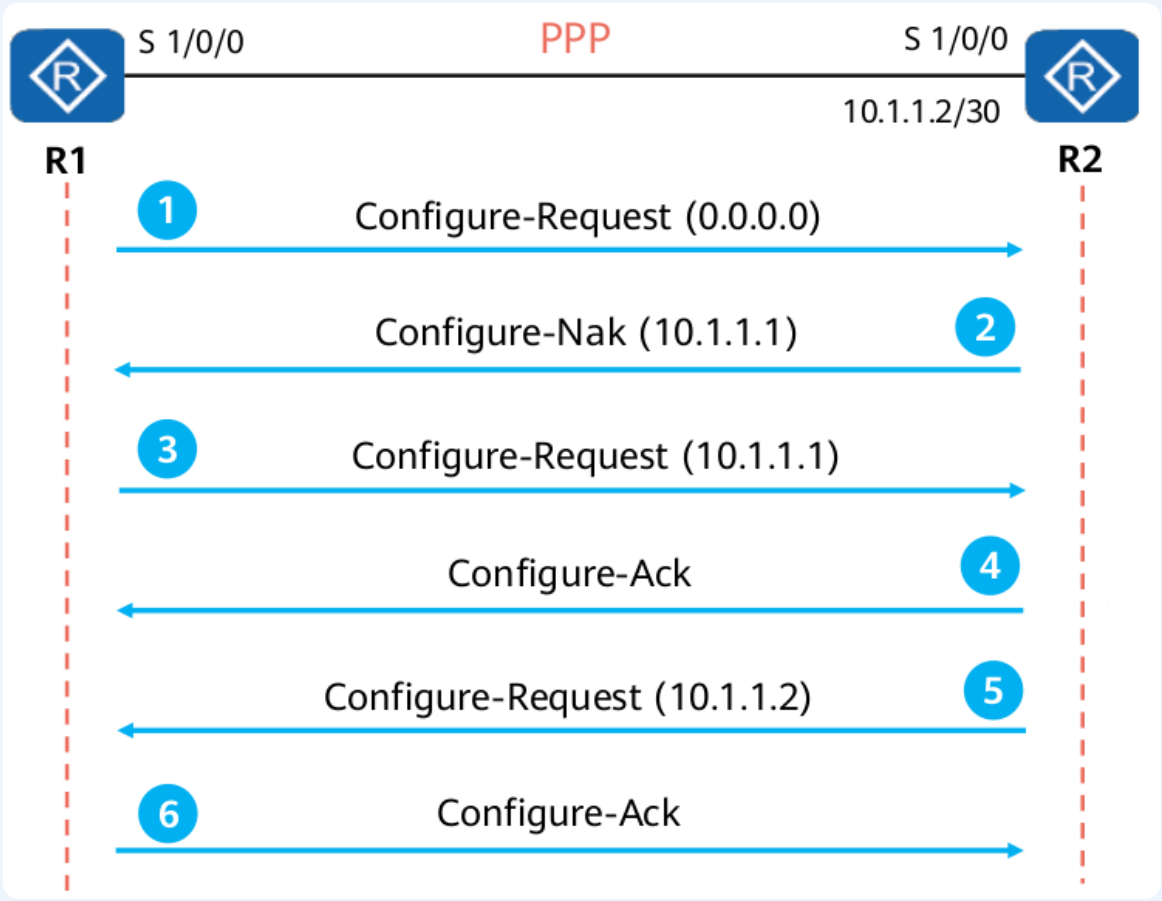
- `PAP` (Password Authentication Protocol) involves a two-way handshake with credentials sent in clear text.
- `CHAP` (Challenge Handshake Authentication Protocol) uses a three-way handshake with encrypted (MD5{ID+random number+password}) credentials.

