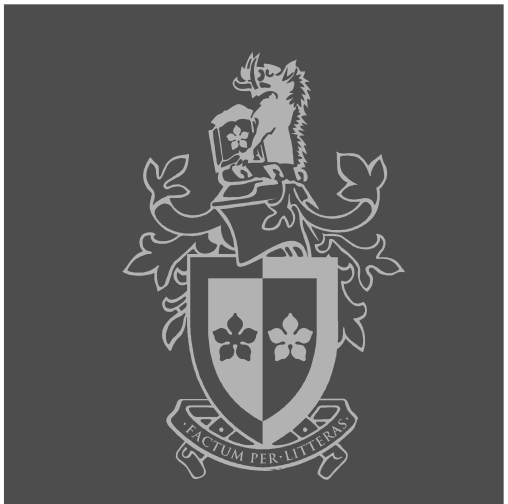
SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE20002 / TNE70003

Topic 9. PPP and CHAP



Rev. 1.3

Outline

9.1 Introducing HDLC and PPP

- Serial Point-to-Point Connections
- WAN Encapsulation Protocols
- HDLC & PPP Characteristics

9.2 PPP Operation

- PPP Link Establishment Phase
- PPP Authentication Link Quality Phase
- PPP Network Layer Protocol Phase

9.3 Challenge Handshake Authentication Protocol CHAP

- Overview CHAP Three Way Handshake
- CHAP Challenge
- CHAP Response
- CHAP Verification

9.4 CHAP Configuration & Verification

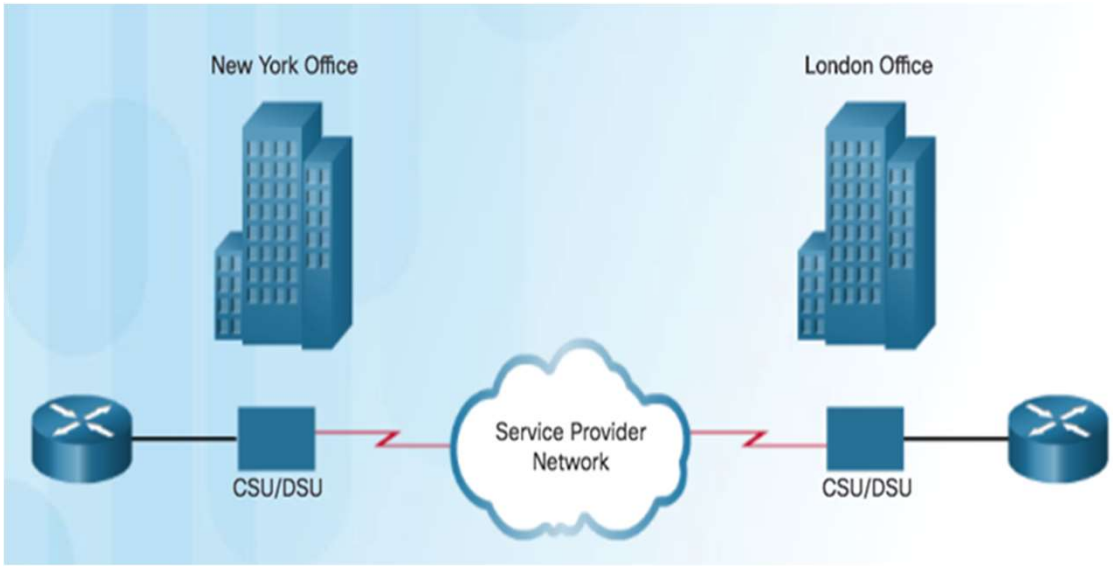
- Configure CHAP
- Verify PPP

Serial Communications

Serial Point-to-Point Connections

Point-to-point connections connect LANs to service provider WANs
& connect LAN segments.
WAN owned by service provider
LAN typically owned by organization.

A LAN-to-WAN point-to-point connection
is also referred to as a serial connection
or
leased-line connection.
Lines are leased from a carrier.



Time-Division Multiplexing TDM

'Time Division multiplexing' and other multiplexing techniques are used on a serial links to carry multiple channels or conversations..

eg. Integrated Services Digital Network or ISDN
uses TDM to carry multiple channels.

WAN Encapsulation

WAN Encapsulation Protocols

Data is encapsulated into frames before crossing the WAN link and must be configured for the appropriate Layer 2 protocol depending on WAN technology & communications equipment.

Leased Line Services

HDLC , PPP replaced SLIP on carrier services

Circuit Switched Services

Public Switched telephone Network ‘PSTN’

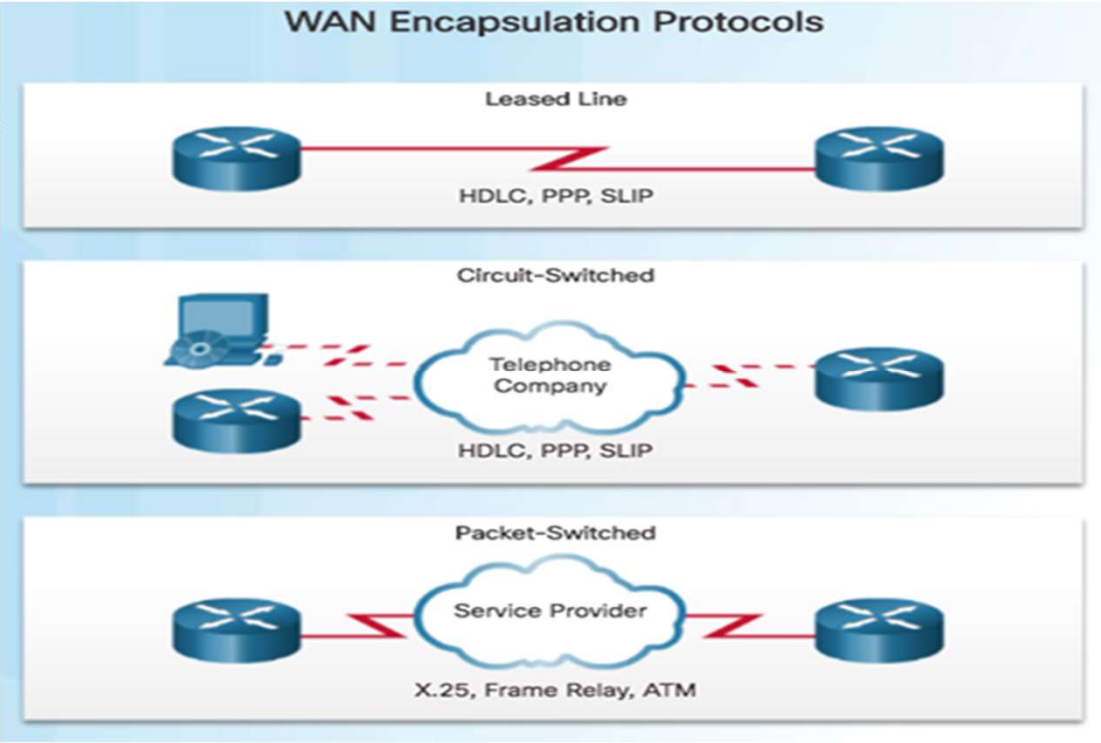
Integrated Services Digital Network ISDN

Packet Switched Services

X25 , Asynchronous Transfer Mode ‘ATM’

