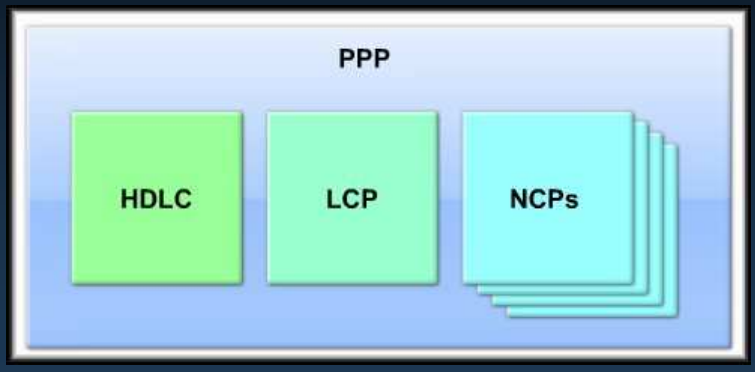
Chapter 2

Point-to-Point Protocol (PPP)

Part II

Point-to-Point Protocol (PPP)

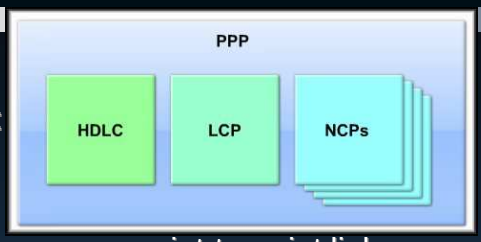
PPP Concepts



Introducing PPP

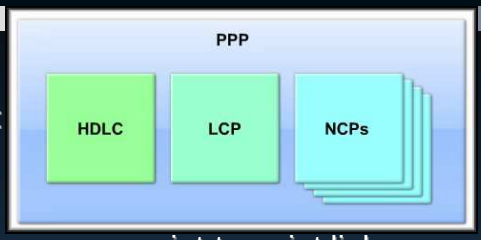
- What is PPP?
  - Recall that HDLC is the default serial encapsulation method when you connect two Cisco routers.
  - *Cisco HDLC can only work with other Cisco devices*.
  - When you need to connect to a non-Cisco router, you should use PPP encapsulation.
    - PPP includes many features not available in HDLC.
    - The link quality management feature monitors the quality of the link. If too many errors are detected, PPP takes the link down.
    - PPP supports PAP and CHAP authentication.

Introducing PPP



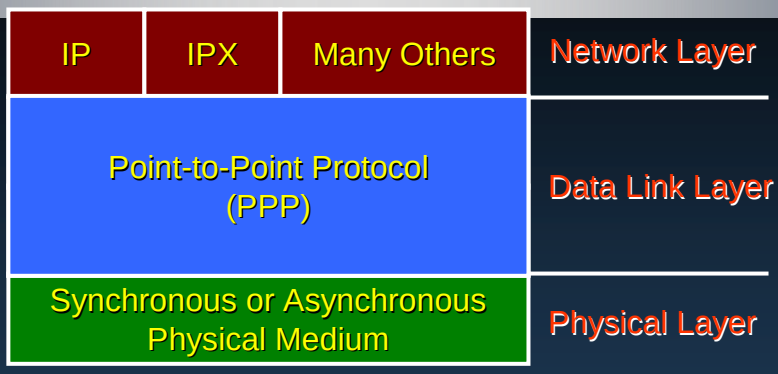
- What is PPP?
  - Three main components:
  - HDLC:
    - HDLC protocol for encapsulating datagrams over point-to-point links.
  - LCP:
    - Extensible Link Control Protocol (LCP) to establish, configure, and test the data link connection.
  - NCPs:
    - Family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols.

Introducing PPP



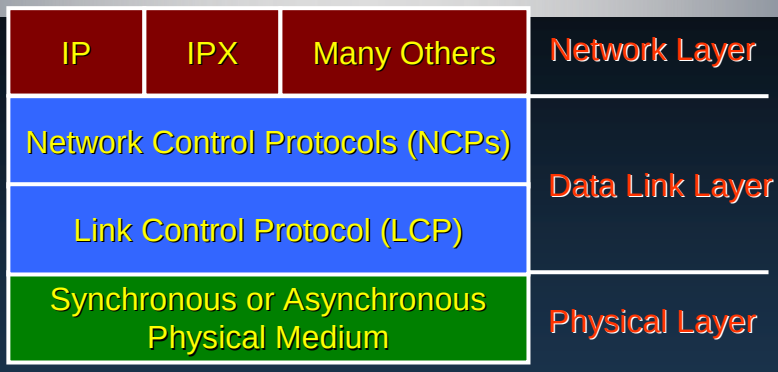
- What is PPP?
  - Three main components:
  - HDLC:
    - HDLC protocol for encapsulating datagrams over point-to-point links.
  - LCP:
    - Extensible Link Control Protocol (LCP) to establish, configure, and test the data link connection.
  - NCPs:
    - Family of Network Control Protocols (NCPs) for establishing and configuring different network layer protocols.