1.2.1.2.3 NCP (Network Control Protocols) Negotiation

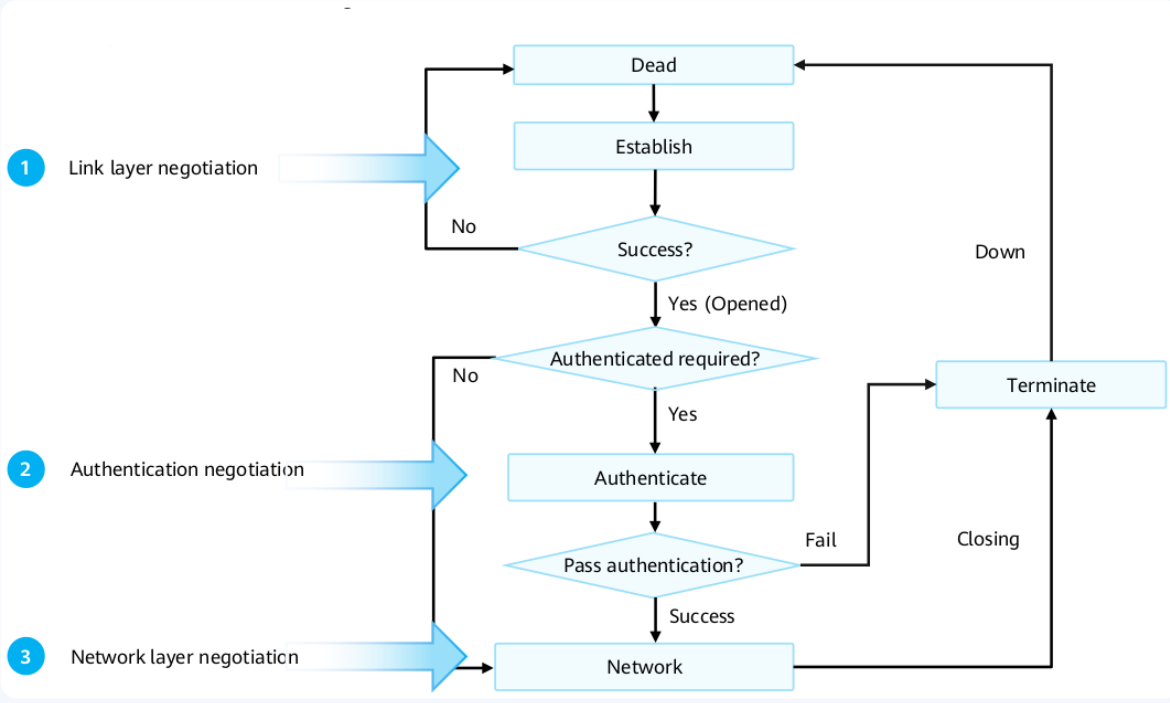
- Responsible for selecting and configuring network layer protocols like IP.
- Examples include `IPCP` for IP address configuration.

> **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

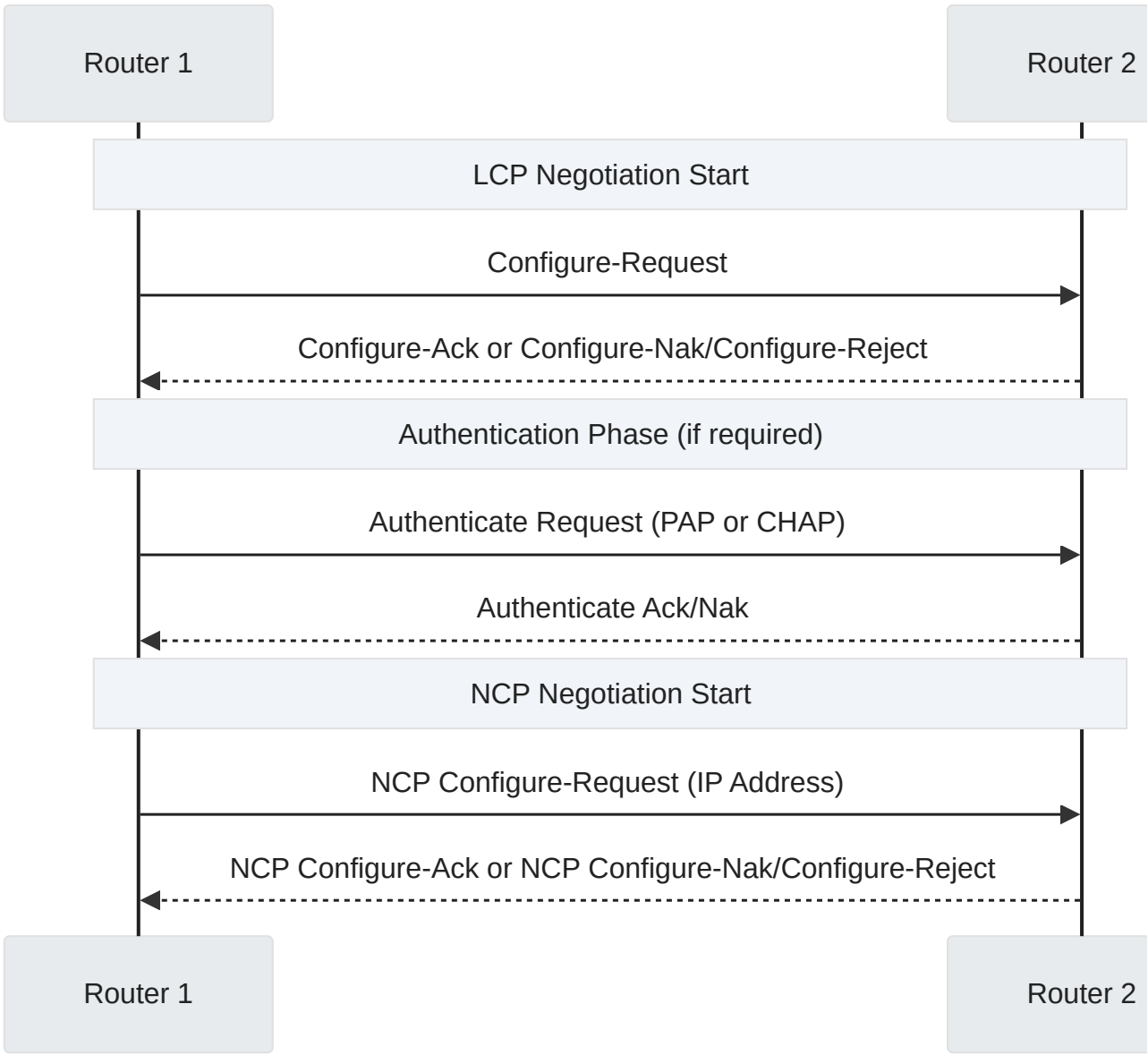
new address is acceptable.