Frame Relay, Ethernet WAN

Multiprotocol Label Switching MPLS

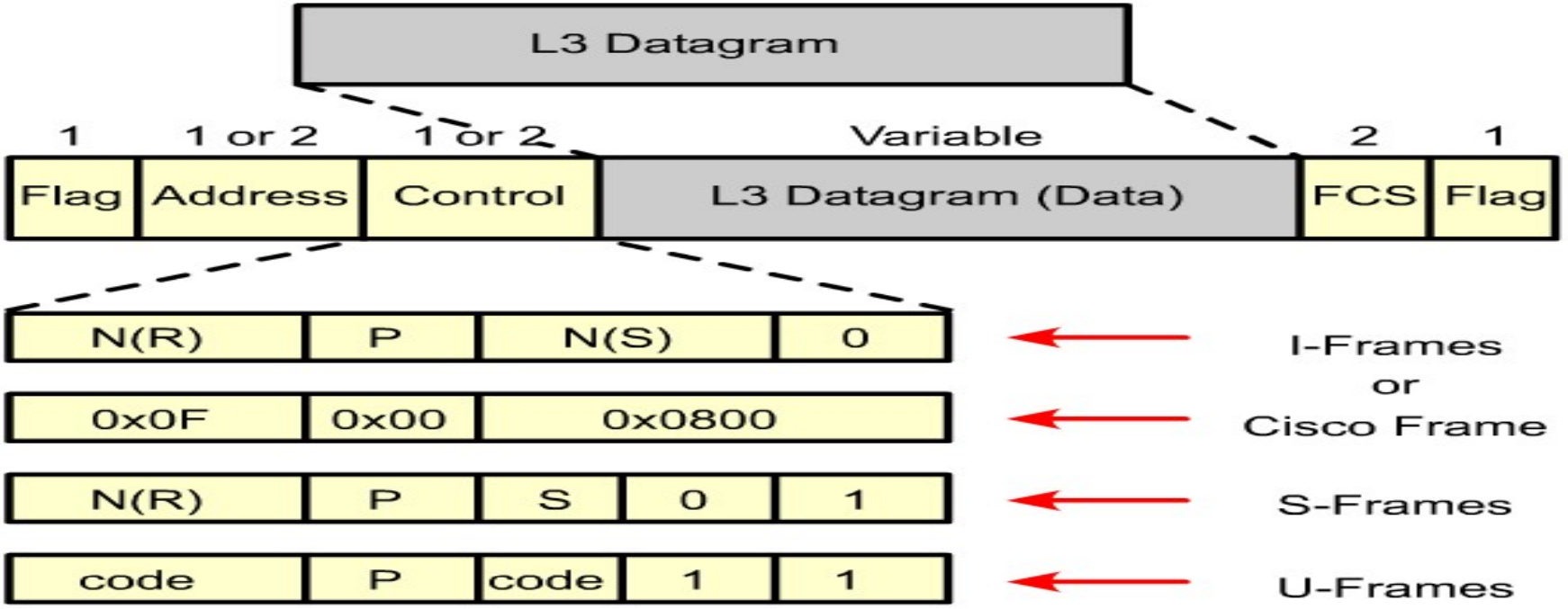


Point-to-Point Encapsulation

HDLC - Default encapsulation on point-to-point connections, dedicated links & circuit-switched connections using two ‘Cisco’ devices.

PPP - Provides router-to-router and host-to-network connections on various WAN circuits.
Has built-in security mechanisms such as PAP and CHAP

HDLC Link Access Protocols



HDLC → Derivative Protocols

- In **1979**, the ISO agreed on HDLC as a standard bit-oriented **data link layer protocol** that encapsulates data on synchronous serial data links.
- Since **1981**, ITU-T has developed a series of HDLC derivative protocols.
- The following **examples of derivative protocols** are called link access protocols:
  - Link Access Procedure, Balanced (LAPB) for X.25
  - Link Access Procedure on the D channel (LAPD) for ISDN
  - Link Access Procedure for Modems (LAPM) and **PPP** for modems **<**
  - Link Access Procedure for Frame Relay (LAPF) for Frame Relay

HDLC encapsulation

```
Router(config-if)#encapsulation hdlc
```

- The default encapsulation method used by Cisco devices on synchronous serial lines is Cisco HDLC.

```
Router#show interfaces s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is
255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
```

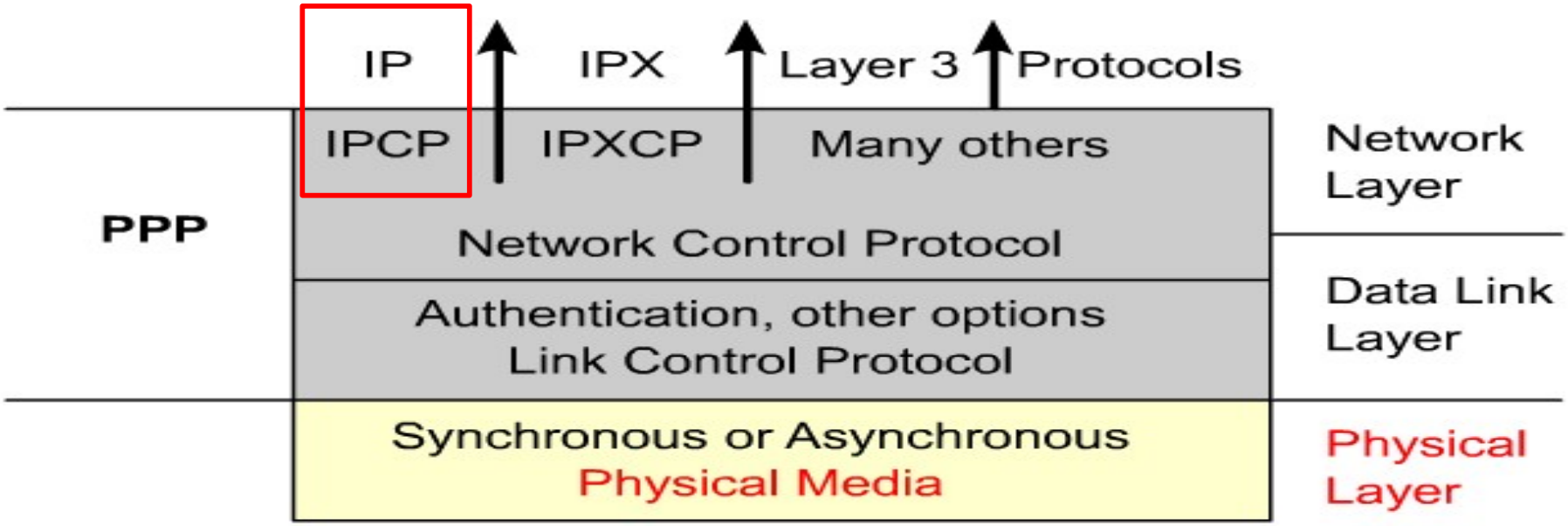
HDLC - -> PPP

HDLC ISO frame					
Flag	Address	Control	Data (Payload)	FCS	Flag
1 byte	1 byte	1 or 2 bytes	1500 bytes	2 (or 4) bytes	1 byte

PPP frame						
Flag	Address	Control	Protocol	Data (Payload)	FCS	Flag
1 byte	1 byte	1 byte	1 or 2 bytes	Up to 1500 bytes	2 (or 4) bytes	1 byte

- HDLC is the default Layer 2 protocol for Cisco router serial interfaces
- HDLC does not have a way to indicate which layer 3 protocol is being carried.
- PPP frame has a Protocol field that indicates it is carrying either a layer 3 IPV4 packet or IPV6 packet

PPP Layered Architecture



PPP contains two sub-protocols:

