PPP, ATM, DMVPN, SIP Trunks, & MPLS

by Sophia

WHAT'S COVERED

In this lesson, you will learn about PPP, ATM, DMVPN, SIP Trunks, and MPLS.

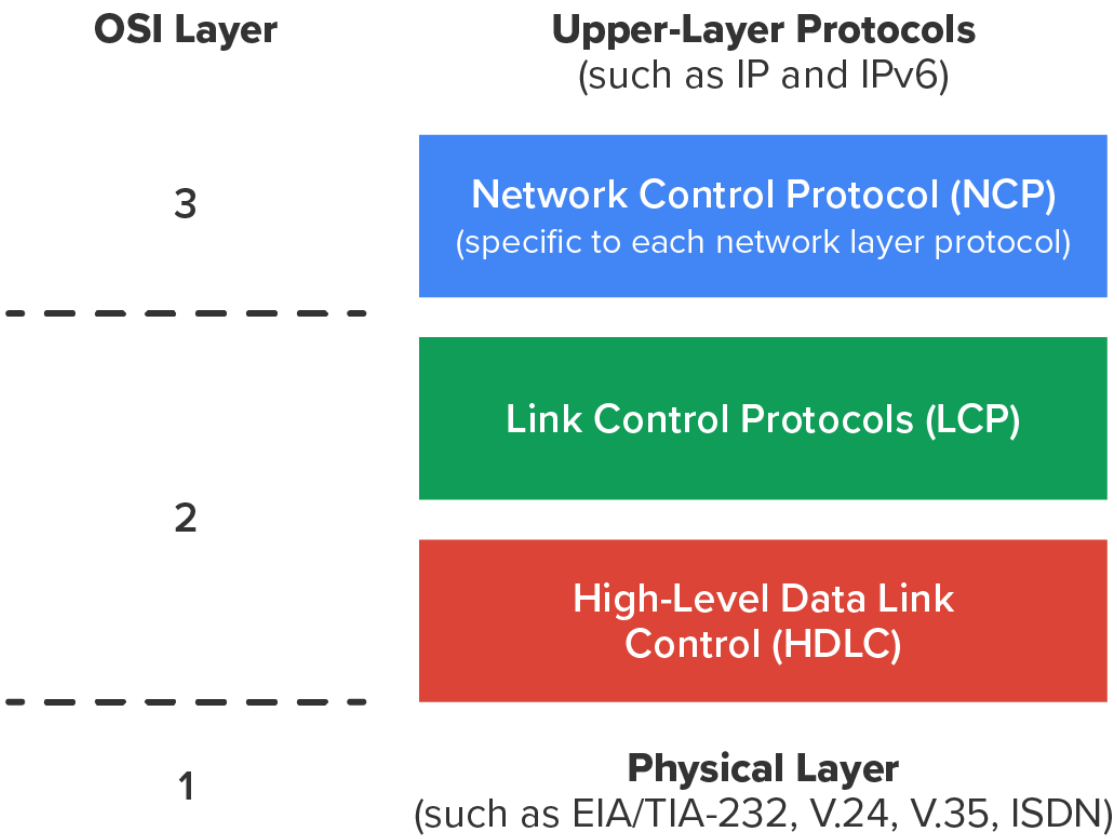
Specifically, this lesson will cover the following:

1. Point-to-Point Protocol

Point-to-Point Protocol (PPP) is a Layer 2 (data-link) protocol that can be used over either asynchronous serial (dial-up) or synchronous serial (ISDN) media. It relies on Link Control Protocol (LCP) to build and maintain data-link connections. Network Control Protocol (NCP) enables Layer 3 (network) routed protocols to be used on a point-to-point connection.

The basic purpose of PPP is to transport Layer 3 packets across a data-link layer point-to-point link, and it is nonproprietary. Cisco routers use **High-Level Data Link Control (HDLC)** as the default serial encapsulation serial links. Because the HDLC encapsulation is Cisco proprietary, you need PPP on your serial interfaces unless you have all Cisco routers. Since PPP can encapsulate several Layer 3 routed protocols and provide authentication, dynamic addressing, and callback, PPP may be a better encapsulation solution than HDLC anyway.