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

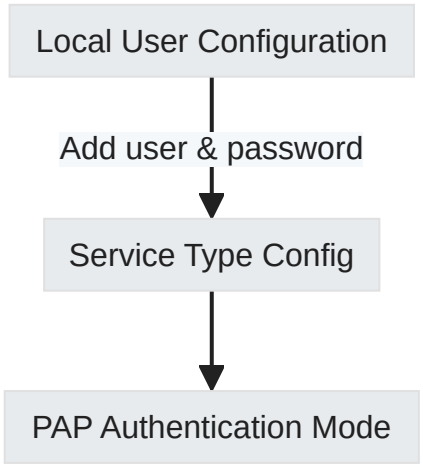
- Configure a negotiation timeout period (in seconds) with:

```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.

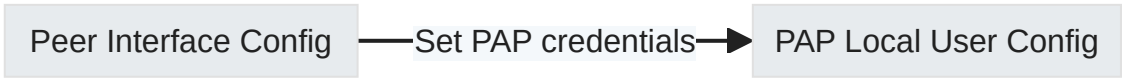
2. Set service type to PPP:

```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



- 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:

```
[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:

```
[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

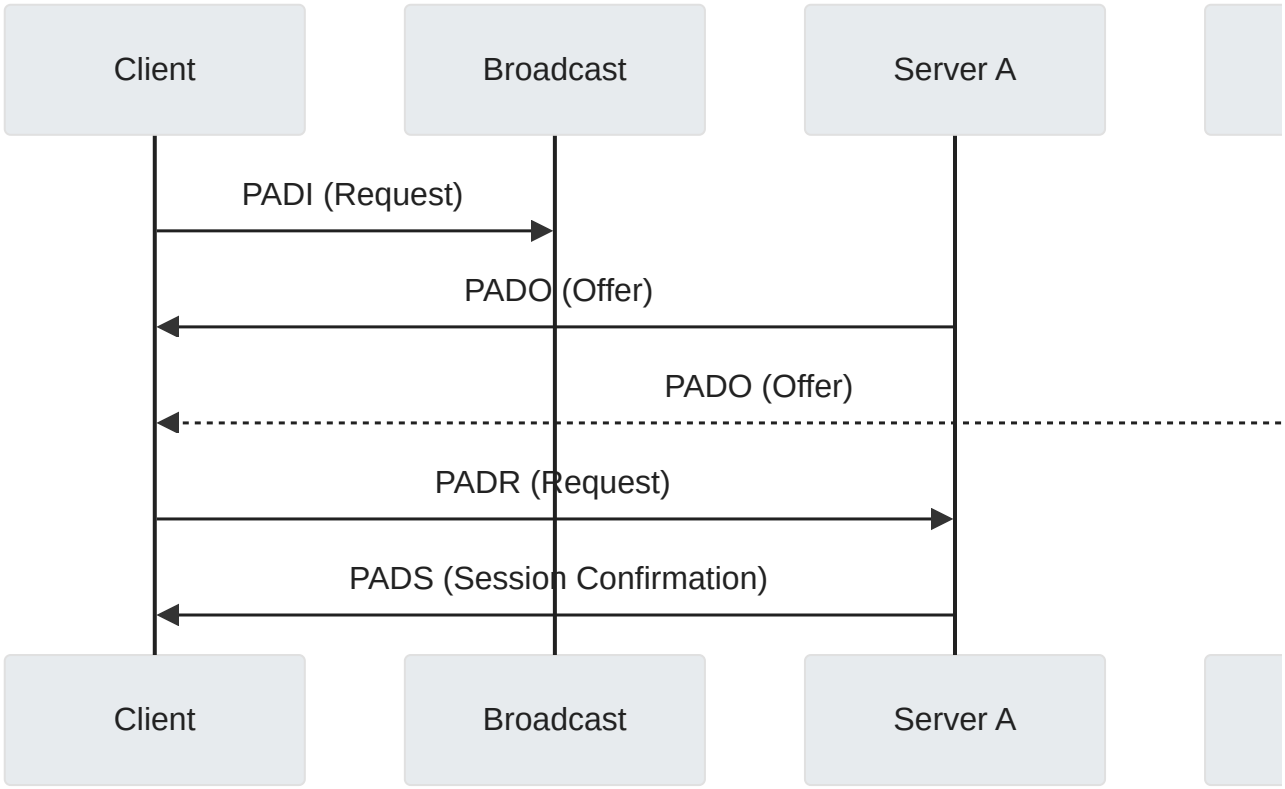
Code	Name	Description
0x09	PADI	PPPoE Active Discovery Initiation packet
0x07	PADO	PPPoE Active Discovery Offer packet
0x19	PADR	PPPoE Active Discovery Request packet
0x65	PADS	PPPoE Active Discovery Session-confirmation packet
0xa7	PADT	PPPoE Active Discovery Terminate packet

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.

