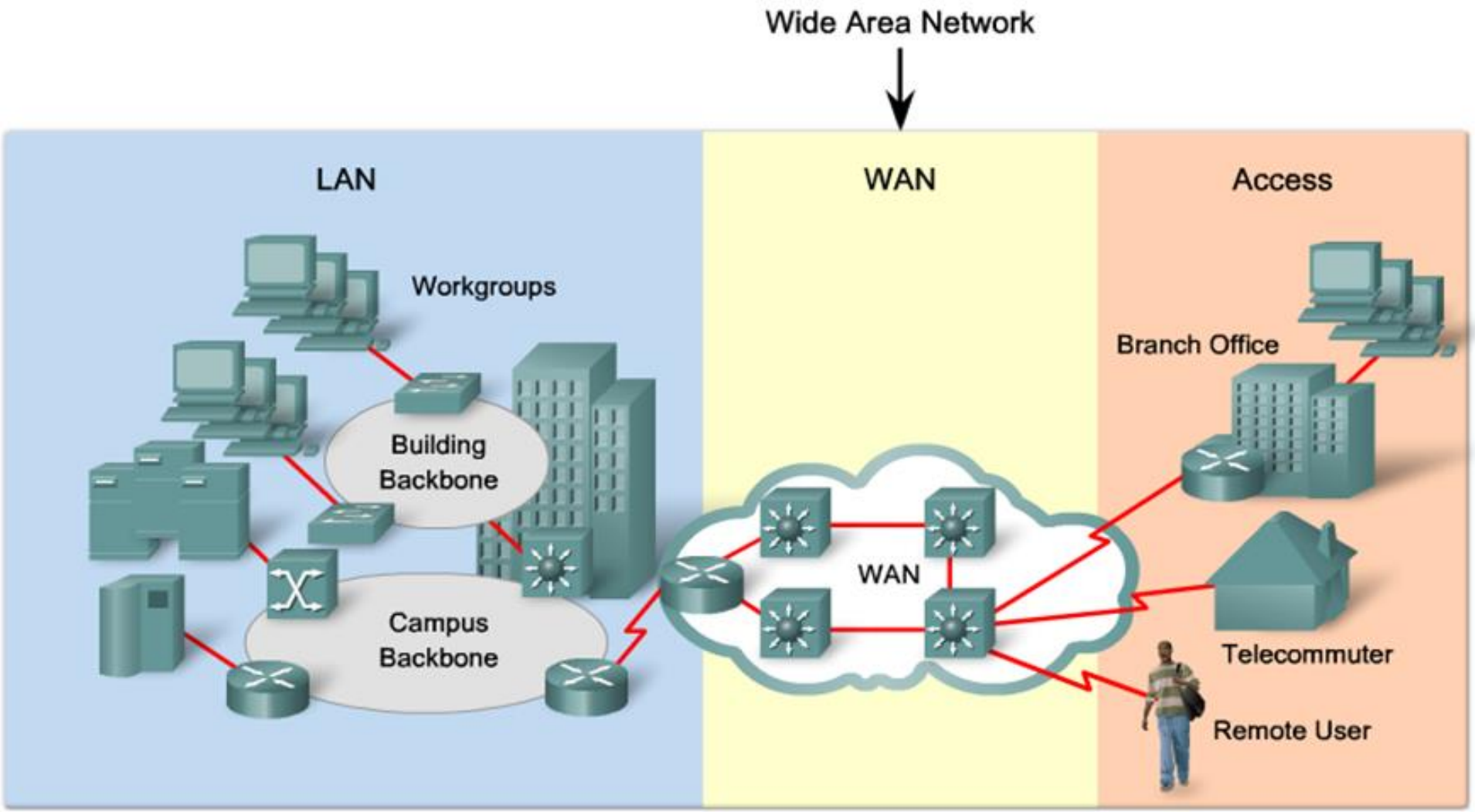
WAN INTRODUCTION

What is WAN?

- A WAN (Wide Area Network) is a data communications network that operates beyond the geographic scope of a LAN.
- WANs are different from LANs in several ways. While a LAN connects computers, peripherals, and other devices in a single building or other small geographic area, a WAN allows the transmission of data across greater geographic distances.
- In addition, an enterprise must subscribe to a WAN service provider to use WAN carrier network services. LANs are typically owned by the company or organization that uses them.

What is WAN? (Cont.)

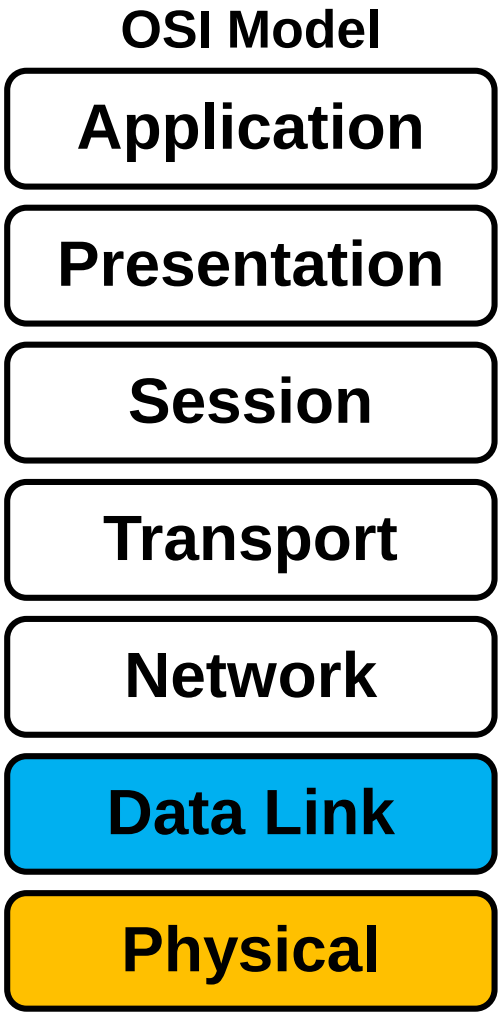


WANs vs. LANs

	WANs	LANs
Area	Wide geographic area	Single building or small geographic area
Ownership	Subscription to outside service provider	Owned by Organization

301P_945

What is WAN? (Cont.)



