

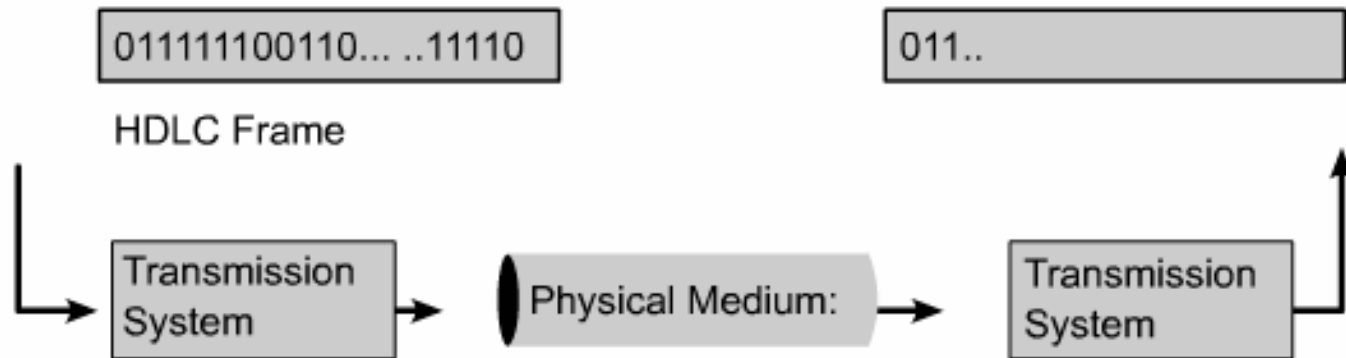
# **CCNA4; Module 3: PPP, PAP, CHAP**

Prednáška 10

# Dnes....

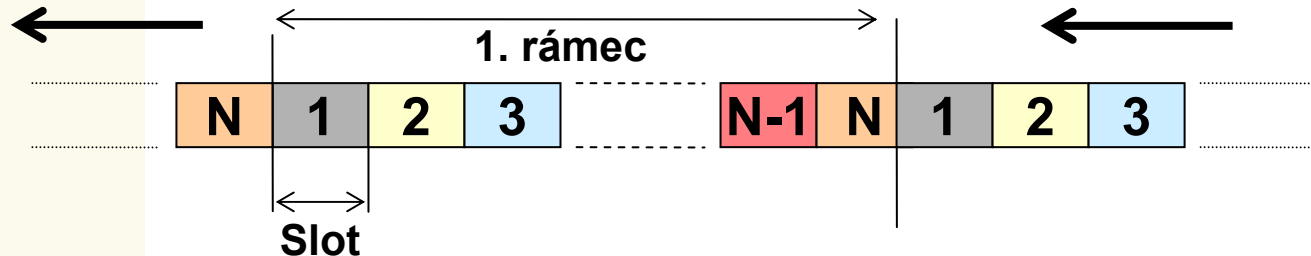
- Serial Point-to-Point links
- PPP
- PPP authentication
  - PAP
  - CHAP
- Configuring PPP

# Serial Communication



- **WAN is based on serial transmission on physical layer**
- **Transmission system encodes bits into electrical voltage using methods like NRZ-L or AMI**
- **Some of the many serial communications standards include the following:**
  - **V.35, RS-232-E, High-Speed Serial Interface (HSSI)**
- **Usually provided by Telco providers**

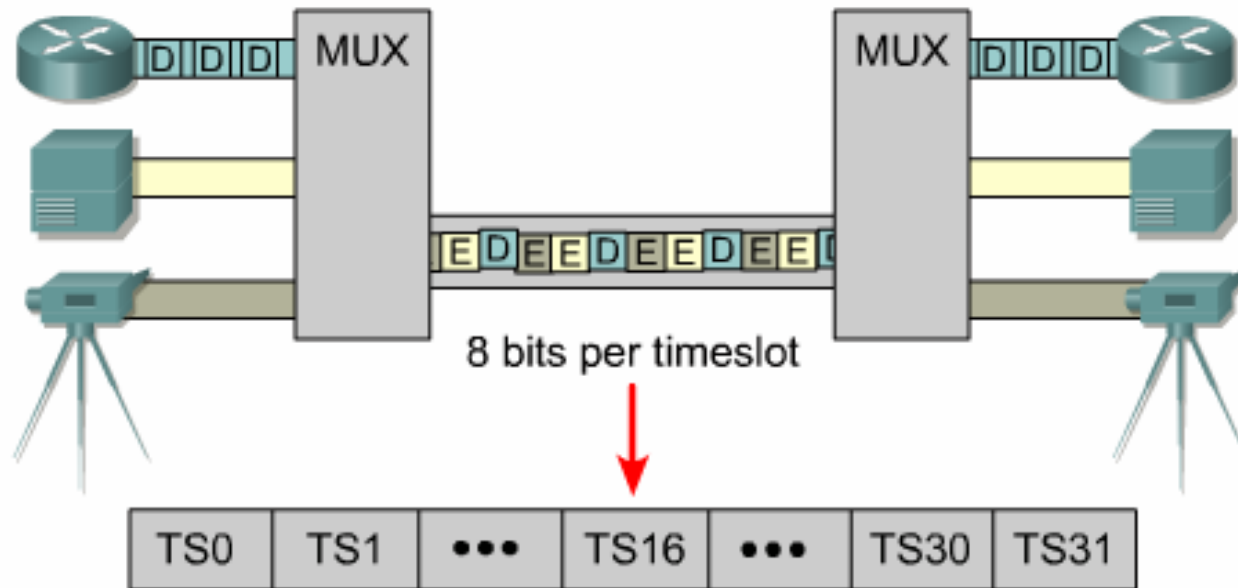
# Synchrónny prenos



- Prenosová cesta sa rozdelí na tzv. **časové sloty**
- Pozícia slotu je presne určená v čase, obsah rovnomerne obsadzovaný pomocou synchrónneho časového multiplexovania
- Používané napr. v telefónnej sieti