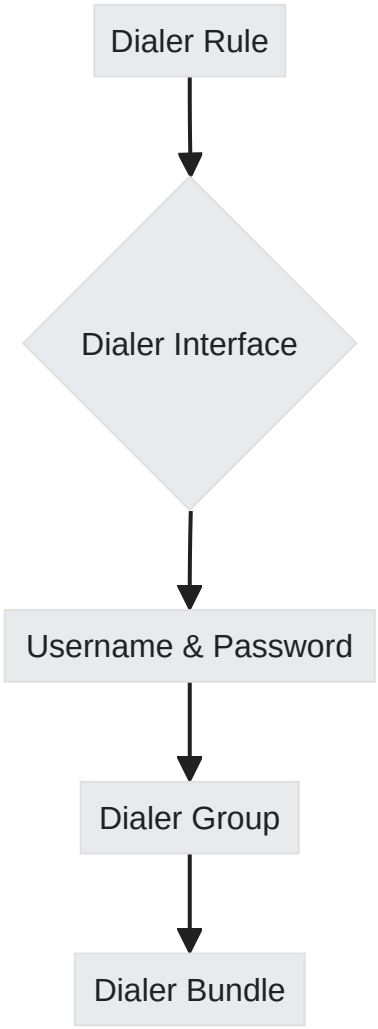
1.3.1.5.2 For Enterprises:

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.