WAN standards are defined and managed by a number of recognized authorities:

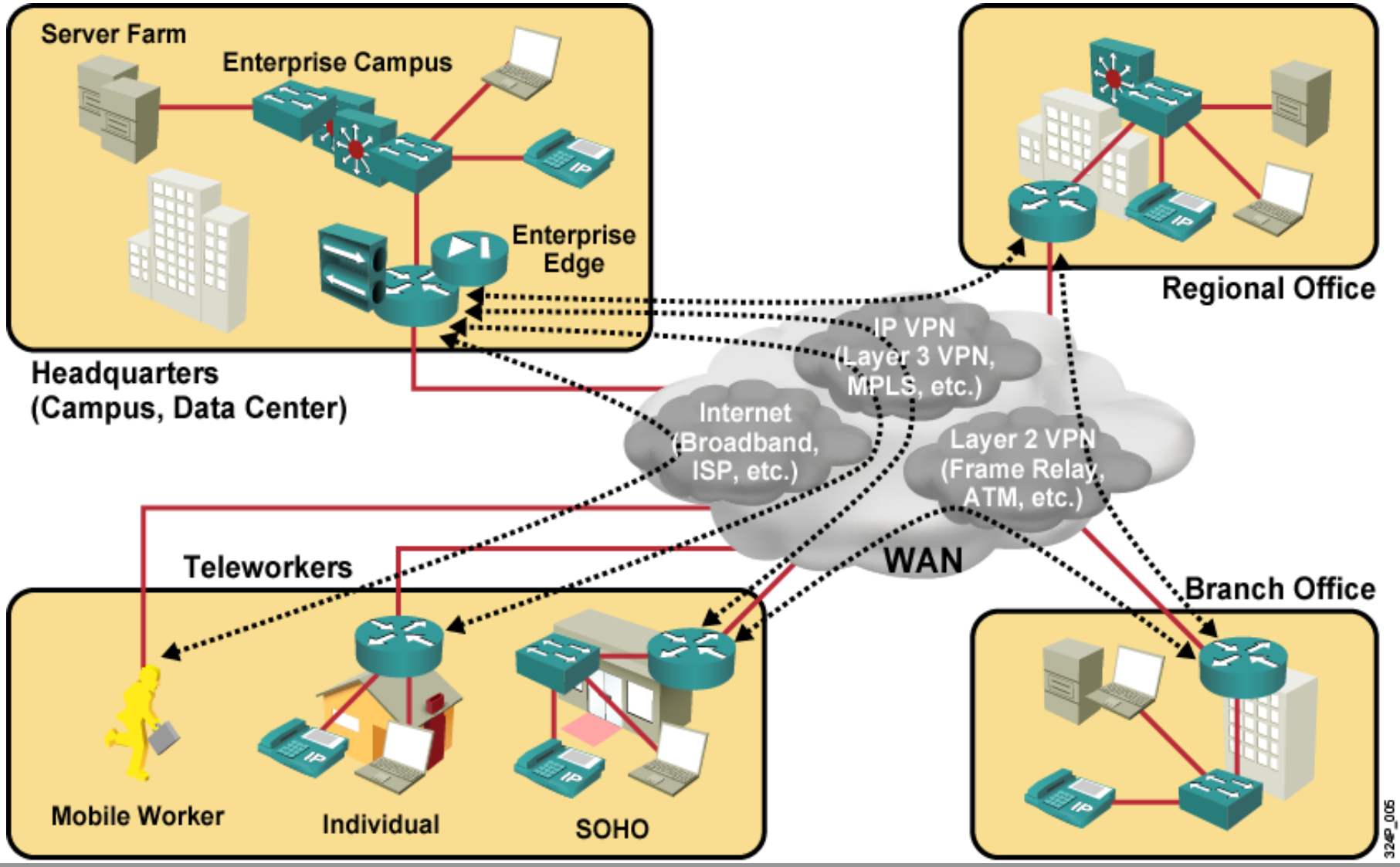
- **ISO** (International Organization for Standardization)
- **IEEE** (Institute of Electrical and Electronics Engineers)
- **TIA/EIA** (Telecommunication Industry Association and the Electronic Industries Alliance)

WAN Services

Frame Relay, ATM (Asynchronous Transfer Mode), HDLC (High-Level Data Link Control), PPP (Point-to-Point Protocol)