Network Control Protocol

Encapsulate and negotiate options for multiple network layer protocols

- Responsible for configuring, enabling and disabling the network layer protocol

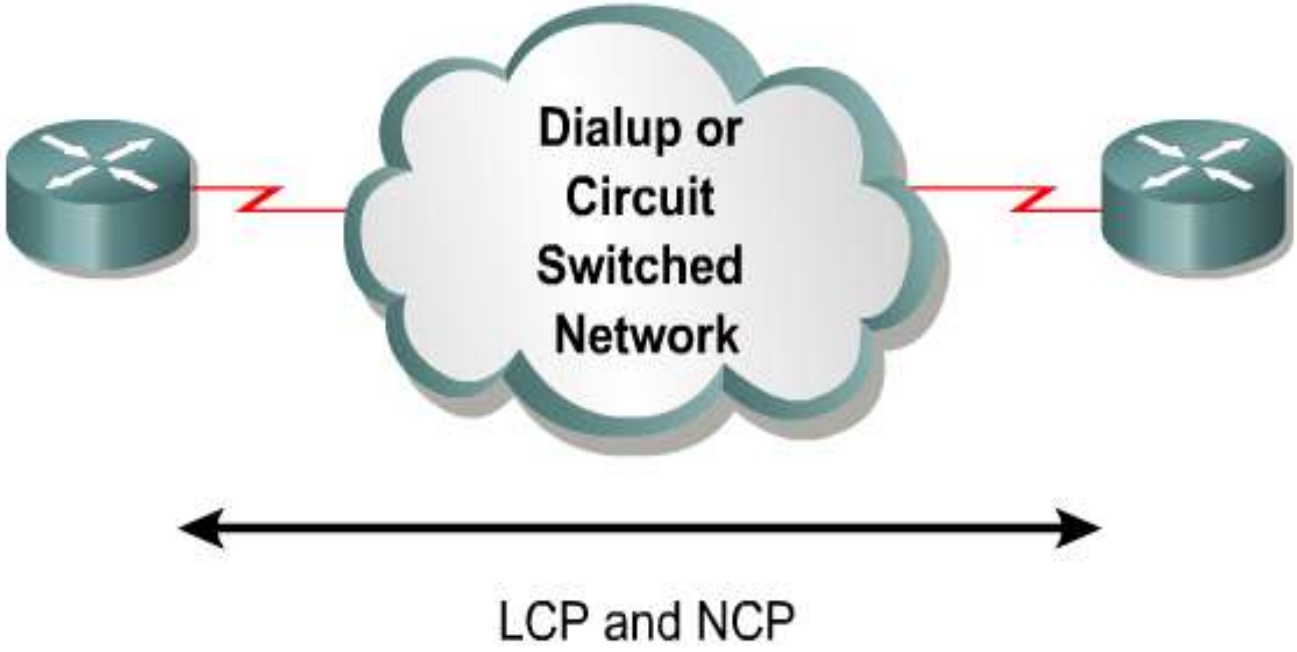
Link Control Protocol

- Negotiate and setup control options on the WAN data link.
- The LCP sits on top of the physical layer and is used to establish, configure, and test the data link connection.

9.2 PPP Operation

- PPP Link Establishment Phase
- PPP Authentication Link Quality Phase
- PPP Network Layer Protocol Phase

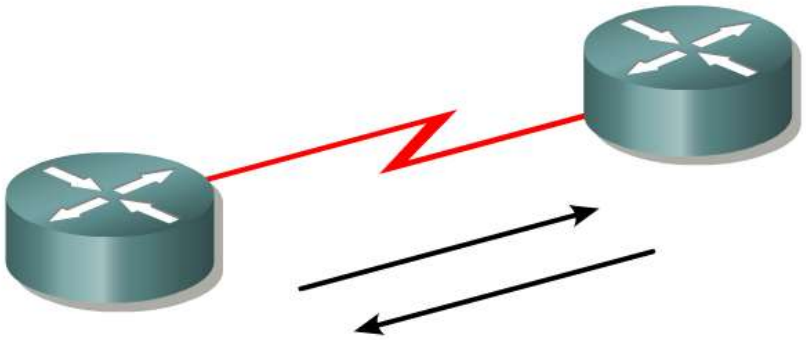
PPP Session Establishment – 3 Phases



PPP Session Establishment

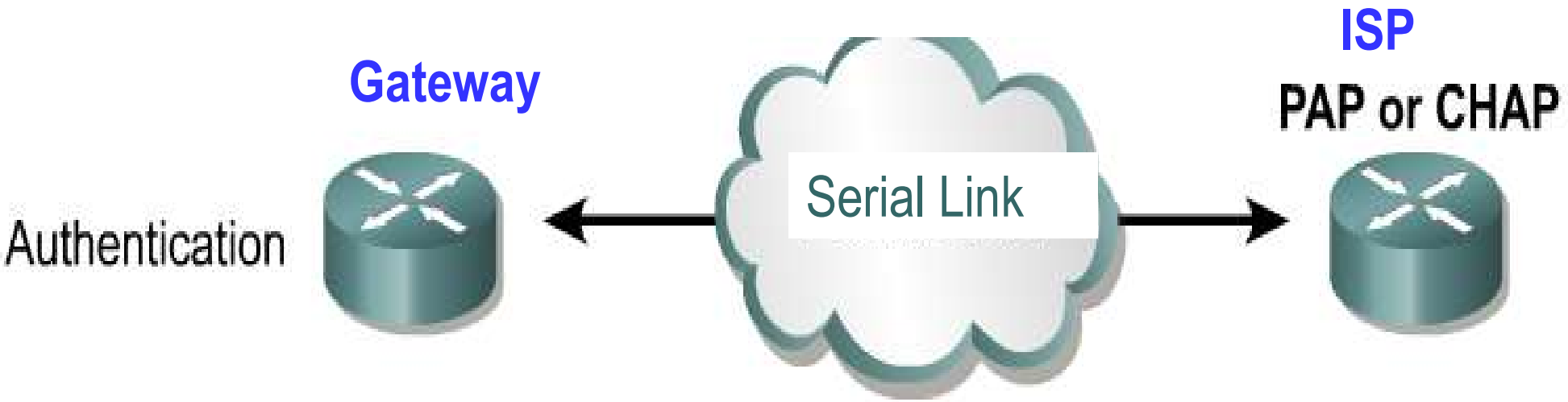
- Link Establishment Phase
- **Authentication/Link Quality Phase**
- Network Layer Protocol Phase

Phase 1 – Link Establishment



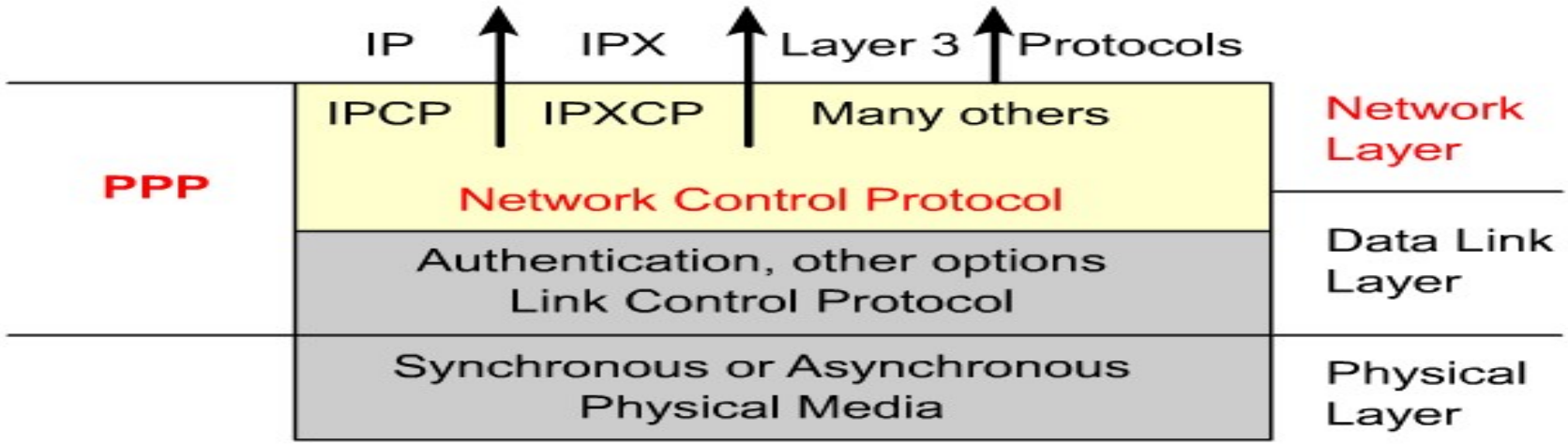
- In this phase each PPP device sends **LCP frames** to **configure and test the data link.**
- LCP frames contain a configuration option field that allows devices to negotiate the use of options such as:
  - the **maximum transmission unit** (**MTU**),
  - **compression** of certain PPP fields,
  - the **link-authentication** protocol.
- 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 ACK frame has been sent and received.