The diagram below shows the PPP stack compared to the OSI reference model.



PPP contains four main components:

- EIA/TIA-232-C, V.24, V.35, and ISDN are Layer 1 (physical) international standards for serial communication.
- HDLC is a method for encapsulating datagrams over serial links.
- LCP is a method of establishing, configuring, maintaining, and terminating the point-to-point connection. It also provides features such as authentication.
- NCP is a method of establishing and configuring different network layer protocols for transport across the PPP link. NCP is designed to allow the simultaneous use of multiple network layer protocols. Two examples of protocols here are Internet Protocol Control Protocol (IPCP) and Cisco Discovery Protocol Control Protocol (CDPCP).

The PPP protocol stack is specified at Layer 1 (physical) and Layer 2 (data link) only. NCP is used to enable communication between multiple Layer 3 (network) protocols by identifying and encapsulating the protocols across a PPP data link. Next, we will cover the options for LCP and PPP session establishment.

TERMS TO KNOW

Point-to-Point Protocol (PPP)

A data-link layer (Layer 2) communication protocol between two routers directly, without any host or any other networking in between.

High-Level Data Link Control (HDLC)

A Cisco-proprietary, bit-oriented code-transparent synchronous network layer protocol.

1a. Link Control Protocol (LCP) Configuration Options

Link Control Protocol (LCP) offers different PPP encapsulation options, including the following:

- Authentication: This option tells the calling side of the link to send information that can identify the user. The three methods for this task are as follows:
  - Password Authentication Protocol (PAP) is a password-based authentication protocol used by PPP to validate users.
  - Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections.
  - Challenge Handshake Access Protocol (CHAP) is an authentication protocol originally used by PPP to validate users. CHAP is also carried in other authentication protocols such as RADIUS.
- Compression: This is used to increase the throughput of PPP connections by compressing the data or payload prior to transmission. PPP decompresses the data frame on the receiving end.
- Error Detection: PPP uses quality and magic-number options to ensure a reliable, loop-free data link.
- Multilink: The multilink option makes several separate physical paths appear to be one logical path at Layer 3. This means that the two T1s running multilink PPP would show up as a single 3 Mbps path to a Layer 3 routing protocol.

TERM TO KNOW

Link Control Protocol (LCP)

Determines the acceptability of the link for a PPP connection.

1b. PPP Callback

On a dial-up connection, PPP can be configured to call back after successful authentication. PPP callback can be a very good thing because it allows us to keep track of usage based on access charges for accounting records and a bunch of other reasons. With callback enabled, a calling router (client) will contact a remote router (server) and authenticate. Both routers need to be configured for the callback feature for this to work. Once authentication is completed, the remote router will terminate the connection and then reinitiate a connection to the calling router.

1c. PPP Session Establishment

When PPP connections are started, the links go through three phases of session establishment, as shown in the diagram below:

PPP Session Establishment

1. Link-establishment phase
2. Authentication phase (optional)
3. Network layer protocol

- Link-Establishment Phase: In this phase, each PPP device sends LCP packets to configure and test the link. These packets contain a field called configuration option that allows each device to see the size of the data, the compression, and the authentication. If no configuration-option field is present, then the default configurations will be used.
- Authentication Phase: This is used if the required CHAP, EAP, or PAP can be used to authenticate a link. Authentication takes place before network layer protocol information is read, and it is also possible that link-quality determination will occur simultaneously.
- Network Layer Protocol Phase: This uses the **Network Control Protocol (NCP)** to allow multiple network layer protocols to be encapsulated and sent over a PPP data link. Each network layer protocol (such as IP and IPv6, which are routed protocols) establishes a service with NCP.

TERM TO KNOW

Network Control Protocol (NCP)

A protocol that runs on PPP.