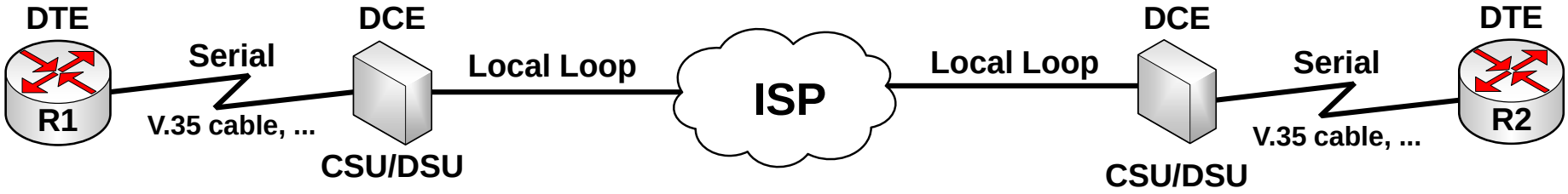
Electrical, mechanical, operational connections

WAN Connection Options



An Overview of PPP

- **Point-to-Point Protocol (PPP)** is a data link layer (layer 2) communications protocol used to establish a direct connection between two nodes
- PPP can provide connection authentication, transmission encryption and compression



- **CSU/DSU (Channel Service Unit/Data Service Unit)**: used to connect the digital WAN line (Leased lines) to the client's DTE device which is usually a router
- The **DTE (Data Terminal Equipment)** would be the router
- The **DCE (Data Communication Equipment - providing clock)** would be the CSU/DSU

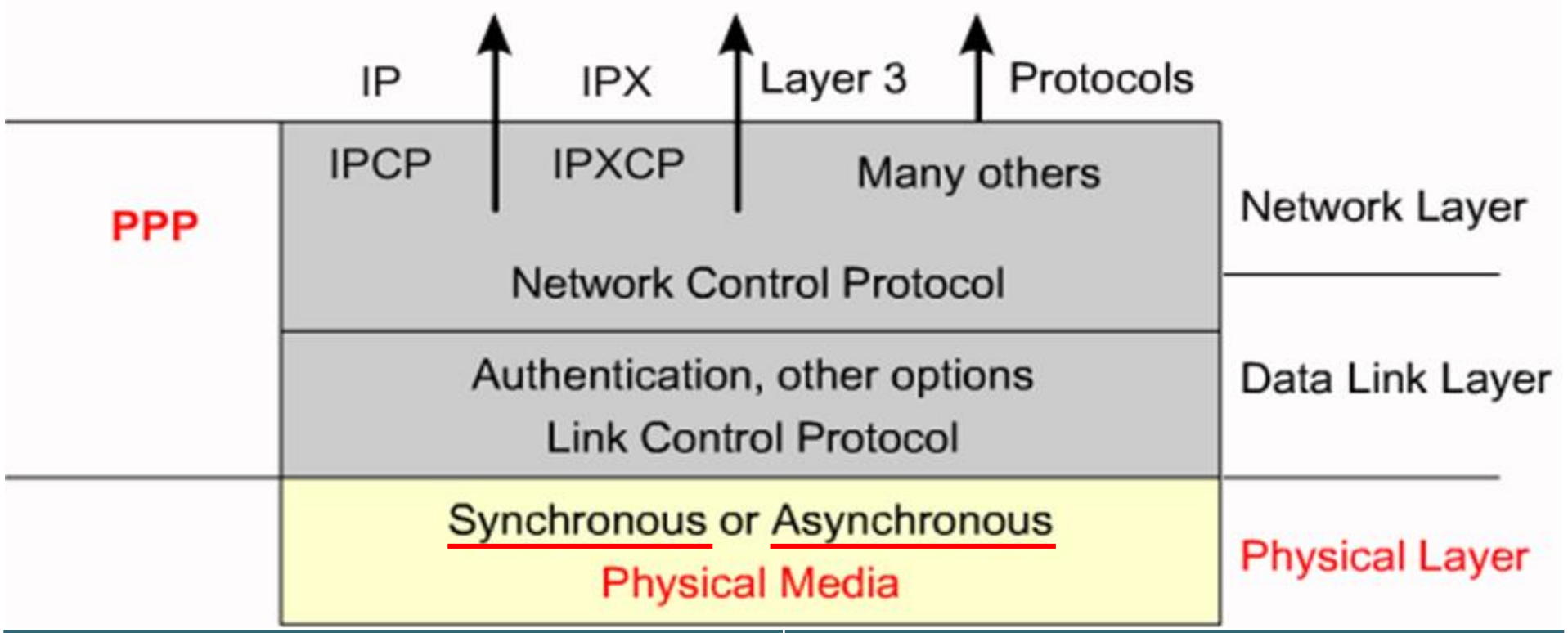
PPP

HDLC is the default encapsulation method on a serial link.

Use PPP encapsulation to connect to a non-Cisco router.