Phase 2 - Authentication | Link Quality



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

Phase 3 - Network Layer Protocol



- In this phase the PPP devices send **NCP frames** to choose **either IPv4 or IPv6 network layer protocol**.
- When the network layer protocol has been configured, packets can be sent over the link.
- The **show interfaces** command reveals the LCP and NCP states under PPP configuration.
- The PPP link remains configured for communications until LCP or NCP frames close the link or until an inactivity timer expires or a user intervenes.

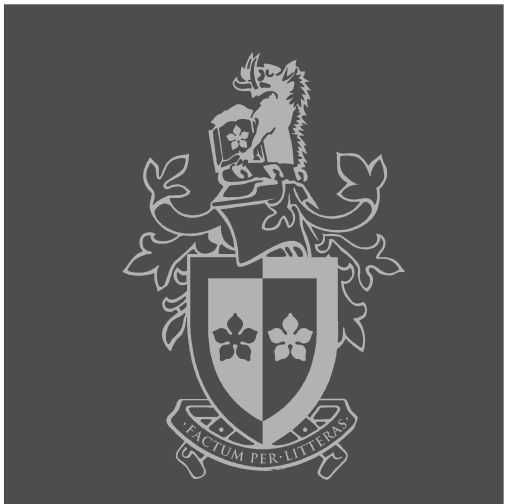
9.3 Challenge Handshake Authentication Protocol CHAP

- Overview CHAP Three Way Handshake
- CHAP Challenge
- CHAP Response
- CHAP Verification

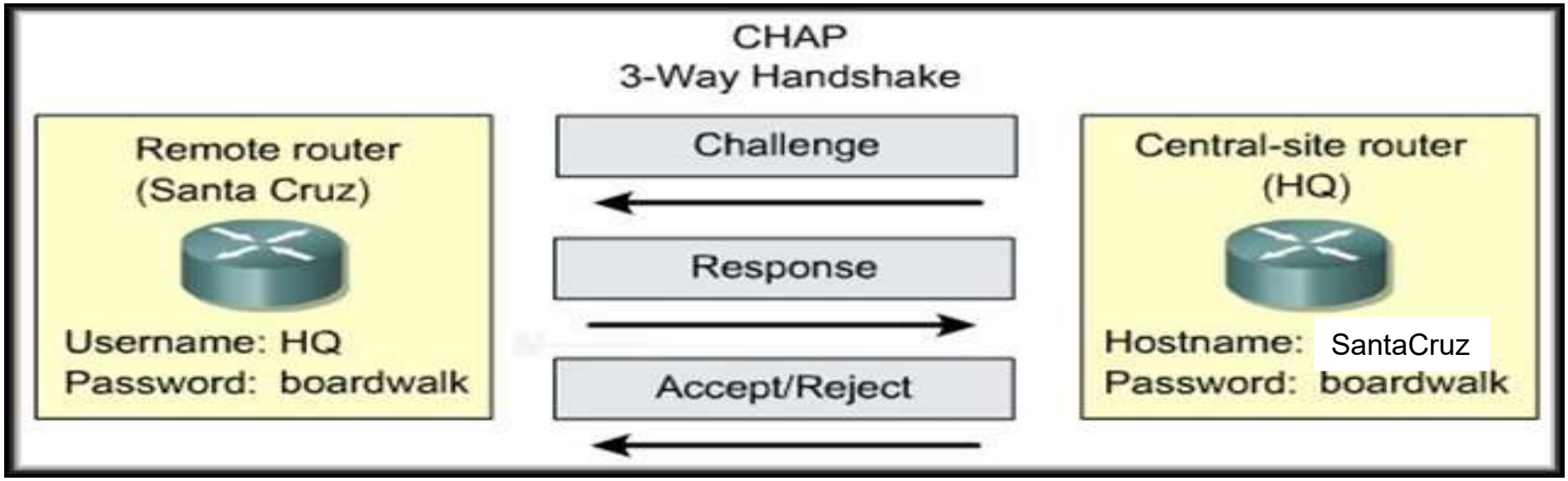
SWINBURNE UNIVERSITY OF TECHNOLOGY

CHAP

Challenge
Handshake
Authentication
Protocol



Challenge Handshake Authentication Protocol - CHAP



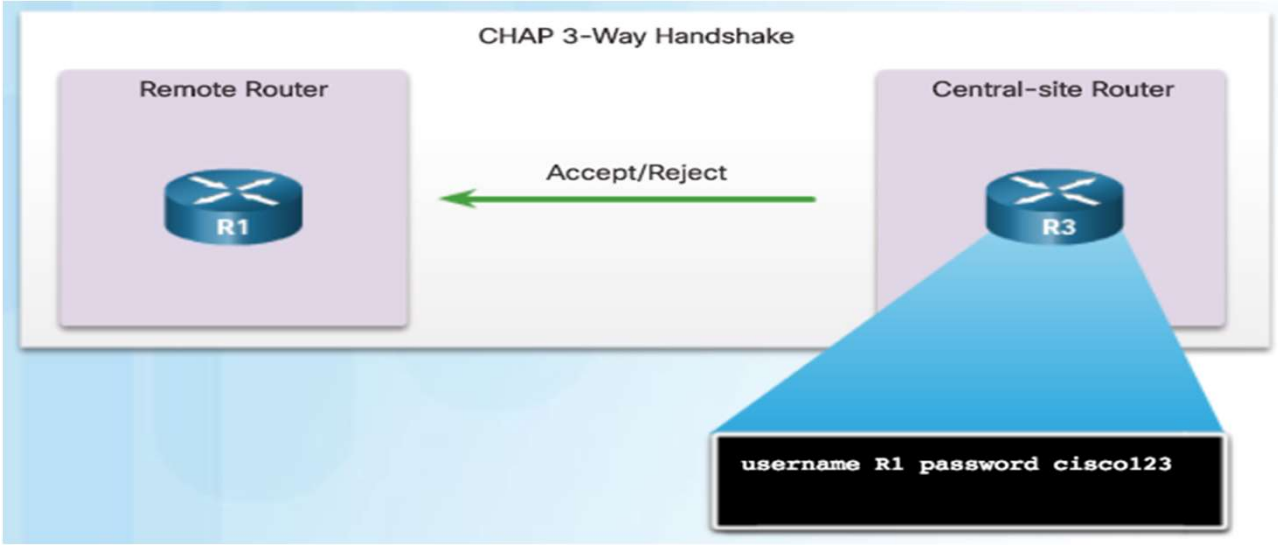
- CHAP is used at the startup of a link and periodically verifies the identity of the remote Host using a three-way handshake.
- During PPP link establishment phase, if (CHAP is configured) the Central-site router sends a "challenge" message to the Remote router.
- The Remote router responds with a value calculated using a one-way hash function, which is typically Message Digest 5 (MD5).

- This response is based on the password and challenge message.
- The Central-site router checks the response against its own calculation of the expected hash value.
- If the values match, the authentication is acknowledged, otherwise the connection is immediately terminated.