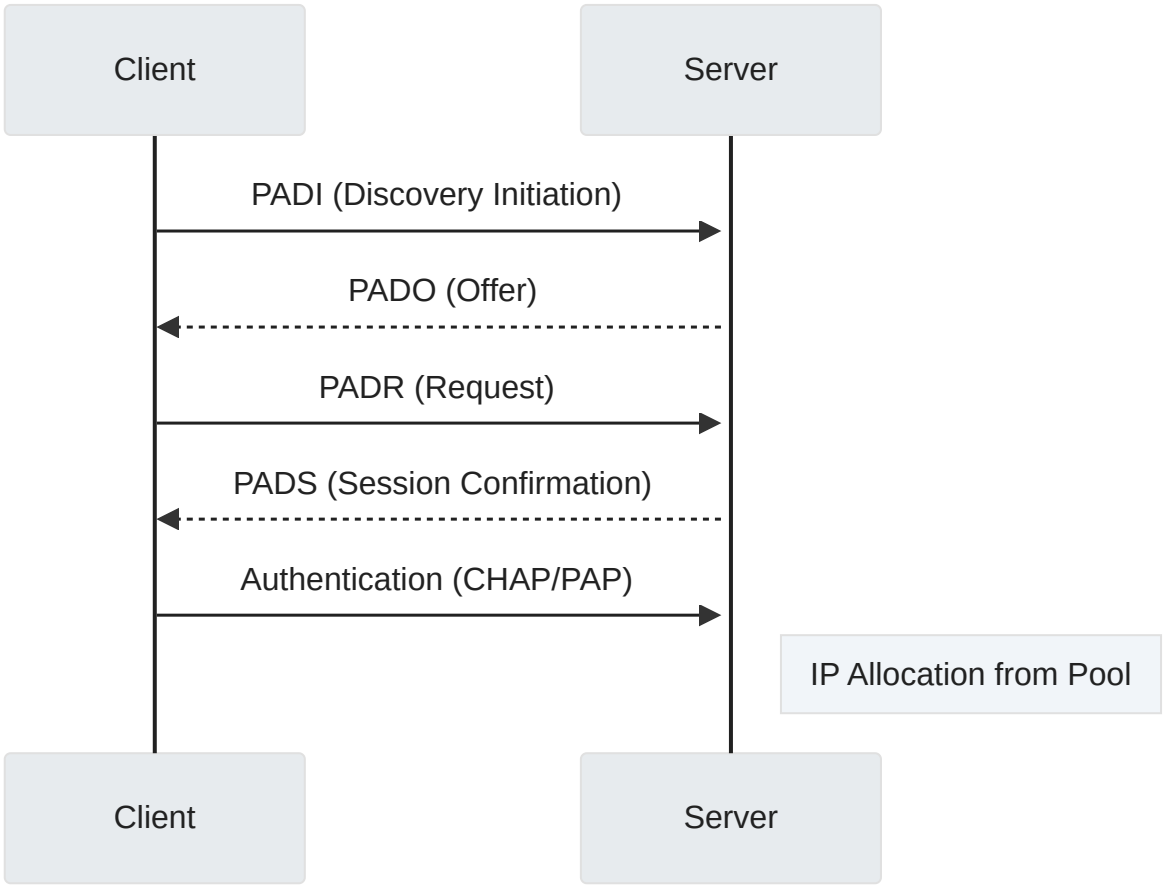
1.3.2.1.2 Verifying Configuration

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
```

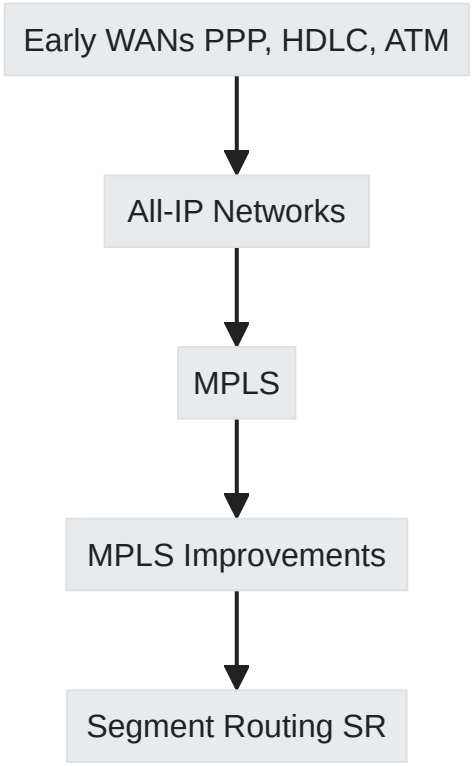
```
[R1]display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf      Client-MAC      Server-MAC      State
0       1       1   GE0/0/1   54899876830c    000000000000    IDLE
```

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.

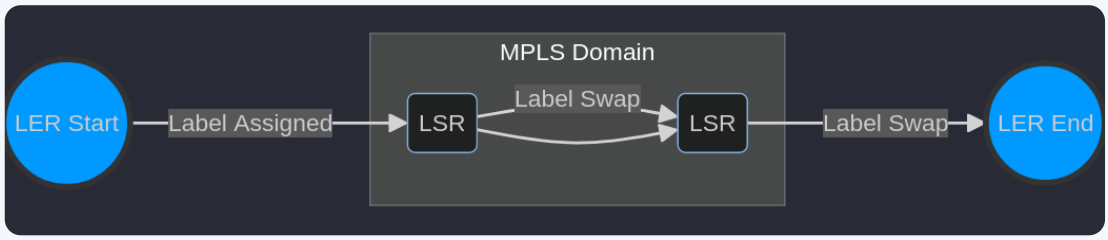
1. **Label Assignment and Switching**: Packets are assigned a label at the network edge that directs their path through routers without IP header analysis.
2. **Fixed-Length Labels**: Routers swiftly process packets based on fixed-length labels, avoiding the need for complex IP routing table lookups.
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**

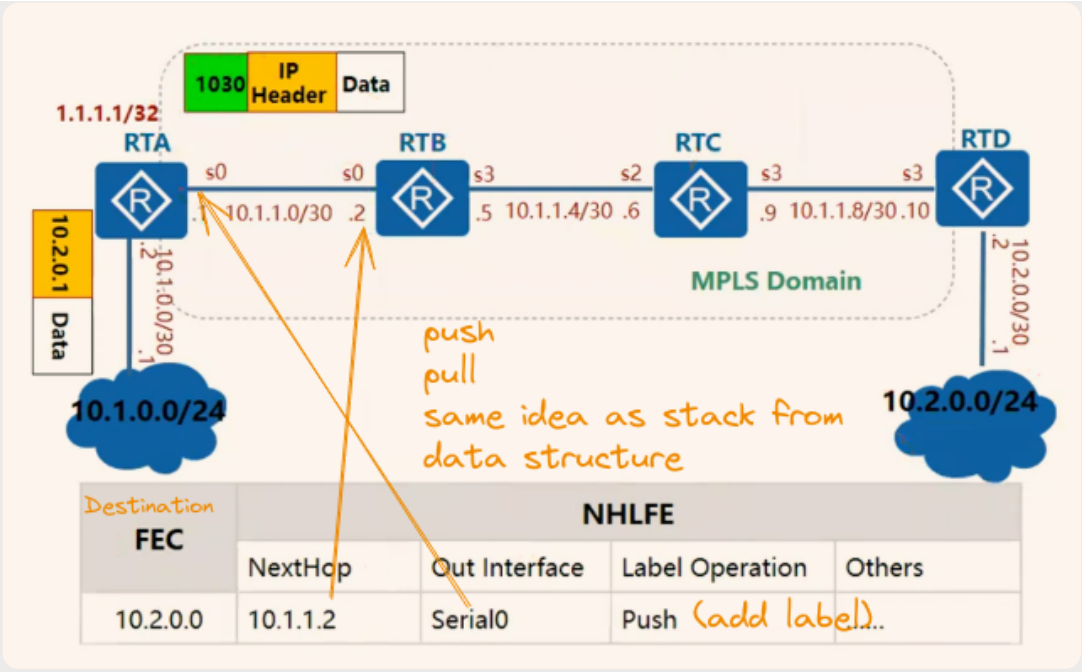
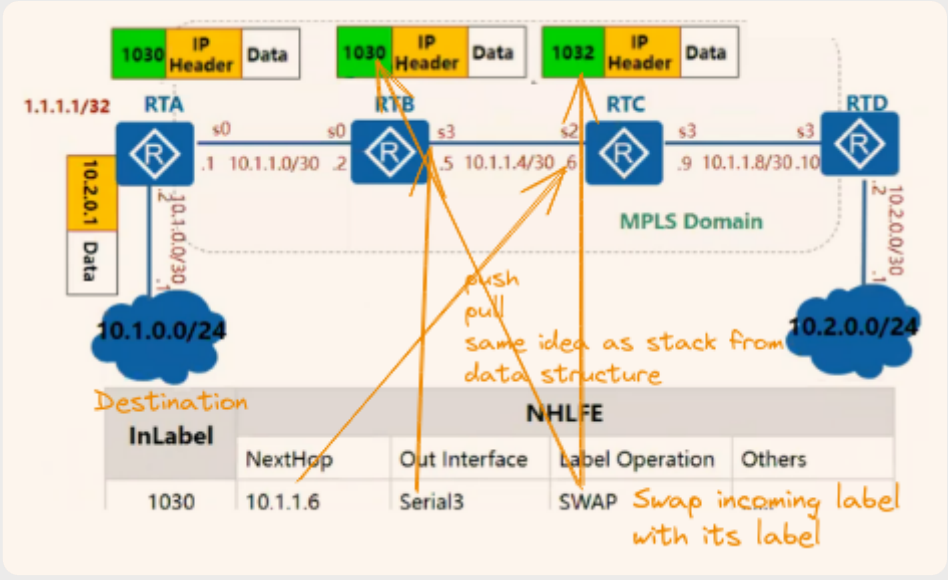