1d. PPP Authentication Methods

There are three methods of authentication that can be used with PPP links:

1. **Password Authentication Protocol (PAP)** is the least secure of the three methods. Passwords are sent in clear text, and PAP is performed only during the initial link establishment. When the PPP link is first established, the remote node sends the username and password back to the originating target router until the authentication is acknowledged.
2. The **Challenge Handshake Authentication Protocol (CHAP)** is used at the initial start-up of a link and at periodic checkups on the link to ensure that the router is still communicating with the same host. After PPP finishes its initial link-establishment phase, the local router sends a challenge request to the remote device. The remote device sends a value calculated using a one-way hash function called MD5. The local router checks this hash value to make sure it matches. If the values do not match, the link is immediately terminated.

3. The **Extensible Authentication Protocol (EAP)** is a framework that supports multiple authentication methods using a variety of credential types, based on the specific implementation.

TERMS TO KNOW

Password Authentication Protocol (PAP)
A password-based authentication protocol used by PPP to validate users.

Challenge Handshake Authentication Protocol (CHAP)
An authentication protocol originally used by PPP to validate users. CHAP is also carried in other authentication protocols such as RADIUS.

Extensible Authentication Protocol (EAP)
An authentication framework frequently used in network and internet connections.

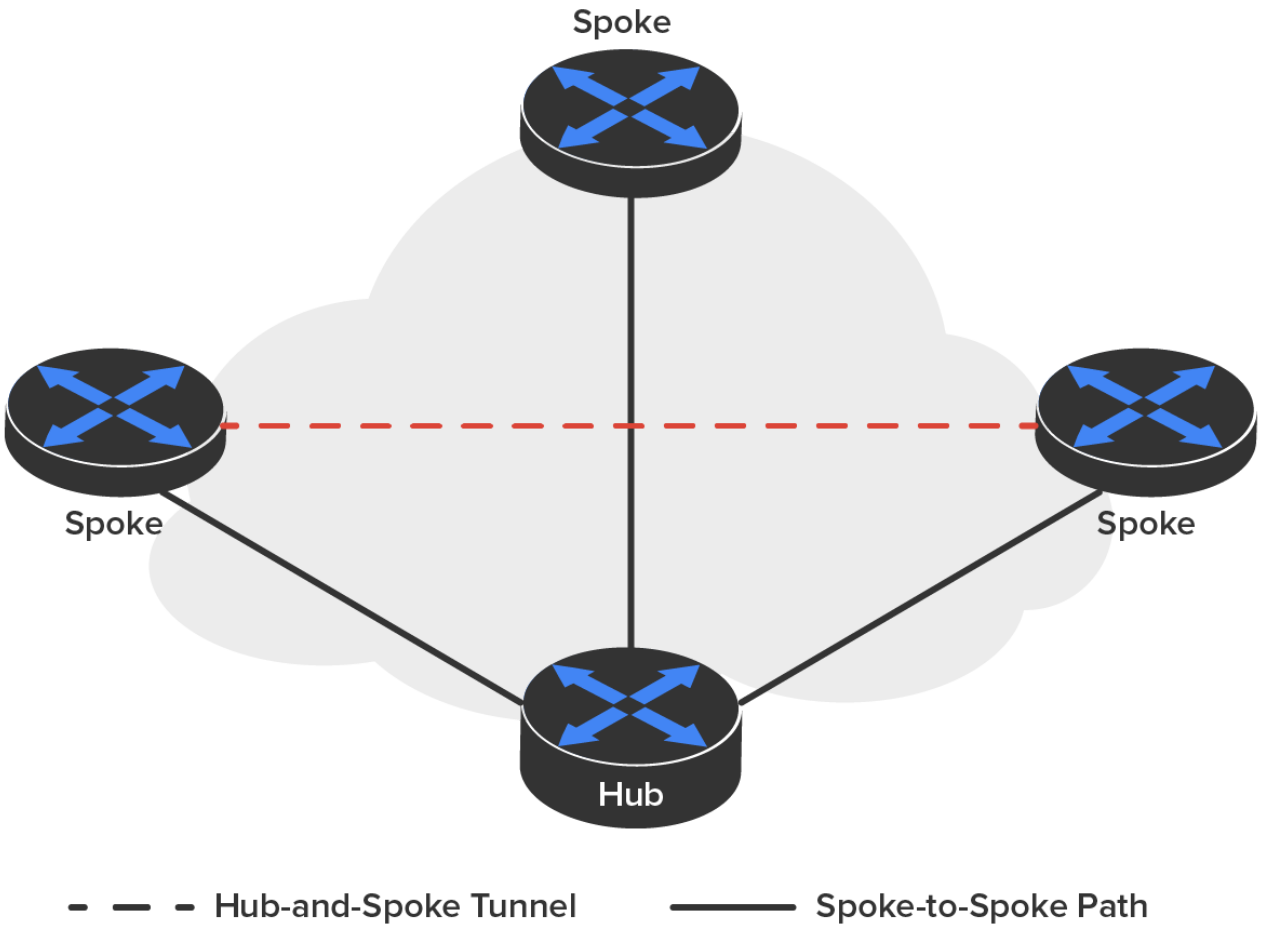
2. Dynamic Multipoint VPN (DMVPN)