Challenge Handshake Authentication Protocol (CHAP)

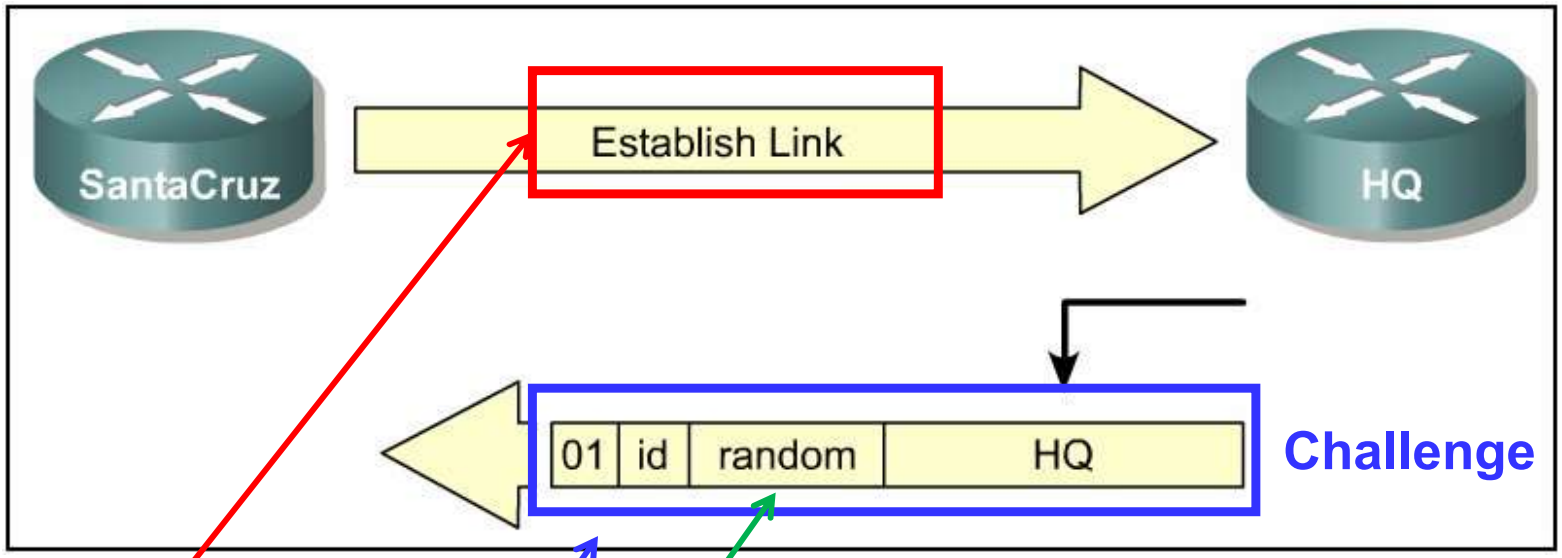
CHAP Random Challenges

CHAP conducts periodic Challenges to make sure that the remote node still has a valid password value.



- CHAP provides protection against playback (relay) attack through the use of a variable challenge value that is unique and unpredictable.
  - Playback attack:
    A breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction.
- Since the challenge is unique and random, the resulting hash value will also be unique and random.
- The Central-site router or a third-party authentication server is in control of the frequency and timing of the challenges.

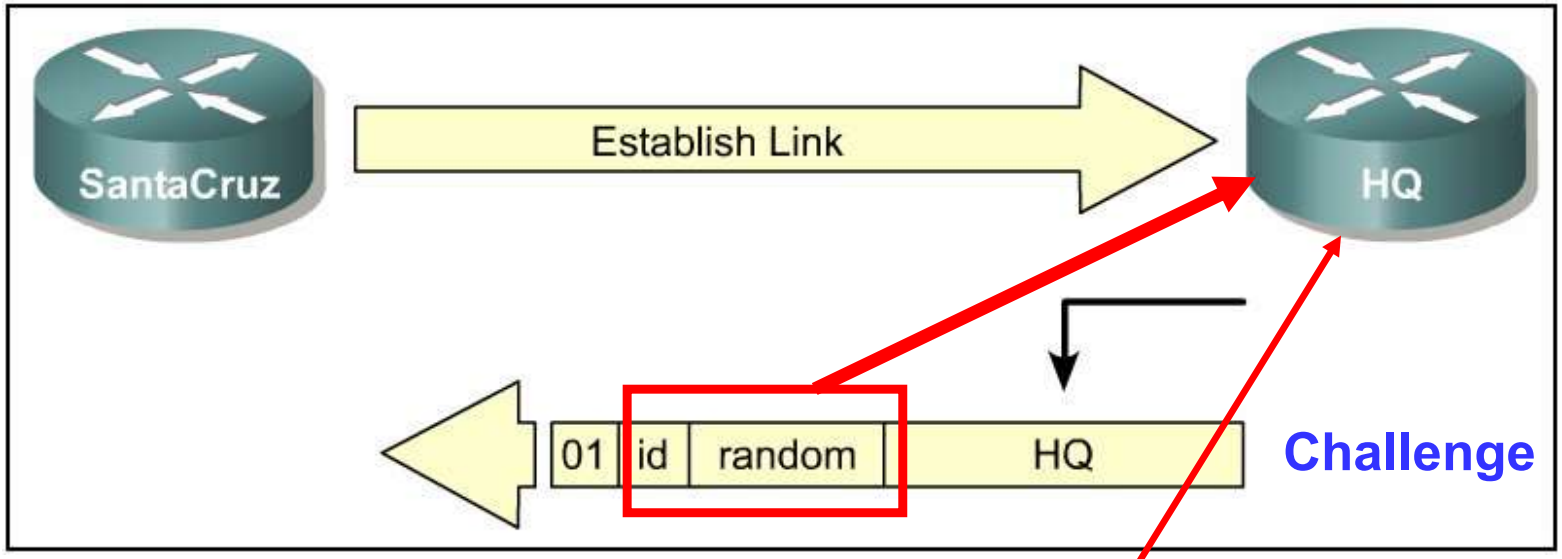
1. PPP Authentication – SantaCruz calls HQ



- SantaCruz **calls** HQ to establish a PPP link.

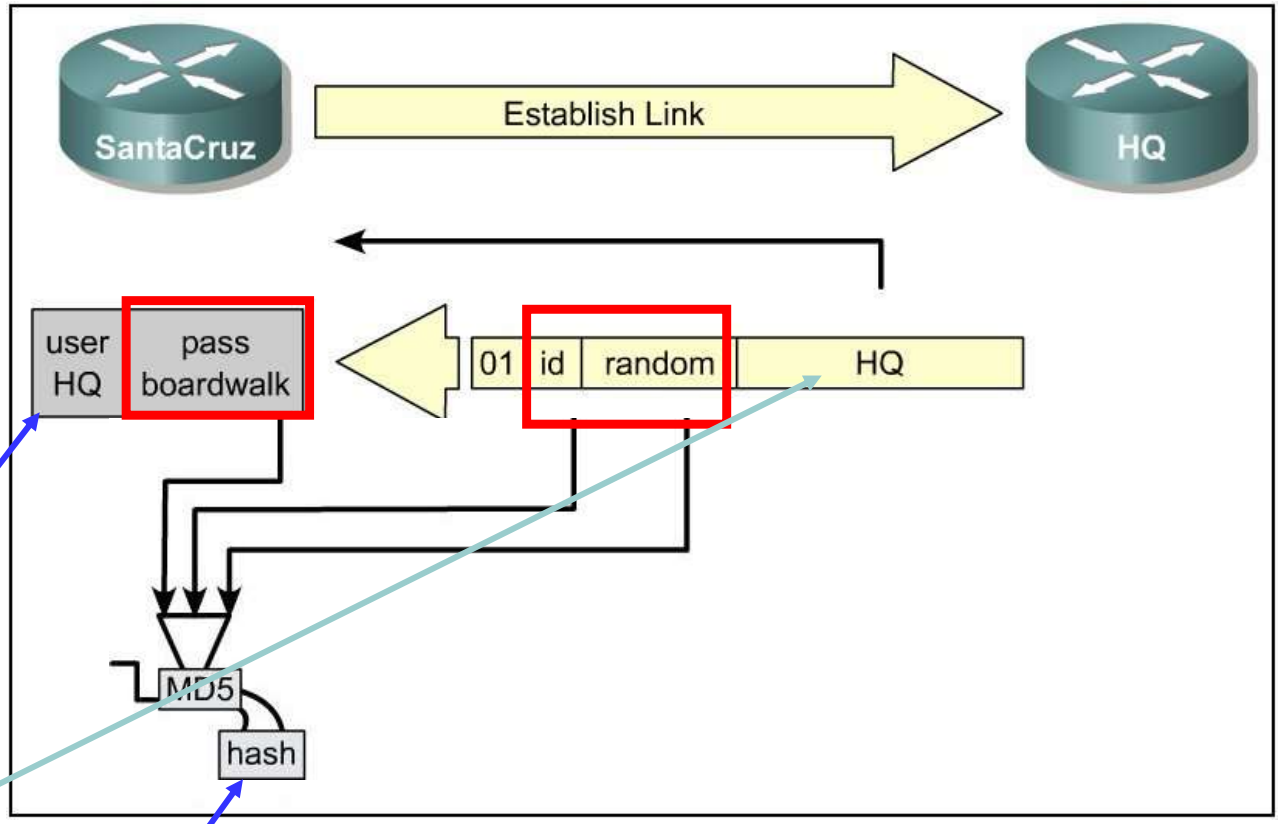
- HQ router sends a **CHAP challenge packet** with the following details:
  - **01** = challenge packet type identifier.
  - **ID** = sequential number that identifies the challenge.
  - **random** = a random value generated by the **HQ** router.
  - **HQ** = the authentication name of the challenger.