PPP Layered Architecture



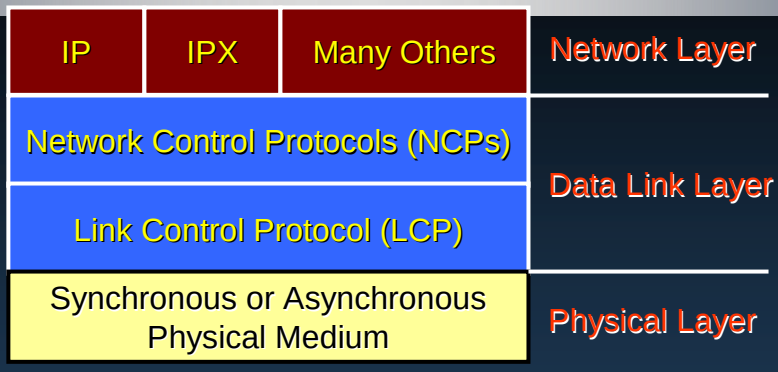
- PPP is a Data Link Layer protocol that provides a standard method for transporting multiprotocol datagrams over point-to-point links.
- Translation: IP *and* IPX *and* others, simultaneously, over a single dialup or higher speed WAN link.

PPP Layered Architecture



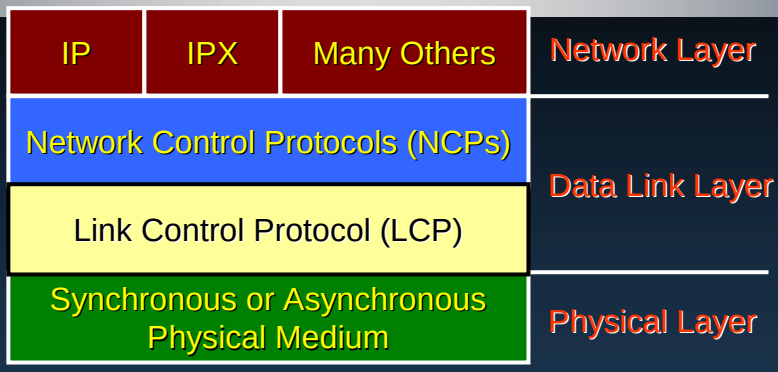
- PPP has a layered architecture:
  - **Link Control Protocol (LCP):** To establish, configure and test the connection.
  - **Network Control Protocols (NCPs):** A family of protocols to establish and configure Network Layer protocols.

PPP Layered Architecture



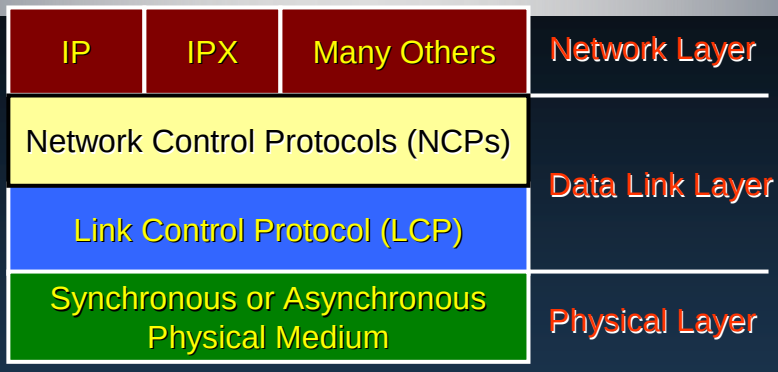
- PPP can be configured on multiple types of interfaces:
  - Asynchronous serial
  - Synchronous serial
  - High-Speed Serial Interface (HSSI)
  - Integrated Services Digital Network (ISDN)

PPP Layered Architecture



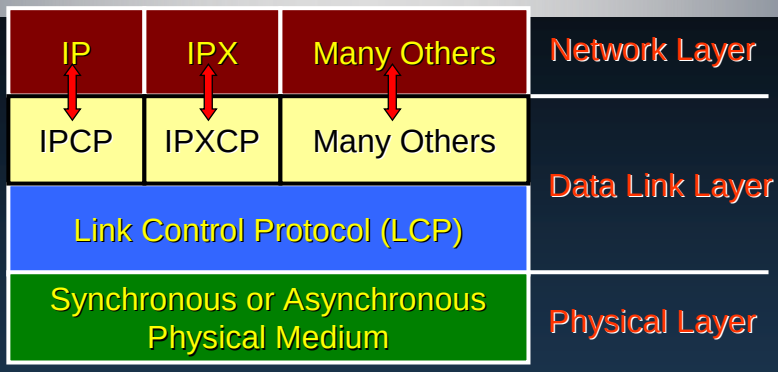
- PPP uses the Link Control Protocol (LCP) ***to negotiate and setup control options on the WAN link***.
  - Authentication, Compression, Error Detection, Multilink for load balancing, PPP Callback and link monitoring functions.