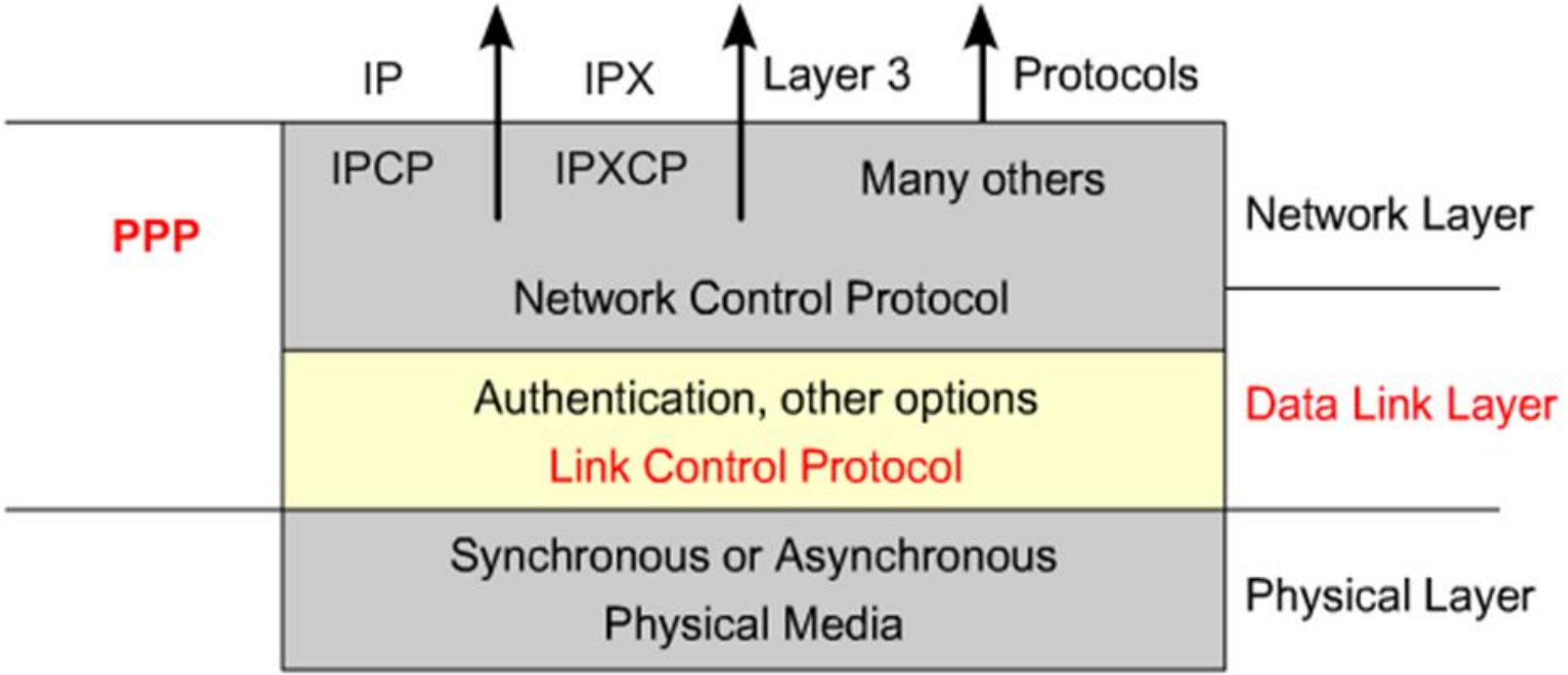
- PPP controls the setup of several link options using **LCP (Link Control Protocol)**
- PPP can carry packets from several protocol suites using **NCP (Network Control Protocol)**

PPP LAYERED ARCHITECTURE: PHYSICAL LAYER



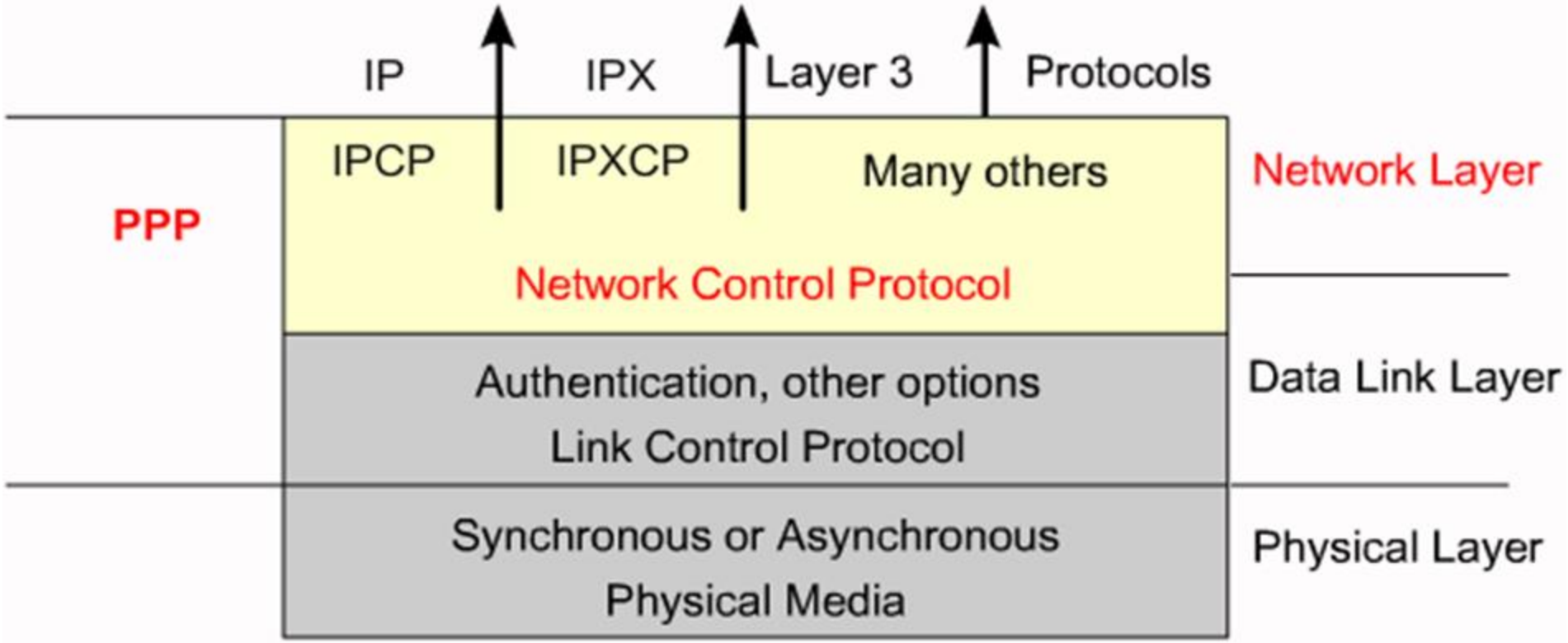
Synchronous	Asynchronous
Supports high data transfer rate	Slower data transfer rate
Needs clock signal between the sender and the receiver	Does not need clock signal between the sender and the receiver
Sender and receiver use the same clock rate	Sender provides a synchronization signal to the receiver before starting the transfer of each message