2. HQ CHAP Challenge sent to SantaCruz



- The challenge packet is sent to the *calling* (SantaCruz) router.
- The **ID** and **random** values are kept in a **table** on the HQ router.
- A list of outstanding challenges is maintained in **table** on HQ router.

3.SantaCruz receives CHAP Challenge

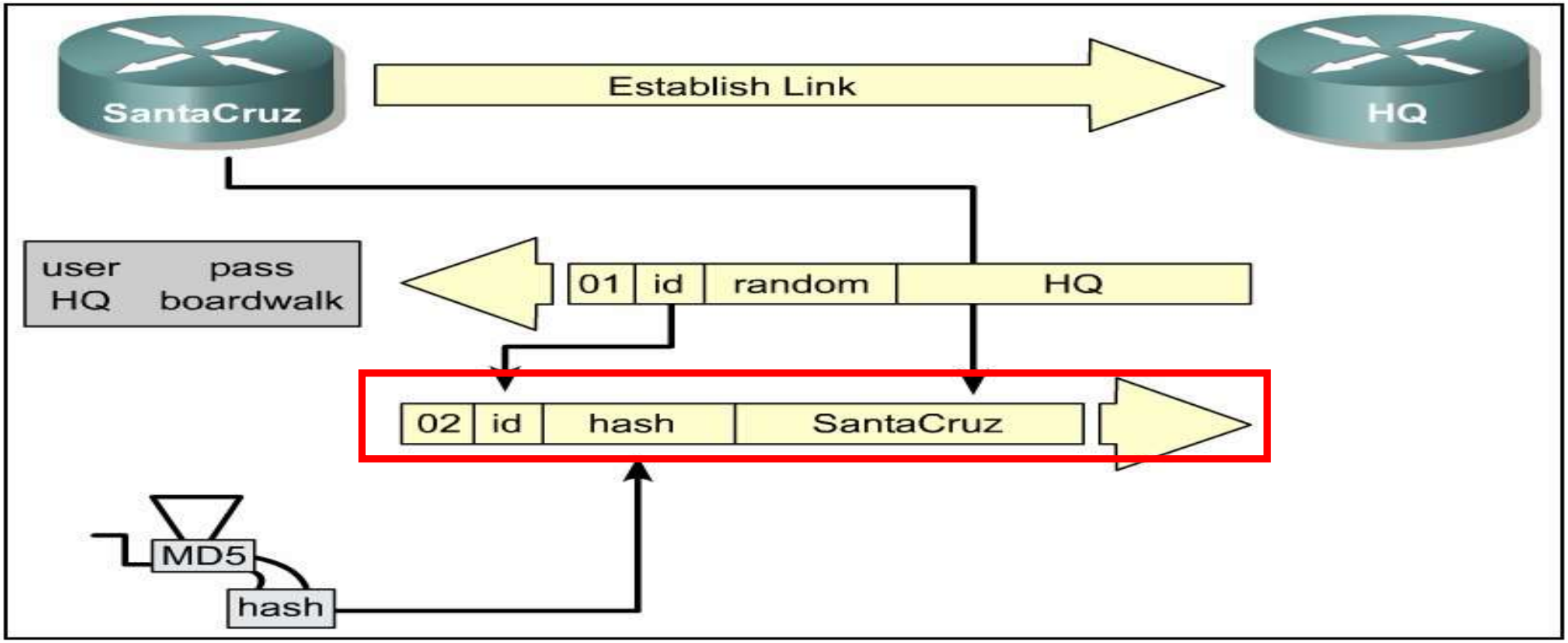


Receive CHAP Challenge

Table of User/Password

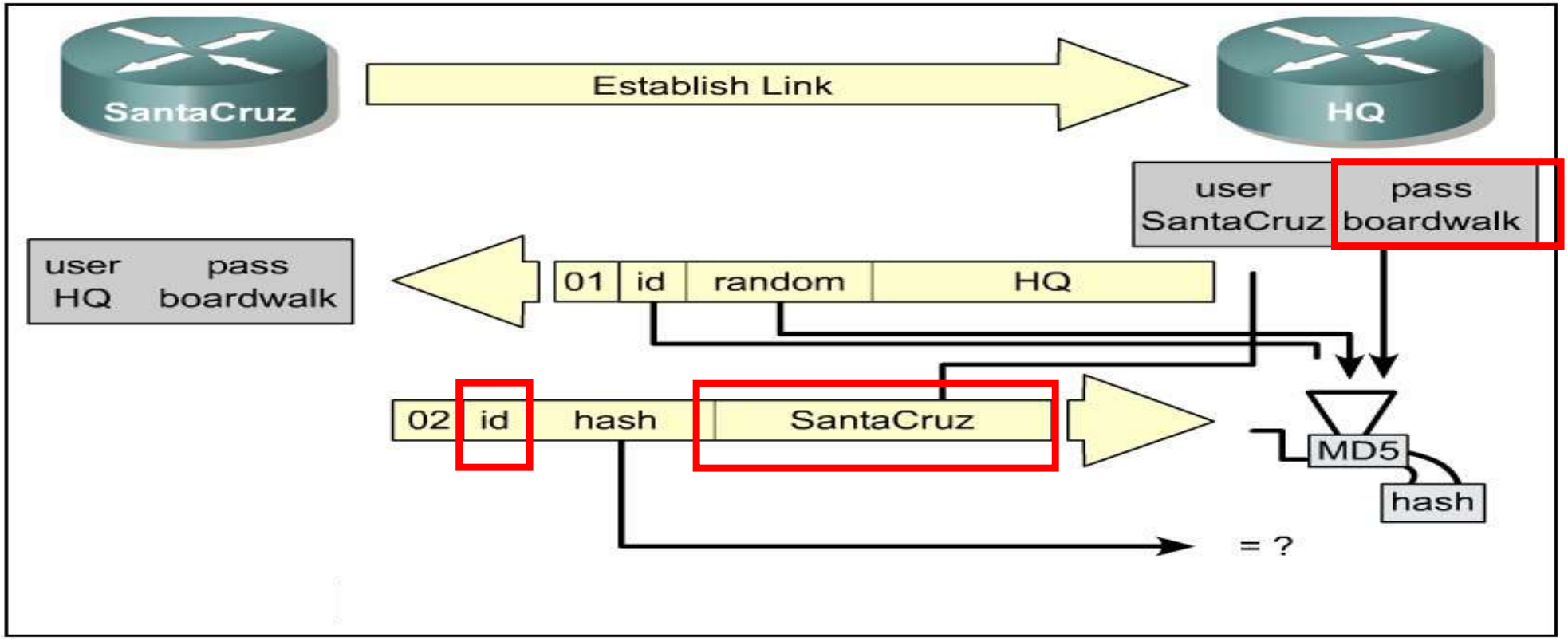
- The name HQ is used to look up the password.
- The ID value, the random value and the password are fed into the MD5 hash generator.
- The result is the one-way MD5-hashed CHAP challenge that will be sent back in the **CHAP response**.