PPP Layered Architecture



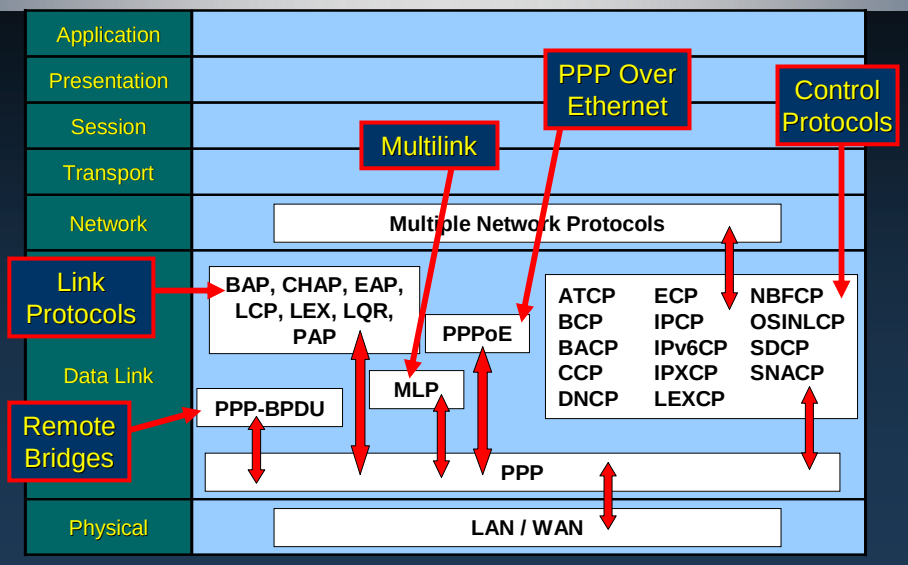
- PPP uses the Network Control Protocols (NCPs) ***to permit multiple network layer protocols to operate on the same communications link***.

PPP Layered Architecture



- For every network layer protocol used, ***a separate Network Control Protocol (NCP) is provided***.
  - NCPs include functional fields containing standardized codes to indicate the network layer protocol type that PPP encapsulates.

FYI - PPP Protocol Suite



FYI - PPP Protocol Suite

- **PPP-BPDU:** PPP Bridge Protocol Data Unit
- **MLP:** Multilink PPP
- **PPPoE:** PPP Over Ethernet

- ***Link Protocols:***
  - **BAP:** Bandwidth Allocation Protocol
  - **CHAP:** Challenge Handshake Authentication Protocol
  - **EAP:** Extensible Authentication Protocol
  - **LCP:** Link Control Protocol
  - **LEX:** LAN Extension Interface Protocol
  - **LQR:** Link Quality Report
  - **PAP:** Password Authentication Protocol

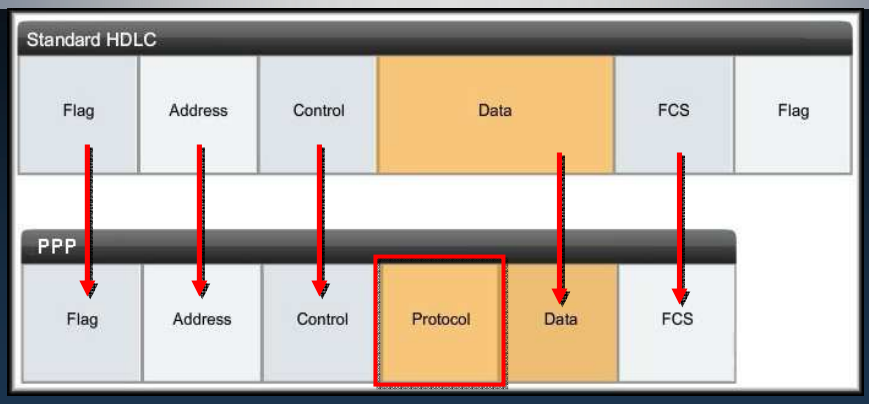
FYI - PPP Protocol Suite

- ***Control Protocols:***
  - **ATCP:** AppleTalk Control Protocol
  - **BACP:** Bandwidth Allocation Control Protocol
  - **BCP:** Bridging Control Protocol
  - **CCP:** Compression Control Protocol
  - **DNCP:** DECNet Phase IV Control Protocol
  - **ECP:** Encryption Control Protocol
  - **IPCP:** IP Control Protocol
  - **IPv6CP:** IPv6 Control Protocol
  - **IPXCP:** Novell IPX Control Protocol
  - **LEXCP:** LAN Extension Interface Control Protocol

FYI - PPP Protocol Suite

- *Control Protocols:*
  - NBFCP: NETBIOS Frames Control Protocol
  - OSINLCP: OSI Network Layer Control Protocol
  - SDCP: Serial Data Control Protocol
  - SNACP: Systems Network Architecture Control Protocol

PPP Frame Structure



- Notice how the PPP frame has been modeled very closely on the standard HDLC frame.
- The protocol field contains specific codes.