PPP LAYERED ARCHITECTURE: LCP LAYER



- **Link Configuration:** The process of setting up and negotiating the parameters of a link.
- **Link Maintenance:** The process of managing an opened link.
- **Link Termination:** The process of closing an existing link when it is no longer needed (or when the underlying physical layer connection closes).

PPP LAYERED ARCHITECTURE: NCP LAYER



Network Protocol	PPP Network Control Protocol
IP (Internet Protocol)	IPCP
IPX (Internetworking Packet Exchange)	IPXCP
NBF (NetBIOS Frames)	NBFCP

Establishing a PPP Session

The LCP does all the talking.

Phase 1 - Link Establishment: “Let’s negotiate.”

LCP must first open the connection and negotiate configuration options.

Phase 2 - Determine Link Quality: “Maybe we should discuss some details about quality. Or, maybe not ...”

The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.

Phase 3 - Network Protocol Negotiation: “OK, I will leave it to the NCPs to discuss higher level details.”

NCP can separately configure the network layer protocols, and bring them up and take them down at any time.

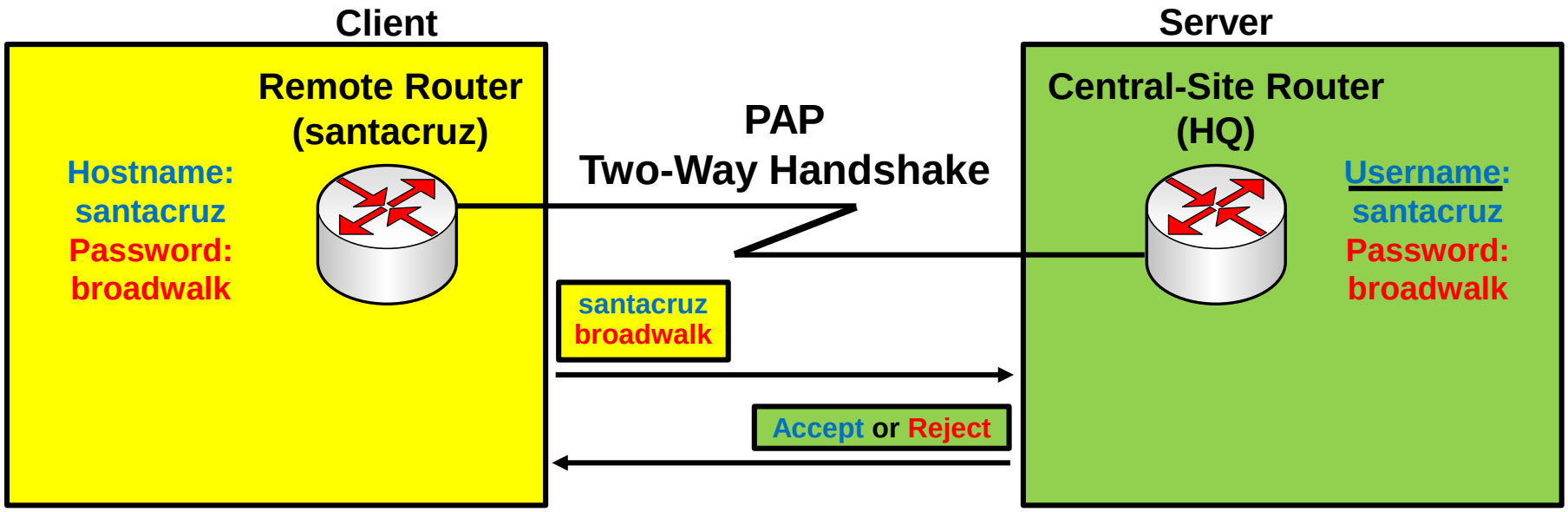
Authentication

Authentication means to put a username and password before accessing the network.