4.SantaCruz sends 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.

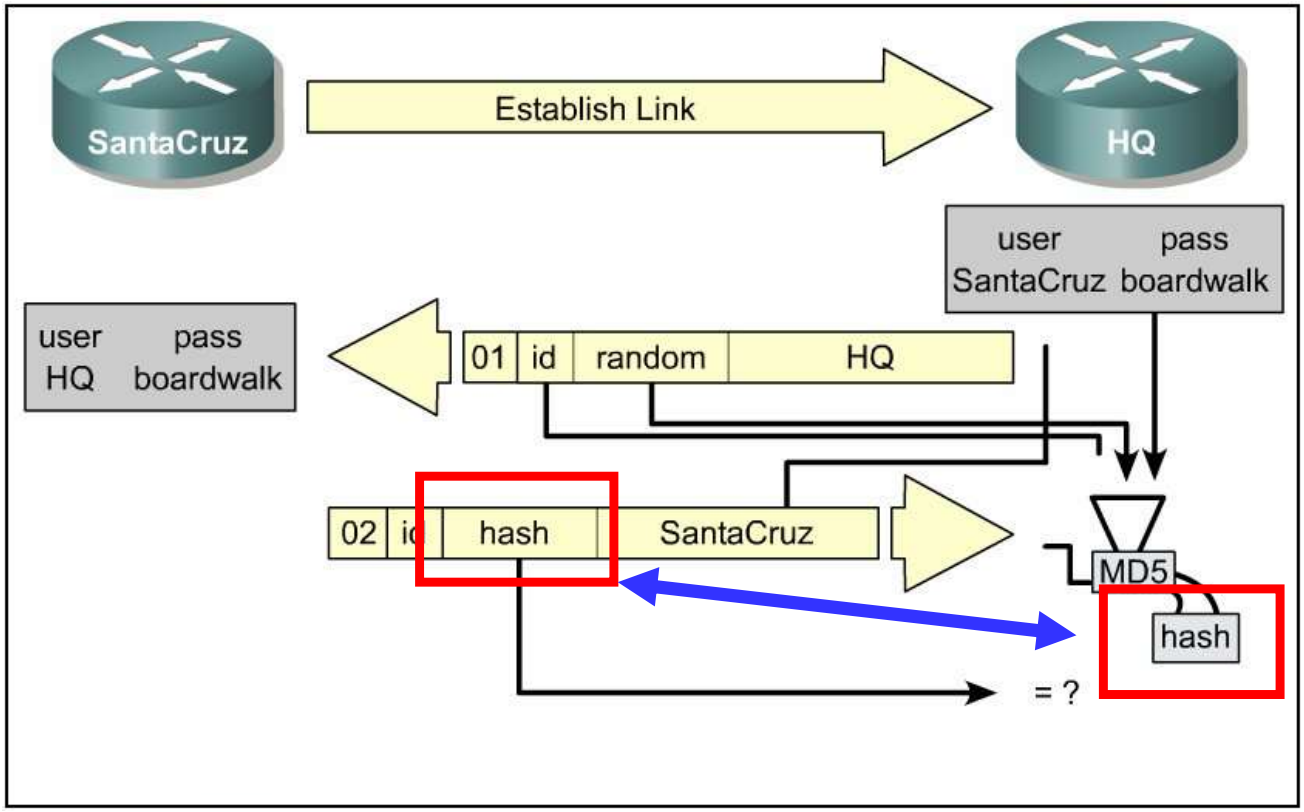
5. HQ receives CHAP Response



- The ID is used to find the original challenge packet in table.
- 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.