Dynamic Multipoint VPN (DMVPN) provides the capability to build a dynamic mesh VPN network by defining only the hub on a hub-and-spoke configuration.

HINT

The benefit is the ability to deploy additional spokes without any reconfiguration of the hub.
Once the DMVPN is deployed, another interesting feature is the ability of the spokes to communicate with one another without passing the traffic though the hub. The spokes do this by dynamically setting up connections to one another by contacting the hub, obtaining the necessary information about the other end, and creating a dynamic IPSec VPN tunnel directly between them.

This connection is shown in the diagram below.



BIG IDEA

The benefits of DMVPNs are as follows:

- Traffic between remote sites does not need to traverse the hub.
- They eliminate additional bandwidth requirements at the hub.
- They eliminate additional network delays.
- They conserve WAN bandwidth.
- Costs for VPN circuits are lower.
- They provide increased resiliency and redundancy.

TERM TO KNOW

Dynamic Multipoint VPN (DMVPN)

A dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers, Huawei AR G3 routers, and Unix-like operating systems.

3. Session Initiation Protocol (SIP) Trunks

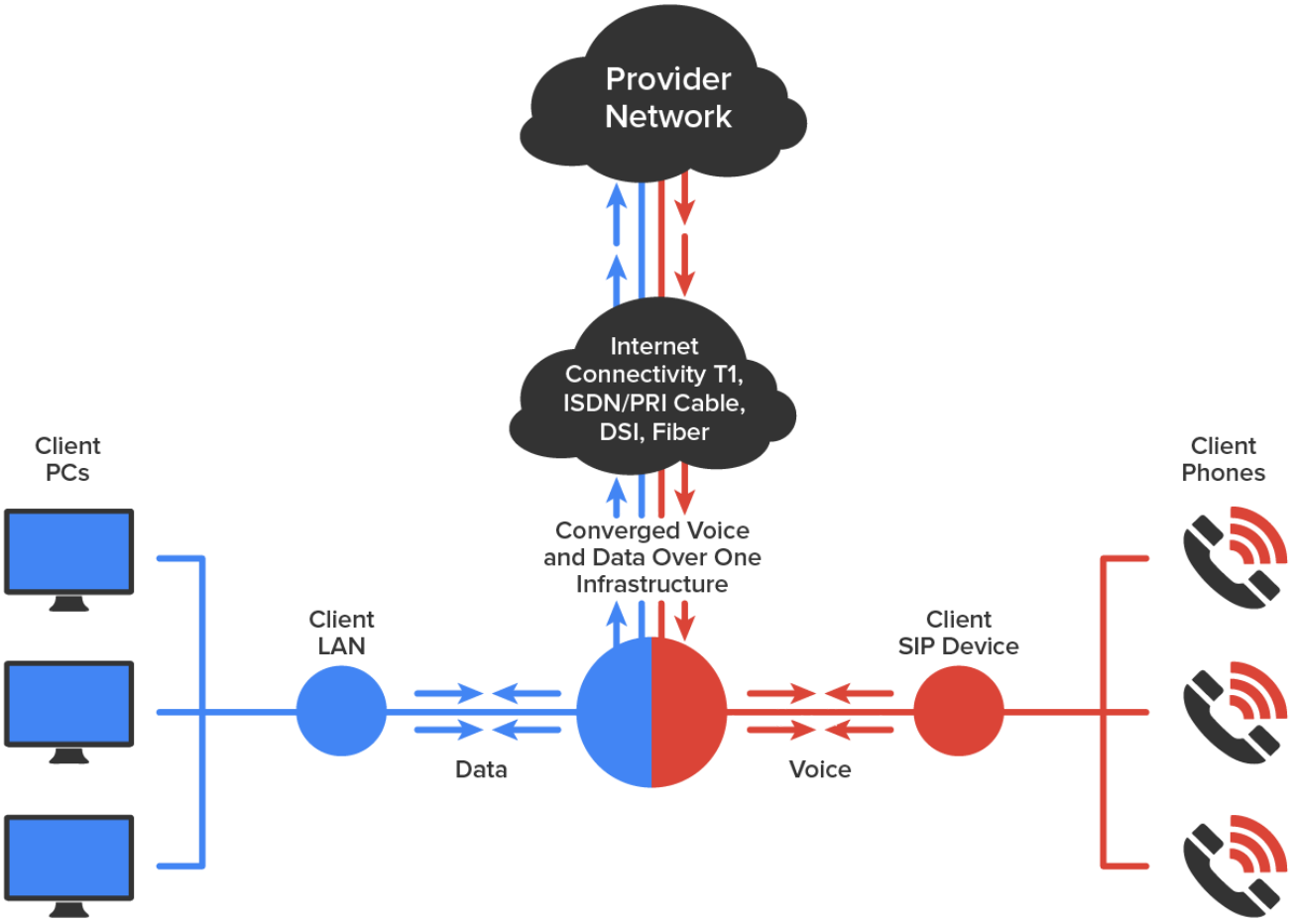
A **Session Initiation Protocol (SIP)** trunk is a link providing streaming media and unified communications to an organization by an internet telephone service provider. It connects to organizations equipped with SIP-based **Private Branch Exchange (PBX)** systems and unified communications (UC) facilities.

KEY CONCEPT

The SIP trunk provides a connection between two different domains of responsibility:

1. Private domain (responsibility of the organization), where the network is connected to the organization's PBX or unified communications server