There is two authentication protocols:

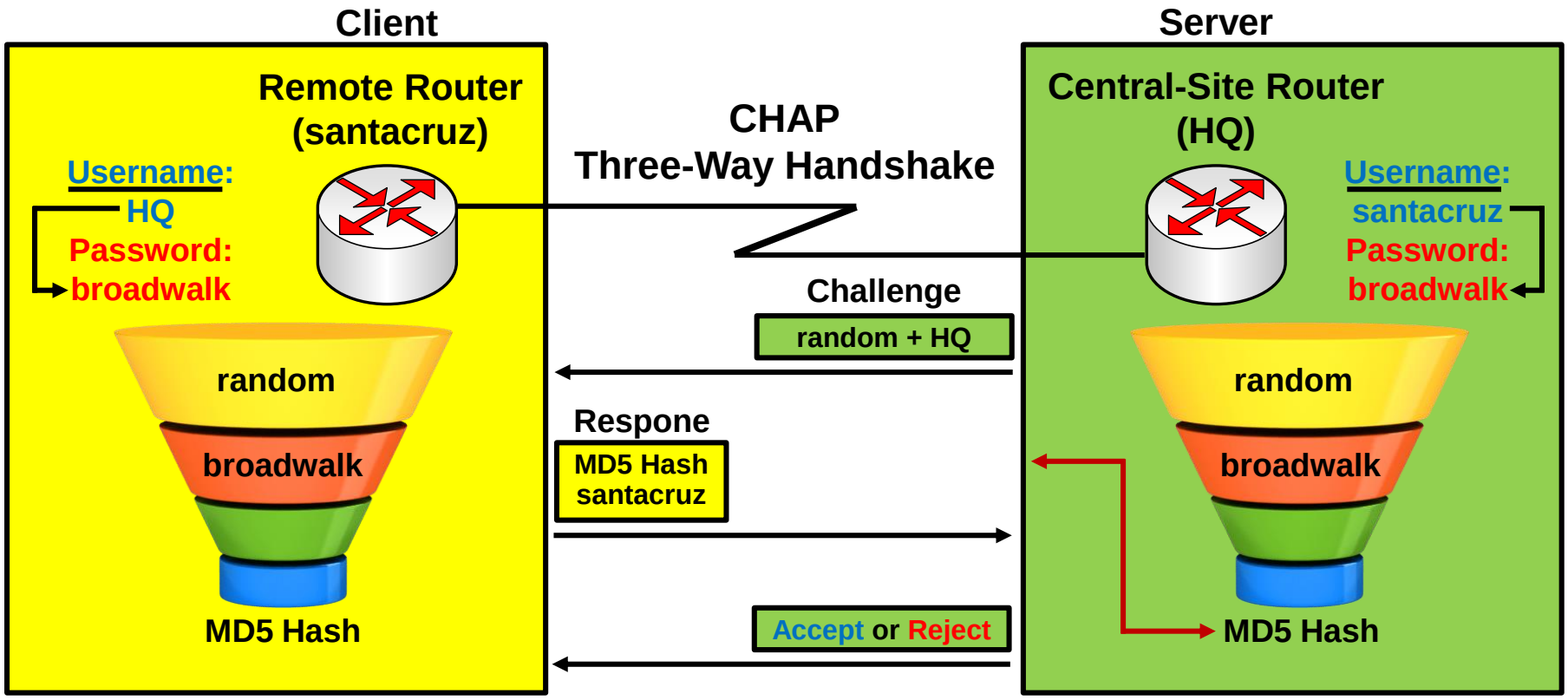
- PAP (PPP Authentication Protocol).
- CHAP (Challenge Handshake Authentication Protocol).

PPP Authentication Protocols: PAP



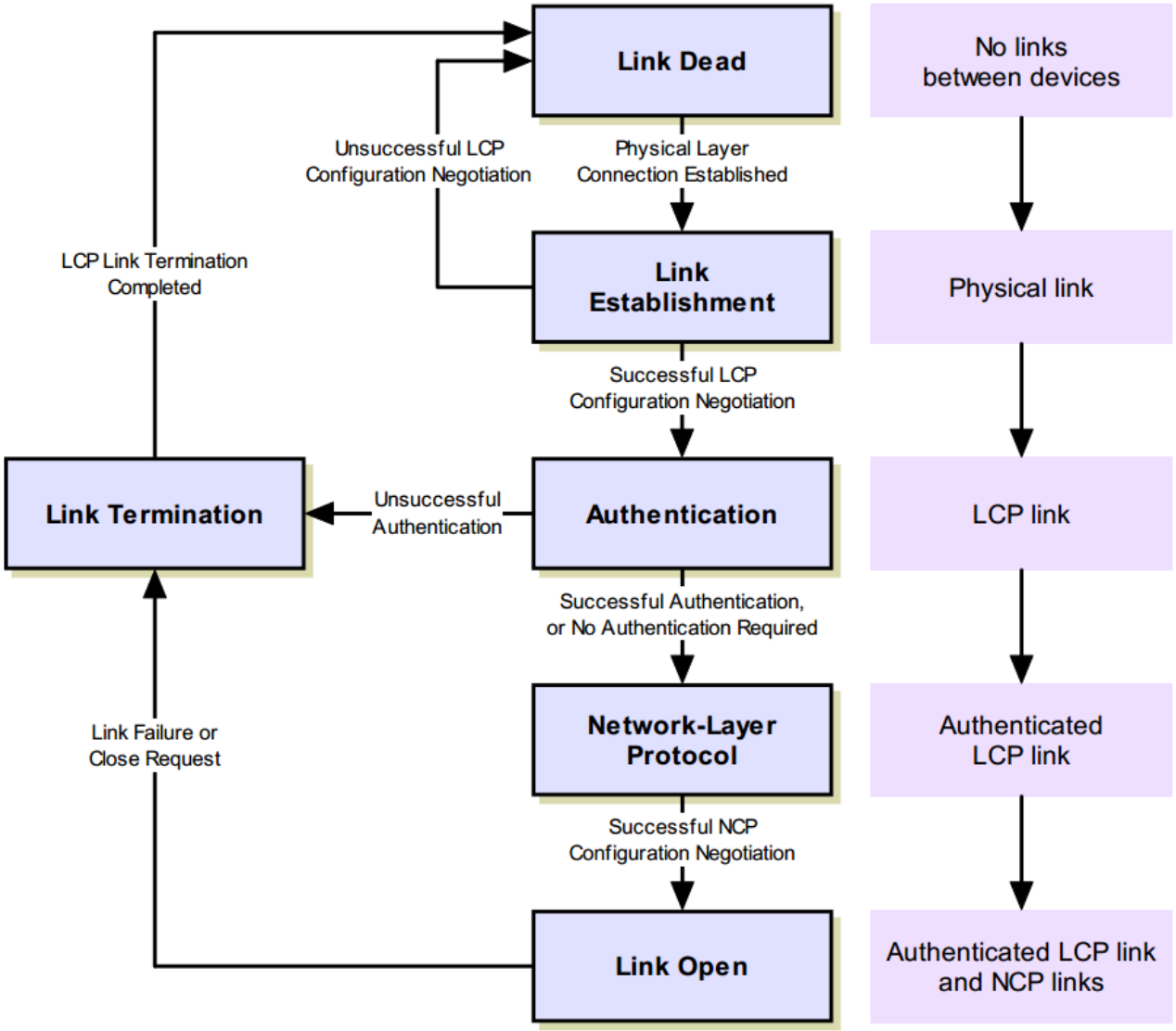
- Username/password pair is repeatedly sent by the remote node.
- Passwords sent in plaintext.
- The remote node is in control of the frequency and timing of the login attempts.