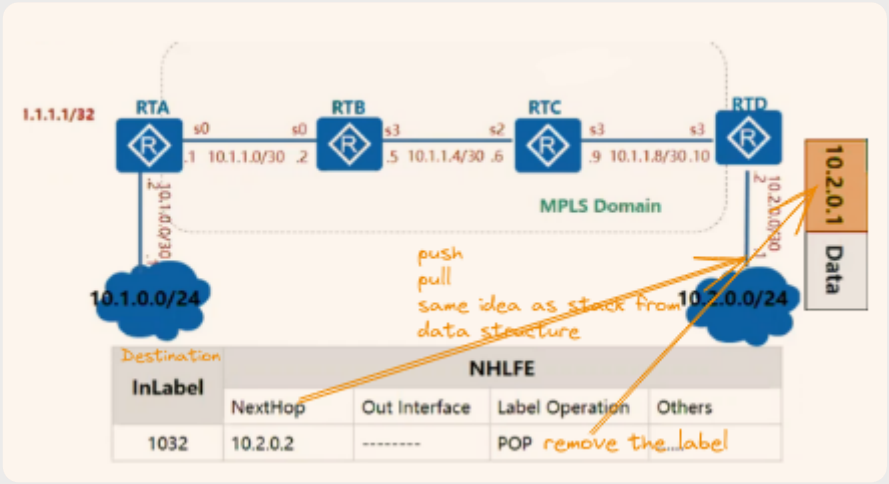
1. **LER (Label Edge Router)**: This is the router at the edge of an MPLS domain that makes decisions about which labels to assign to incoming packets based on their destination. It's where the MPLS paths begin and end.
2. **LSR (Label Switch Router)**: These are routers within the MPLS domain that route 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
.2
10.1.0.0/30
.1
10.2.0.1
Data
MPLS Domain
10.2.0.0/30
.2
.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
.2
10.1.0.0/30
.1
10.2.0.1
Data
MPLS Domain
10.2.0.0/30
.2
.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
.2
10.1.0.0/30
.1
MPLS Domain
10.2.0.0/30
.2
.1
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.

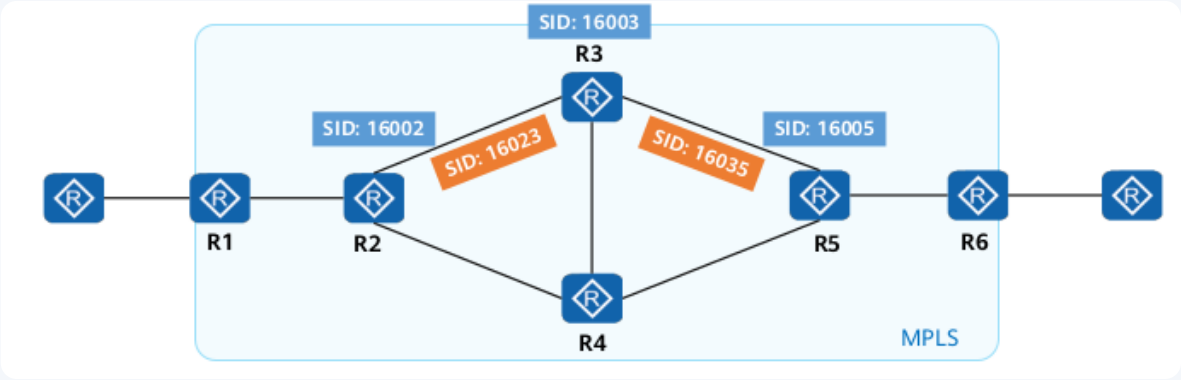
2. Introduces the source routing mechanism.

> 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