2. Public domain (responsibility of the provider), which includes the part of the network that allows access into the PSTN (public switched telephone network) or PLMN (public land mobile network)

SIP architecture is seen in the image below:



TERMS TO KNOW

Session Initiation Protocol (SIP)

A communications protocol for signaling and controlling multimedia communication sessions, including voice-over IP.

Private Branch Exchange (PBX)

A telecommunications switching system, physically located at a customer's place of business, that provides internal communication between users and also access to outside (trunk) telephone lines.

4. Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM), not to be confused with automated teller machines, first emerged in the early 1990s.

ATM was designed to be a high-speed communications protocol that won't depend on any specific LAN topology. It uses a high-speed cell-switching technology that can handle data as well as real-time voice and video. The ATM protocol breaks up transmitted data into 53-byte cells. A **cell** is analogous to a packet or frame, except that an ATM cell is always fixed in length and is relatively small and fast, whereas a frame's length can vary.

ATM is designed to switch these small cells through an ATM network very quickly. It does this by setting up a virtual connection between the source and destination nodes; the cells may go through multiple switching points before ultimately arriving at their final destination. The cells may also arrive out of order, so the receiving system may have to reassemble and correctly order the arriving cells. ATM, like Frame Relay, is a connection-oriented service, in contrast to most data-link protocols, which are best-effort delivery services and do not require virtual circuits to be established before transmitting user data.