FYI - PPP Frame Structure

- The protocol code determines what protocol in the suite receives the payload.

Protocol Field Range (Hex)	Description
02xx – 1Exx xx01 – xx1F	Not Used (compression inefficient)
0xxx – 3xxx	Datagram belongs to a specific network protocol
8xxx – Bxxx	Datagram belongs to an associated NCP
4xxx – 7xxx	Datagram belongs to a low-volume protocol with no NCP
Cxxx - Exxx	Datagram is a control protocol

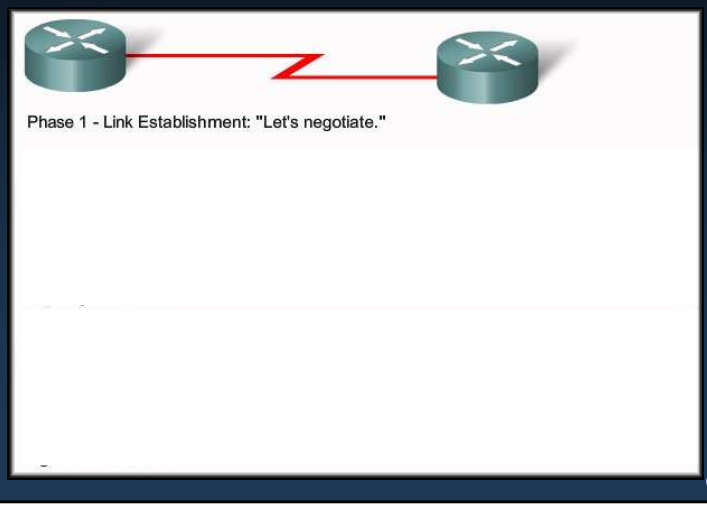
FYI - PPP Frame Structure

- Some of those codes:

Value (in hex)	Protocol Name
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c223	Challenge Handshake Authentication Protocol

Establishing a PPP Session

- PPP session establishment progresses through **Three Phases**.



Establishing a PPP Session

- Phase 1 – **Link Establishment**:
  - The LCP must first open the connection and negotiate configuration options.
- Phase 2 – **Determine Link Quality (Optional)**:
  - The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.
- Phase 3 – **Network Protocol Negotiation**:
  - The appropriate NCP separately configures the network layer protocols.
  - The NCP can bring them up and take them down at any time.

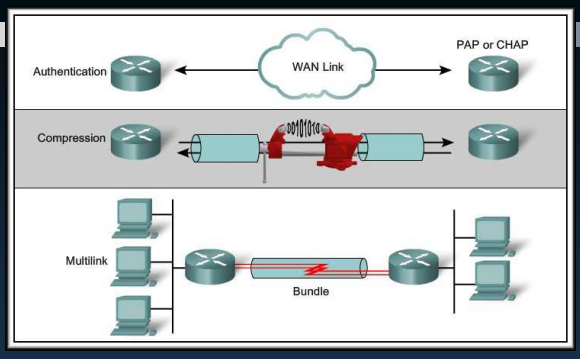
Establishing a Link with LCP

```
Router#configure terminal
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
```

- Phase 1 – Link Establishment:
  - In this phase each PPP device sends LCP frames to configure and test the data link.
  - LCP frames contain a configuration option field that allows devices to negotiate the use of options such as:
    - The maximum transmission unit (MTU)
    - Compression of certain PPP fields
    - The link-authentication protocol.

Establishing a Link with LCP

- If a configuration option is not included in an LCP packet, the default value is assumed.



- Before any network layer packets can be exchanged, LCP must first open the connection and negotiate the configuration parameters.
- This phase is complete when a configuration acknowledgment frame has been sent and received.

Establishing a Link with LCP

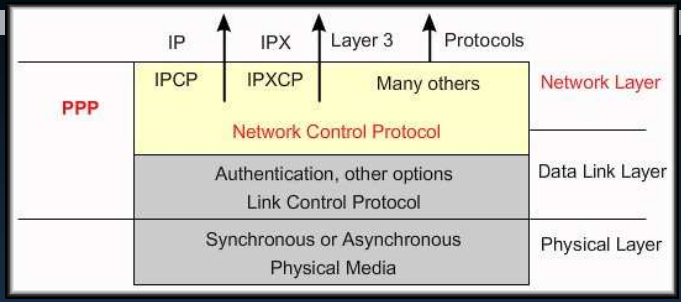
- Authentication:
  - After the link has been established and the authentication protocol decided on, the peer may be authenticated.
  - Authentication, if used, takes place before the network layer protocol phase is entered.