---

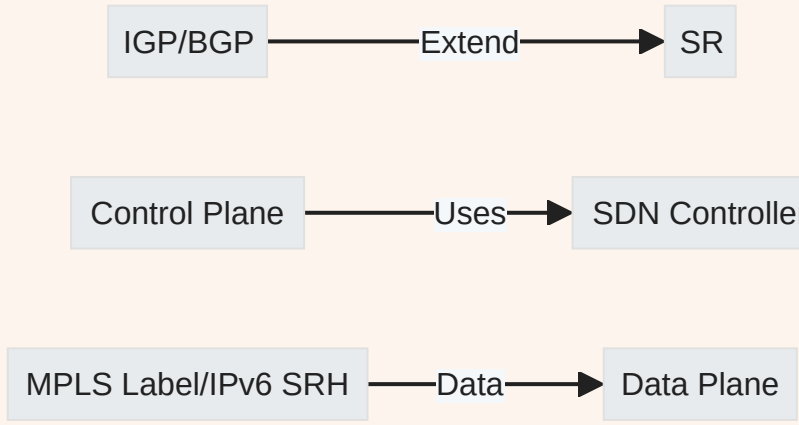
1. LDP determines paths based on the shortest IGP routes and does not support in Traffic Engineering, which could lead to non-optimal data flow that doesn't account for network load or bandwidth.
2. The protocol uses 11 Different packet types for various operations, introducing complexity in packet management 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

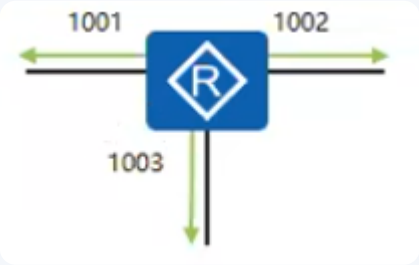
> Segment Routing is a networking technique where data packets follow a pre-determined path with specific stops, simplifying and streamlining the route they take.

Segments

Node Segment

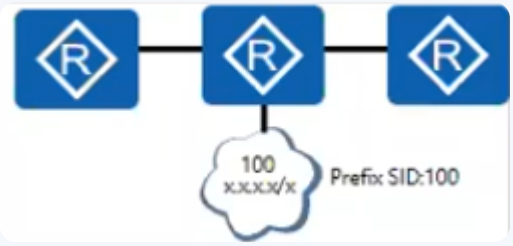
- Identifies a specific node; typically mapped to the loopback address prefix SID.

Adjacency Segment



- Identifies an adjacency between two nodes; dynamically allocated and local to the node.