PPP Authentication Protocols: CHAP



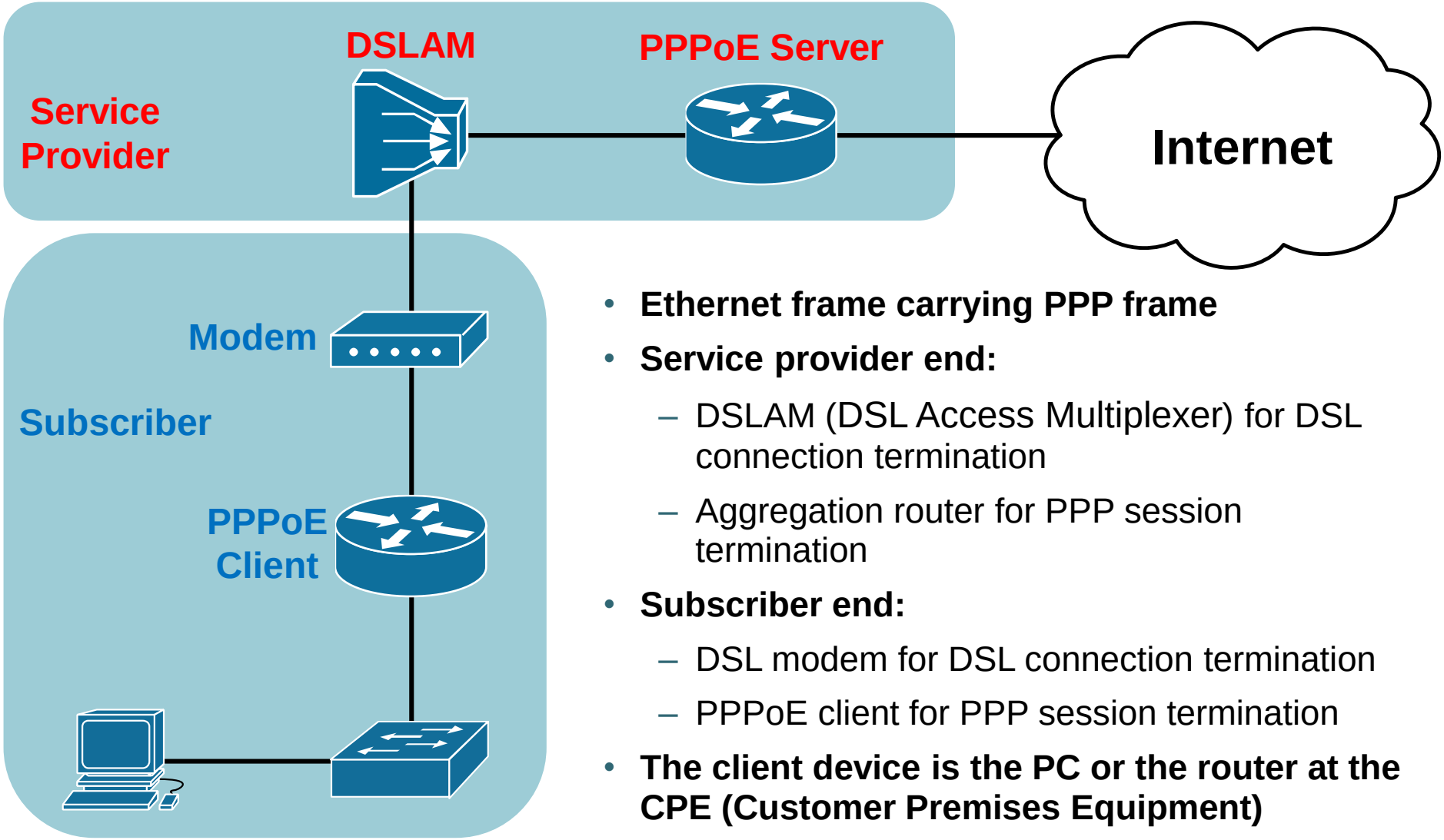
- This is an example of the Santa Cruz router authenticating to the HQ router.
- Hash values, not actual passwords, are sent across the link.
- The local router or external server is in control of authentication attempts.