6. HQ Compares

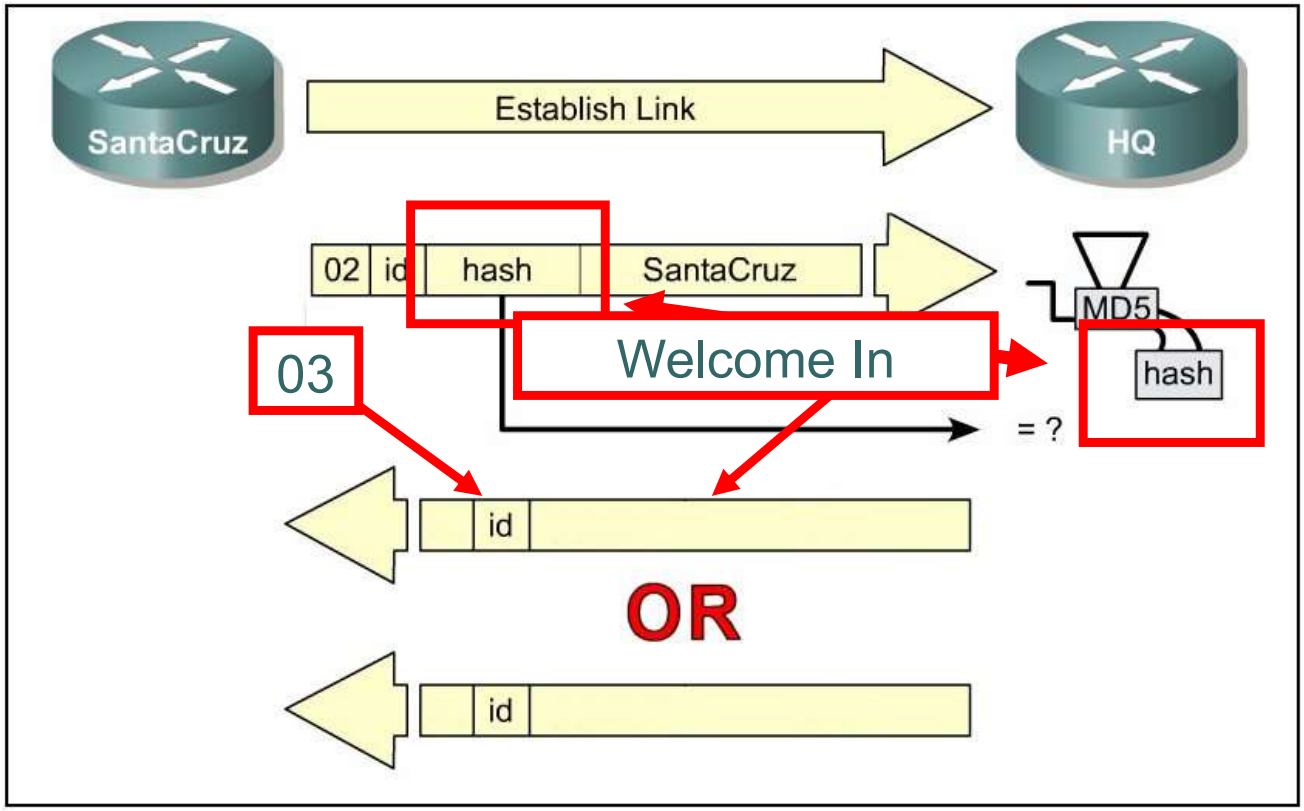
Receive CHAP Response



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

CHAP Verification

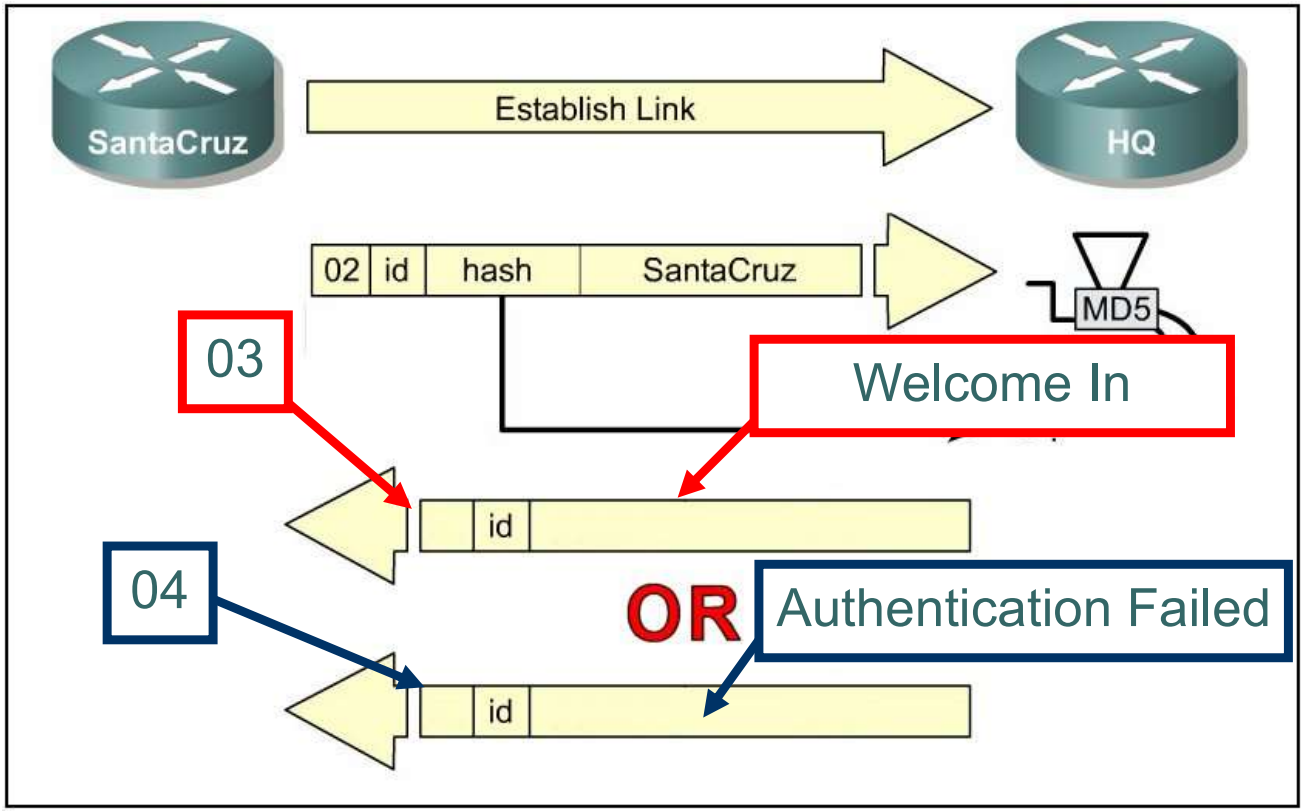
Success
OR
Failure



- 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.

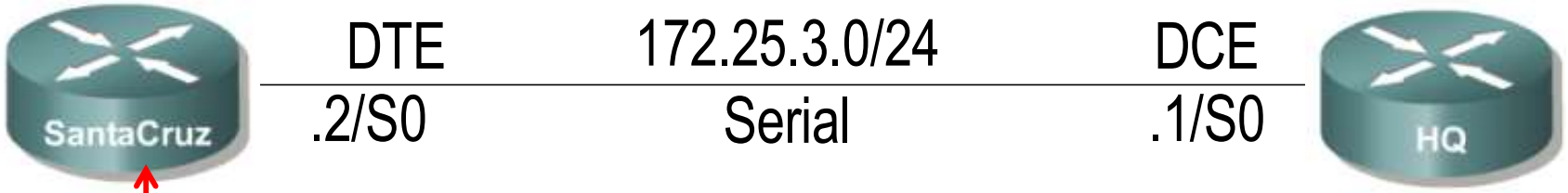
CHAP Verification

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.

CHAP Username + Password



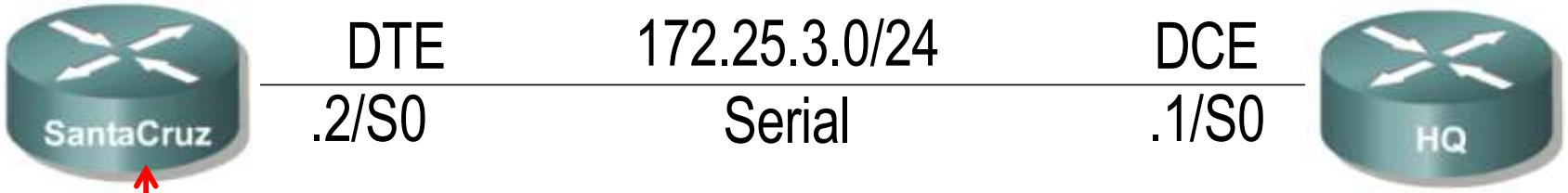

```
username HQ password cisco
interface Serial0
  ip address 172.25.3.2 255.255.255.0
  encapsulation ppp
  ppp authentication chap
```

```
username SantaCruz password cisco
interface Serial0
    ip address 172.25.3.1 255.255.255.0
    encapsulation ppp
    ppp authentication chap
```

9.4 CHAP Configuration & Verification

- Configure CHAP
- Verify PPP

Configuring CHAP




```
username HQ password cisco
interface Serial0
  ip address 172.25.3.2 255.255.255.0
  encapsulation ppp
  ppp authentication chap
```

```
username SantaCruz password cisco
interface Serial0
    ip address 172.25.3.1 255.255.255.0
    encapsulation ppp
    ppp authentication chap
```

Verifying PPP

```
Router#show interfaces serial0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive
set (10 sec)
  LCP Open                          <- LCP
  Open: IPCP, CDPCP                 <- NCP
  Last input 00:00:05, output 00:00:05, output
hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
```

debug ppp negotiation

```
Router#debug ppp negotiation
PPP protocol negotiation
    debugging is on
. . .
BR0:1 LCP: State is Open
. . .
PPP: Phase is AUTHENTICATING
. . .
BR0:1 IPCP: State is Open
. . .
```

Phase	Description
DOWN	In this phase, PPP is down. This message is seen after the link and PPP are completely brought down: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ESTABLISHING	PPP transitions to this phase when it receives an indication that the physical layer is up and ready to be used. LCP[1] negotiation occurs in this phase. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTICATING	If PPP authentication (CHAP[2] or PAP[3]) is desired on the link, then PPP transitions to this phase. Keep in mind that PPP authentication is optional. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
UP	Once authentication is complete, PPP transitions to the UP phase. NCP[4] negotiation occurs in this phase. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINATING	In this phase, PPP is shutting down. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

- The **debug ppp negotiation** command enables you to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution.
- During PPP negotiation, the link goes through several phases, as shown above.
- The end result is that PPP is either up or down.

debug ppp authentication

Output	Description
Se0/0 PPP: Phase is AUTHENTICATING, by both	Two way authentication
Se0/0 PAP: O AUTH-REQ id 4 len 18 from "left"	Outgoing authentication request
Se0/0 PAP: I AUTH-REQ id 1 len 18 from "right"	Incoming authentication request
Se0/0 PAP: Authenticating peer right	Authenticating incoming
Se0/0 PAP: O AUTH-ACK id 1 len 5	Outgoing acknowledgement
Se0/0 PAP: I AUTH-ACK id 4 len 5	Incoming acknowledgement

- The **debug ppp authentication** command displays the authentication exchange sequence.
- With two-way authentication configured, each router authenticates the other.
- Messages appear for both the authenticating process and the process of being authenticated.