Prefix Segment



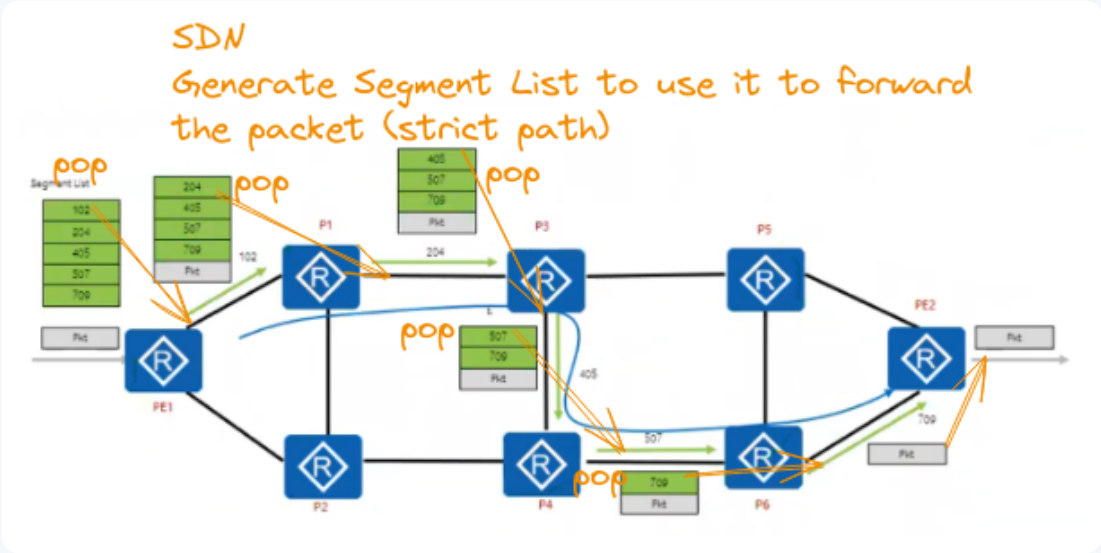
- Identifies the prefix of a destination address; globally valid and advertised via IGP.

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.

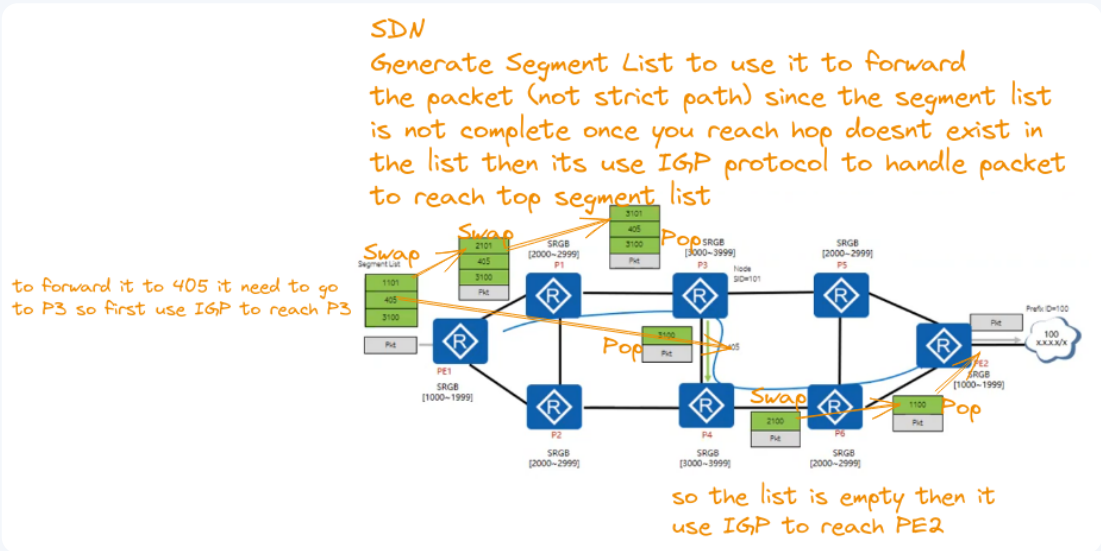
Working Principles

Strict explicit path



Used In SR-TE

Loose Explicit



Used In SR-TE

1.5 Extra

1.5.1 GRE

> ⚠ **Extra**

Overview of GRE

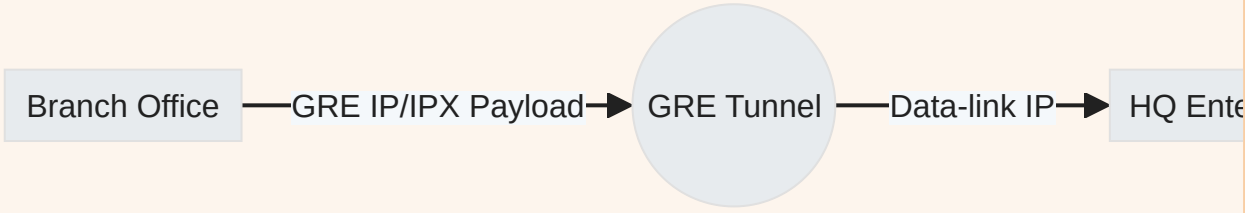
GRE Tunnel Concept

- 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 see-able 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.

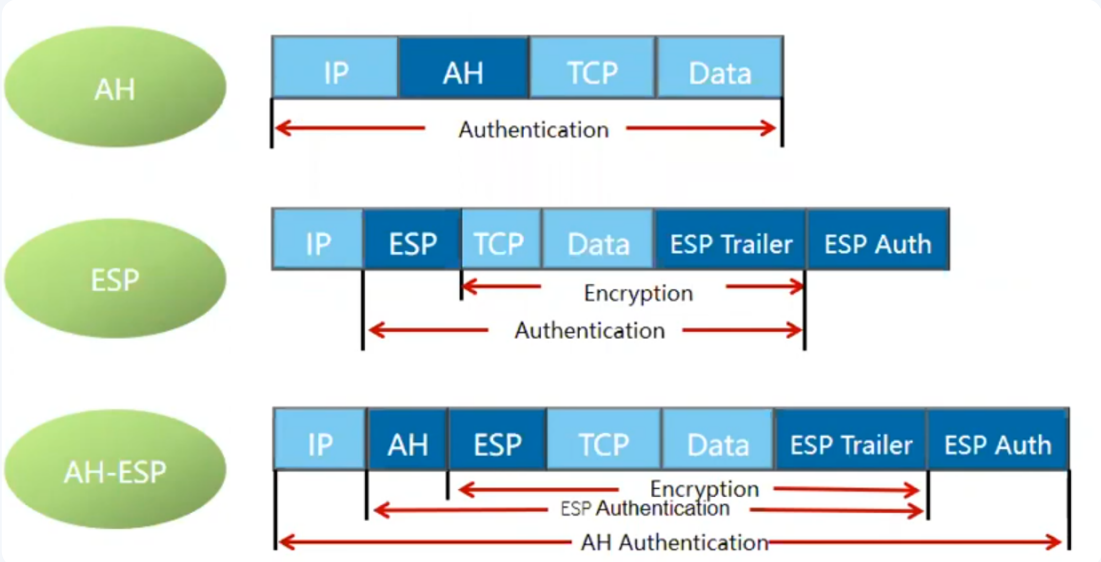
Security Association (SA)

> 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

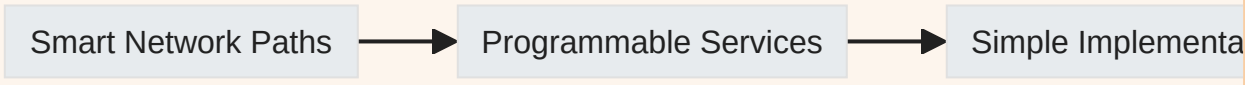
To verify IPSec proposal:

```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:** 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