PPP Phases


Link Dead
No links between devices
Unsuccessful LCP Configuration Negotiation
Physical Layer Connection Established
LCP Link Termination Completed
Link Establishment
Physical link
Successful LCP Configuration Negotiation
Link Termination
Unsuccessful Authentication
Authentication
LCP link
Successful Authentication, or No Authentication Required
Link Failure or Close Request
Network-Layer Protocol
Authenticated LCP link
Successful NCP Configuration Negotiation
Link Open
Authenticated LCP link and NCP links

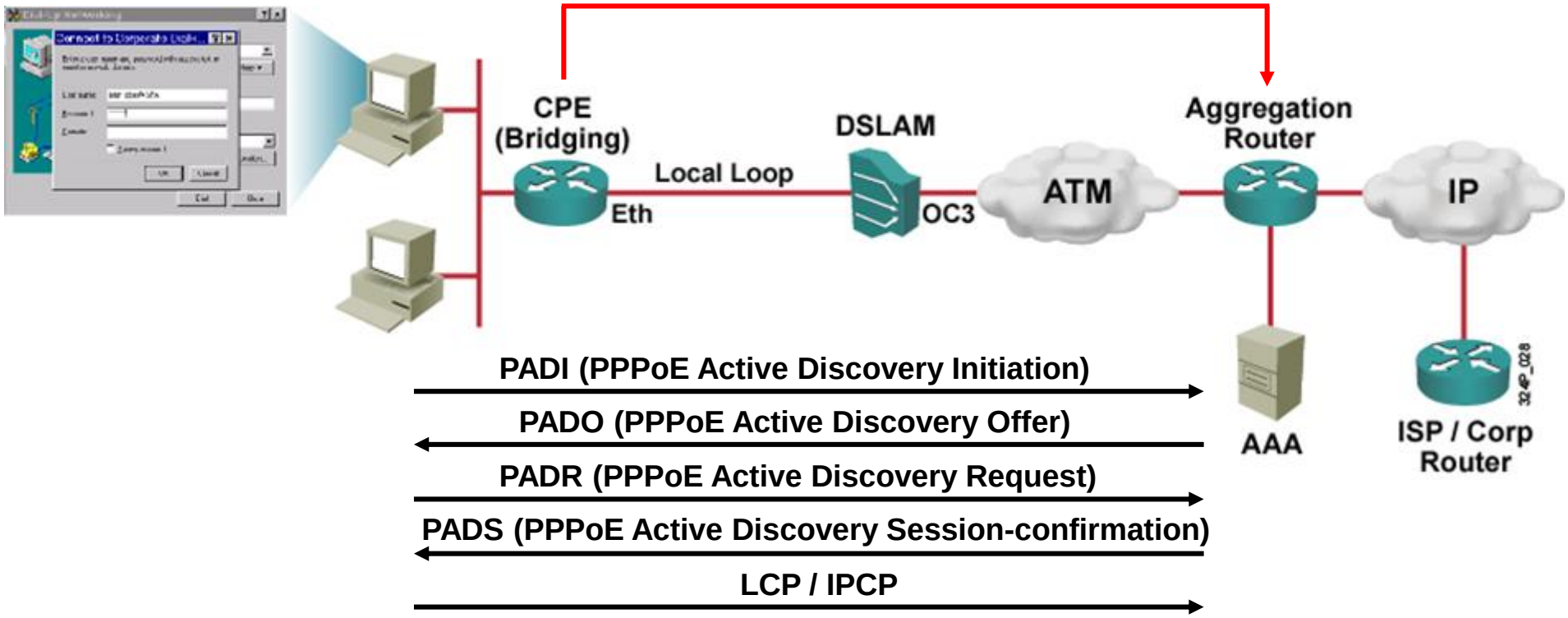
PPPoE

PPP over Ethernet



- **Ethernet frame carrying PPP frame**
- **Service provider end:**
  - DSLAM (DSL Access Multiplexer) for DSL connection termination
  - Aggregation router for PPP session termination
- **Subscriber end:**
  - DSL modem for DSL connection termination
  - PPPoE client for PPP session termination
- **The client device is the PC or the router at the CPE (Customer Premises Equipment)**

PPPoE Session Establishment



- **PPP session is from PPPoE client to the aggregation router.**
- **Subscriber IP address is assigned by the aggregation router via IPCP.**

PPPoE Client Configuration

PPPoE Client:

```
Client(config)#interface dialer 0
Client(config-if)#encapsulation ppp
Client(config-if)#ip address negotiated
Client(config-if)#ppp pap sent-username user1 password cisco
Client(config-if)#dialer pool 1

Client(config)#interface g1
Client(config-if)#pppoe enable
Client(config-if)#pppoe-client dial-pool-number 1

Client(config)#ip route 0.0.0.0 0.0.0.0 dialer 0
```

PPPoE Verification

Ping successfully:

```
Client#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/30 ms
```

PPPoE Verification

```
Client#show pppoe session
     1 client session

Uniq ID   PPPoE   RemMAC           Port                VT   VA          State
            SID   LocMAC                               VA-st
    N/A      18   000c.297c.c044   G1                  Di0  Vi1         UP
                  000c.297c.d19e                       UP
```

PPPoE Server

PPPoE Client


CISCO