Establishing a Link with LCP

Features	How It Operates	Protocol
Authentication	Require a password and perform challenge handshake	PAP CHAP
Compression	Compress data at source and reproduce data at destination	Stacker, Predictor, TCP Header, or MPPC
Error Detection	Monitor data dropped on link Avoid frame looping	Quality Magic Number
Multilink	Load balancing across multiple links	Multilink Protocol (MP)

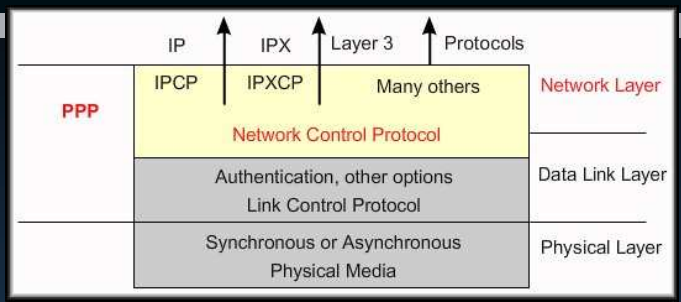
- As part of this phase, LCP also allows for an optional link-quality determination test.
  - The link is tested to determine whether the link quality is good enough to bring up network layer protocols.

Network Layer Protocol Negotiation



- PPP permits multiple Network layer protocols to operate on the same communications link.
  - For every Network layer protocol used, PPP uses a separate NCP module.
    - IP uses the IPCP module.
    - IP Version 6 uses the IPv6CP module.
    - IPX uses the IPXCP module.

Network Layer Protocol Negotiation



- In this phase the PPP devices send NCP packets to choose and configure one or more network layer protocols (e.g. IP).
- *Once each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link.*
- If LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

Network Layer Protocol Negotiation

```
Router#show interfaces serial 0/2/0
Serial 0/2/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544Kbit, DLY 20000 usec,
rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive
set (10sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output
hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
      .
```

LCP open = connection made.

NCPs

- The **show interfaces** command reveals the LCP and NCP states under PPP configuration.

FYI - PPP Configuration Options

Option Name	Option Type	Option Length	Description
Maximum Receive Unit (MRU)	1	4	MRU is the maximum size of a PPP frame and cannot exceed 65,535. The default is 1,500 and if neither peer is changing the default, it is not negotiated.
Asynchronous Control Character Map (ACCM)	2	6	This is a bit map that enables character escapes for asynchronous links. By default, character escapes are used.
Authentication Protocol	3	5 or 6	This field indicates the authentication protocol, either PAP or CHAP.
Magic Number	5	6	This is a random number chosen to distinguish a peer and detect looped back lines.
Protocol Compression	7	2	A flag indicating that the PPP protocol ID be compressed to a single octet when the 2-byte protocol ID is in the range 0x00-00 to 0x00-FF.
Address and Control Field Compression	8	2	A flag indicating that the PPP Address field (always set to 0xFF) and the PPP Control field (always set to 0x03) be removed from the PPP header.
Callback	13 or 0x0D	3	A 1-octet indicator of how callback is to be determined.

PPP Configuration Commands

- Enabling PPP:

```
Router#config t
Router(config)#interface s0/2/0
Router(config-if)#encapsulation ppp
```

- Configuring Compression:
  - You can configure point-to-point compression on serial interfaces after you have enabled PPP. Because this option invokes a software compression process, it can affect system performance. If the traffic already consists of compressed files (.zip, .tar, or .mpeg, for example), do not use this option.

```
Router(config-if)#compress [predictor|stac]
```


PPP Configuration Commands

- Link Quality Monitoring:
  - LCP provides an optional link quality determination during the LCP Negotiation.
  - If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down.

```
Router(config-if)#ppp quality percentage
```

- Load Balancing Across Links:
  - Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) provides a method for spreading traffic across multiple physical WAN links.

```
Router(config-if)#ppp multilink
```

Verifying a Serial PPP Configuration

- Use the **`show interfaces serial`** command to verify proper configuration PPP encapsulation.
  - When you configure PPP, the output of the show interfaces serial command should show **"encapsulation ppp"**.
  - When you configure PPP, you can check its LCP and NCP states.

Command	Description
`show interfaces`	Displays statistics for all interfaces configured on the router or access server
`show interfaces serial`	Displays information about a serial interface
`debug ppp`	Debugs PPP
`undebug all`	Turns off all debugging displays

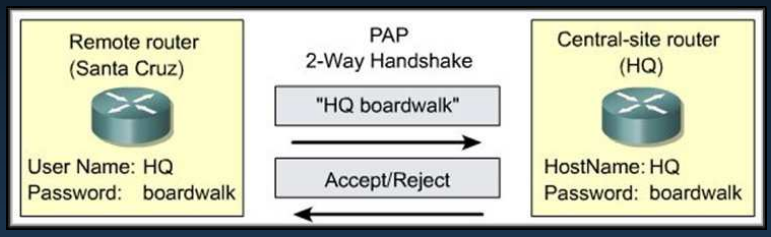
Troubleshooting PPP Encapsulation

```
debug ppp {packet | negotiation | error | authentication | compression |
           cbcp}
```