Data rates are scalable and start as low as 1.5 Mbps, with speeds of 25 Mbps, 51 Mbps, 100 Mbps, 155 Mbps, and higher. The common speeds of ATM networks today are 51.84 Mbps and 155.52 Mbps; both of them can be used over either copper or fiber-optic cabling. You can also get ATM with a speed of 622.08 Mbps, but that is currently used exclusively over fiber-optic cable. ATM supports very high speeds because it's designed to be routed by hardware rather than software, which makes faster processing speeds possible.

Fiber-based service-provider ATM networks are running today at data rates of 10 Gbps. These fast speeds make real-time payloads like voice and video travel with data on an ATM network and arrive without too much delay or latency. The small size of the payload, compared to the size of each cell's header, makes ATM less efficient than other WAN technologies like MPLS.

Asynchronous Transfer Mode (ATM)

A broadband voice and data technology with quality (class) of service (QoS) transmission for sending and receiving voice, data, and multimedia information over a fiber-optic network.

Cell

Analogous to a packet or frame, except that an ATM cell is always fixed in length and is relatively small and fast, whereas a frame's length can vary.

5. Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a data-carrying mechanism that emulates some properties of a circuit-switched network over a packet-switched network. So, MPLS is actually a switching mechanism that imposes labels (numbers) on packets and then uses them to forward packets.

The labels are assigned on the edge of the MPLS network, and forwarding inside the MPLS network is carried out solely based on the labels. The labels usually correspond to a path to Layer 3 destination addresses, which is similar to IP destination-based routing. MPLS was designed to support the forwarding of protocols other than TCP/IP. Because of this, label switching within the network is achieved in the same way, irrespective of the Layer 3 protocol.

HINT

In larger networks, the result of MPLS labeling is that only the edge routers perform a routing lookup. All the core routers forward packets based on the labels, which makes forwarding the packets through the service provider network faster. This is a big reason many companies have replaced their Frame Relay networks with MPLS service.

TERM TO KNOW

Multiprotocol Label Switching (MPLS)
A routing technique in telecommunications networks that directs data from one node to the next based on labels rather than network addresses.

SUMMARY

In this lesson, you learned about WAN protocols like **Point-to-Point Protocol (PPP)**, which included **Link Control Protocol (LCP) configuration options**. You also learned about **PPP callback**, **PPP session establishment**, **PPP authentication methods**, **Dynamic Multipoint VPN (DMVPN)**, **Session Initiation Protocol (SIP) trunks**, **Asynchronous Transfer Mode (ATM)**, and **Multiprotocol Label Switching (MPLS)**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)

TERMS TO KNOW

Asynchronous Transfer Mode (ATM)
A broadband voice and data technology with quality (class) of service (QoS) transmission for sending and receiving voice, data, and multimedia information over a fiber-optic network.

Cell

Analogous to a packet or frame, except that an ATM cell is always fixed in length and is relatively small and fast, whereas a frame's length can vary.

Challenge Handshake Authentication Protocol (CHAP)

An authentication protocol originally used by PPP to validate users. CHAP is also carried in other authentication protocols such as RADIUS.

Dynamic Multipoint VPN (DMVPN)

A dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers, and Huawei AR G3 routers, and on Unix-like operating systems.

Extensible Authentication Protocol (EAP)

An authentication framework frequently used in network and internet connections.

High-Level Data Link Control (HDLC)

A Cisco-proprietary, bit-oriented code-transparent synchronous network layer protocol.

Link Control Protocol (LCP)

Determines the acceptability of the link for a PPP connection.

Multiprotocol Label Switching (MPLS)

A routing technique in telecommunications networks that directs data from one node to the next based on labels rather than network addresses.

Network Control Protocol (NCP)

A protocol that runs on PPP.

Password Authentication Protocol (PAP)

A password-based authentication protocol used by PPP to validate users.

Point-to-Point Protocol (PPP)

A data link layer (Layer 2) communication protocol between two routers directly without any host or any other networking in between.

Private Branch Exchange (PBX)

A telecommunications switching system, physically located at a customer's place of business, that provides internal communication between users and also access to outside (trunk) telephone lines.

Session Initiation Protocol (SIP)

A communications protocol for signaling and controlling multimedia communication sessions, including voice-over IP.