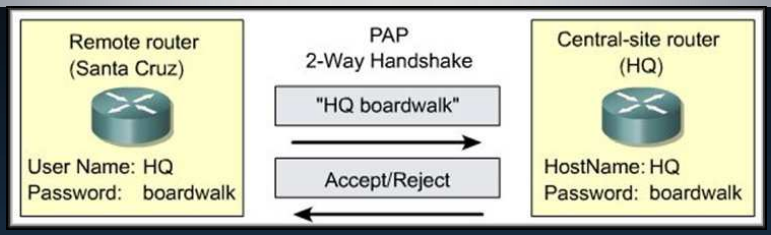
Parameter	Usage
`packet`	Displays PPP packets being sent and received. (This command displays low-level packet dumps.)
`negotiation`	Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
`error`	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
`authentication`	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
`compression`	Displays information specific to the exchange of PPP connections using MPPC. This command is useful for obtaining incorrect packet sequence number information where MPPC compression is enabled.
`cbcp`	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB.

Point-to-Point Protocol (PPP)

PPP Authentication



PPP Authentication Protocol - PAP



- **Password Authentication Protocol (PAP):**
  - Not a strong protocol.
  - Username/Password sent in **clear text**.
  - Uses a **two-way handshake**.
  - **Remote node** in control of attempts.
    - Username/Password pair are **repeatedly sent** across the link until authentication is acknowledged or the link is terminated.

Configuring PAP

```
Rtr(config)#username remote-host
                    password remote-password
```

- This needs to match the *ppp pap sent-username and password* on the remote host.
- When received and validated, routers with these username/password combinations will be allowed to connect.

```
Rtr(config-if)#ppp pap
          sent-username local-host-username
               password local-host-password
```

- The passwords do not have to be the same on the remote and the local routers.
- It should not be the same as the enable-secret password.

PAP

```
hostname SantaCruz
username HQ password HQpass

interface serial 0/2/0
  ip address 172.25.3.5 255.255.255.252
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username SantaCruz
                  password SantaCruzpass
```

Remote usernames and passwords

```
hostname HQ
username SantaCruz password SantaCruzpass

interface serial 0/2/0
  ip address 172.25.3.6 255.255.255.252
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username HQ
                  password HQpass
```

Local usernames and passwords

1. Establish PPP Link

2. Configuration request for PAP authentication.

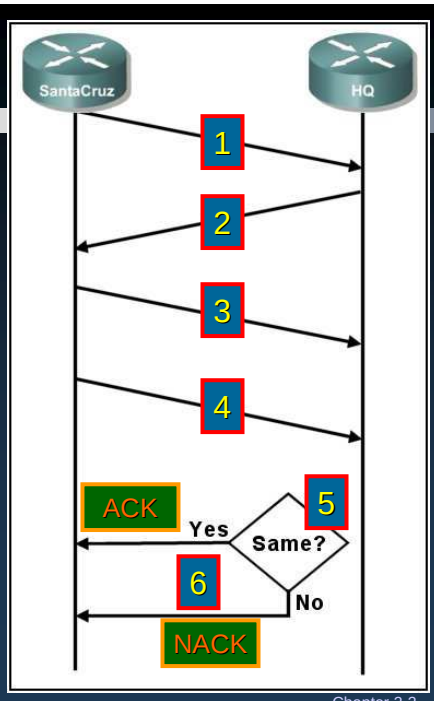
3. Configuration ACK.

4. SantaCruz sends the *SantaCruz* username and *SantCruzpass* password configured for the interface.

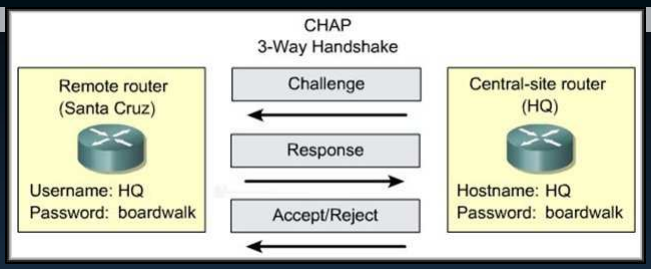
5. HQ looks up the received name, retrieves the password and *compares configured to received.*

6. *If they are the same*, send an ACK and allow access.

   If they are not the same, send a NACK and terminate the connection.

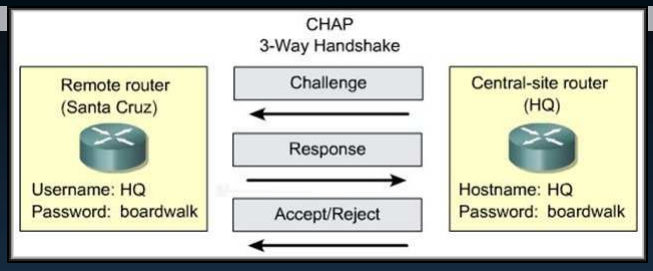


PPP Authentication Protocol - CHAP



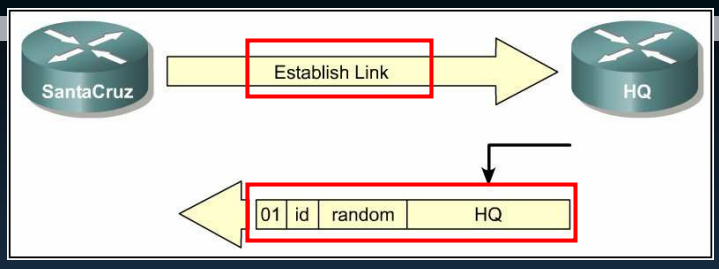
- **Challenge Handshake Authentication Protocol (CHAP):**
  - The preferred authentication protocol.
  - Uses a **three-way handshake**.
  - Challenge/Response messages use MD5 hashing on random values and the password.
  - Challenge/Response sequence **repeated at random periods** during the connect.

PPP Authentication Protocol - CHAP



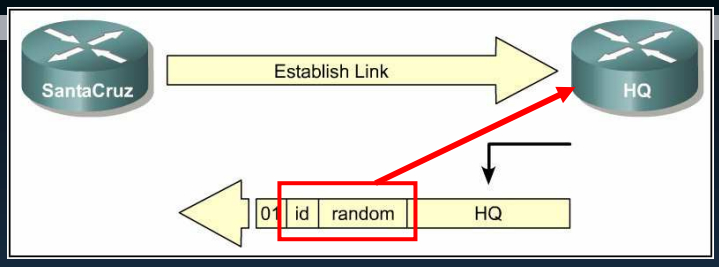
- CHAP provides protection against playback attack through the use of a variable and hashed challenge value that is unique and unpredictable.
- The use of repeated challenges is intended to limit the time of exposure to any single attack.
- Unlike PAP, **the local router or a third-party authentication server is in control** of the frequency and timing of the challenges.

PPP Authentication – CHAP Challenge



- **SantaCruz calls HQ and establishes a ppp link.**
- A CHAP challenge packet is built by the HQ router with the following characteristics:
  - **01** = challenge packet type identifier.
  - **ID** = sequential number that identifies the challenge.
  - **random** = a reasonably random number generated by the router.
  - **HQ** = the authentication name of the challenger.

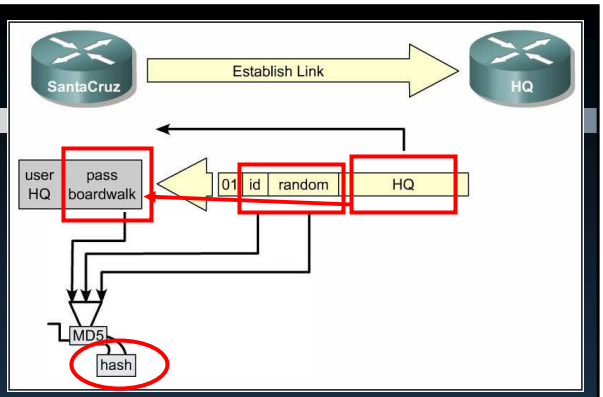
CHAP Challenge



- The ID and random values are kept on the HQ router or the ***called*** router.
- The challenge packet is sent to the ***calling*** router.
- A list of outstanding challenges is maintained.

CHAP Challenge

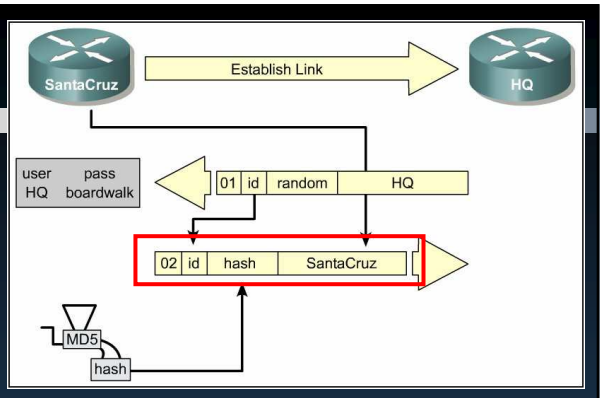
Receive CHAP Challenge



- The name **HQ** is used to look up the password.
- The **ID value, the random value and the password** are fed into the MD5 hash generator.
- The **result is the one-way MD5-hashed CHAP challenge** that will be sent back in the CHAP response.

CHAP Challenge

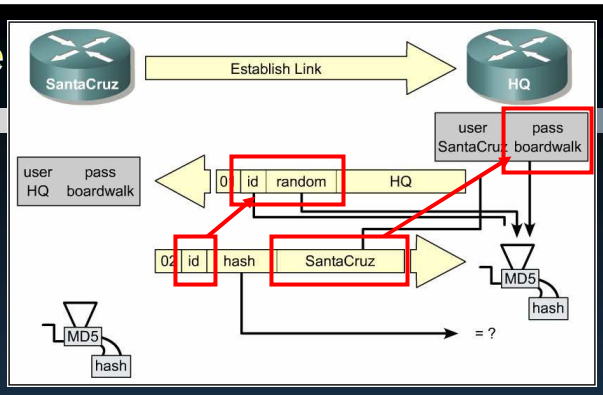
CHAP Response



- The response packet is assembled and sent.
  - 02 = CHAP response packet type identifier.
  - ID = copied from the challenge packet.
  - hash = the output from the MD5 hash generator.
  - SantaCruz = the hostname of the responding device.
    (*From the* ***hostname*** *command or the* ***ppp chap hostname*** *command).*

CHAP Challenge

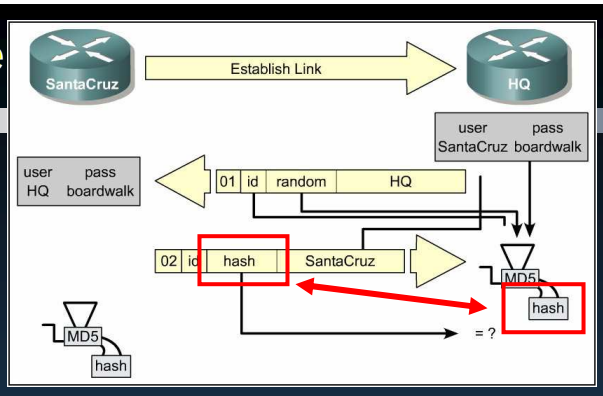
Receive CHAP Response



- The ID is used to find the original challenge packet.
- The name is used to look up the password from a configured name or a security server.
- The original ID, the original random value and the password are fed into the MD5 hash generator.

CHAP Challenge

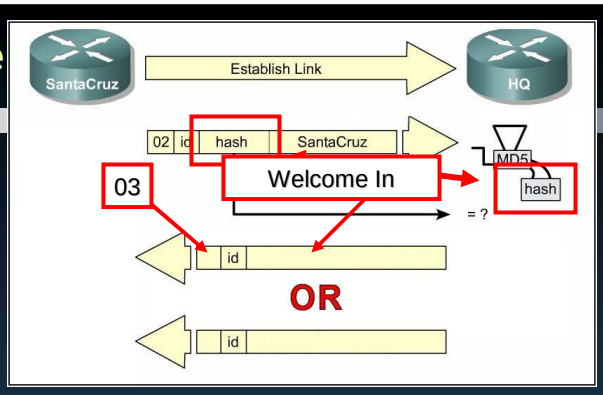
Receive CHAP Response



- The **hash value received** in the response packet is then ***compared to the calculated MD5 hash value***.
- CHAP authentication succeeds if the calculated and the received hash values are equal.

CHAP Challenge

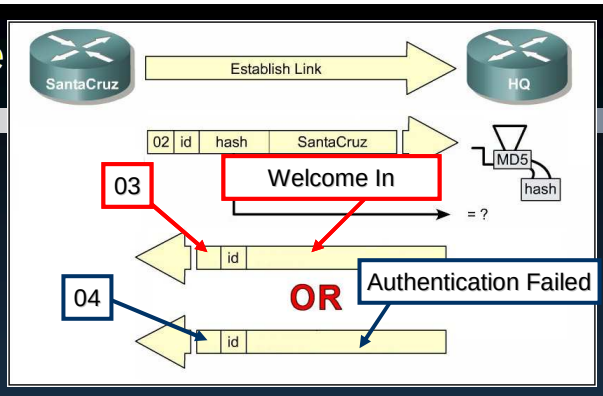
Success OR Failure



- If authentication is **successful**, a CHAP success packet is built from the following components:
  - **03** = CHAP success message type.
  - **ID** = copied from the response packet.
  - **"Welcome In"** is simply a text message providing a user-readable explanation.

CHAP Challenge

Success
OR
Failure



- If authentication fails, a CHAP failure packet is built from the following components:
  - 04 = CHAP failure message type.
  - ID = copied from the response packet.
  - "Authentication failure" or other text message, providing a user-readable explanation.

PPP Configuration Command Summary

```
Router(config)#username name password password

Router(config)#interface serial 0/2/0
Router(config-if)#ip address address subnetmask
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
```

OR

```
Router(config-if)#ppp authentication pap
Router(config-if)#ppp pap sent-username name
                        password password
```

debug ppp Command Summary

- **debug ppp *argument***
  - **debug ppp *authentication***
    - Display the authentication exchange sequence.
  - **debug ppp *chap***
    - Display CHAP packet exchanges.
  - **debug ppp *error***
    - Display protocol errors and error statistics.
  - **debug ppp *negotiation***
    - Display packets during connection establishment.
  - **debug ppp *packet***
    - Display packets being sent and received.