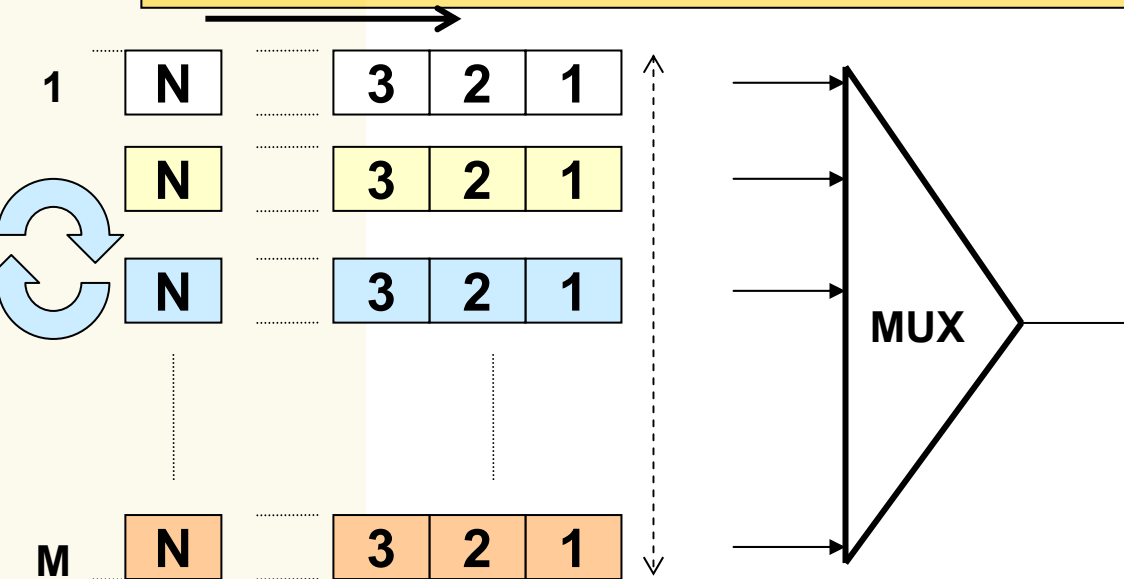
- **Výhody**
  - Jeden slot pridelený jednému komunikujúcemu
  - Získam garanciu prenosovej šírky pásma
  - Prenášajú sa len „užitočné dáta“
- **Nevýhody**
  - Plytvanie prenosovými prostriedkami (ak nemám konšt. gener. dáta)
  - Pre dátové siete nie veľmi vhodné

# Time-Division Multiplexing



- Timeslots are always present even if data is not available for sending.
- Bandwidth is statically allocated to the application.
- Protocol independent (HDLC, PPP).

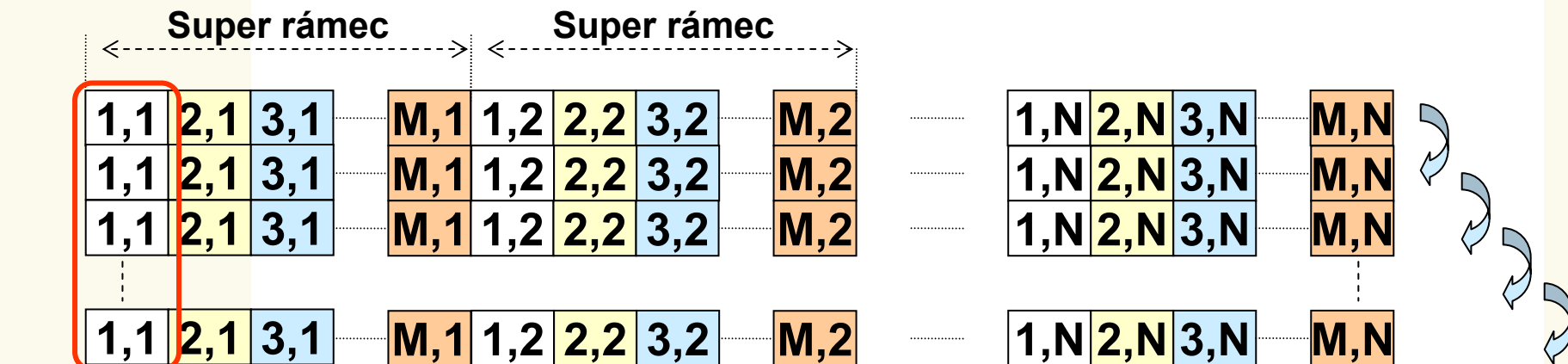
# Super rámce



Napr. prenosový digitálny okruh E1:

32 PCM kanálov o rýchlosti 64kb/s

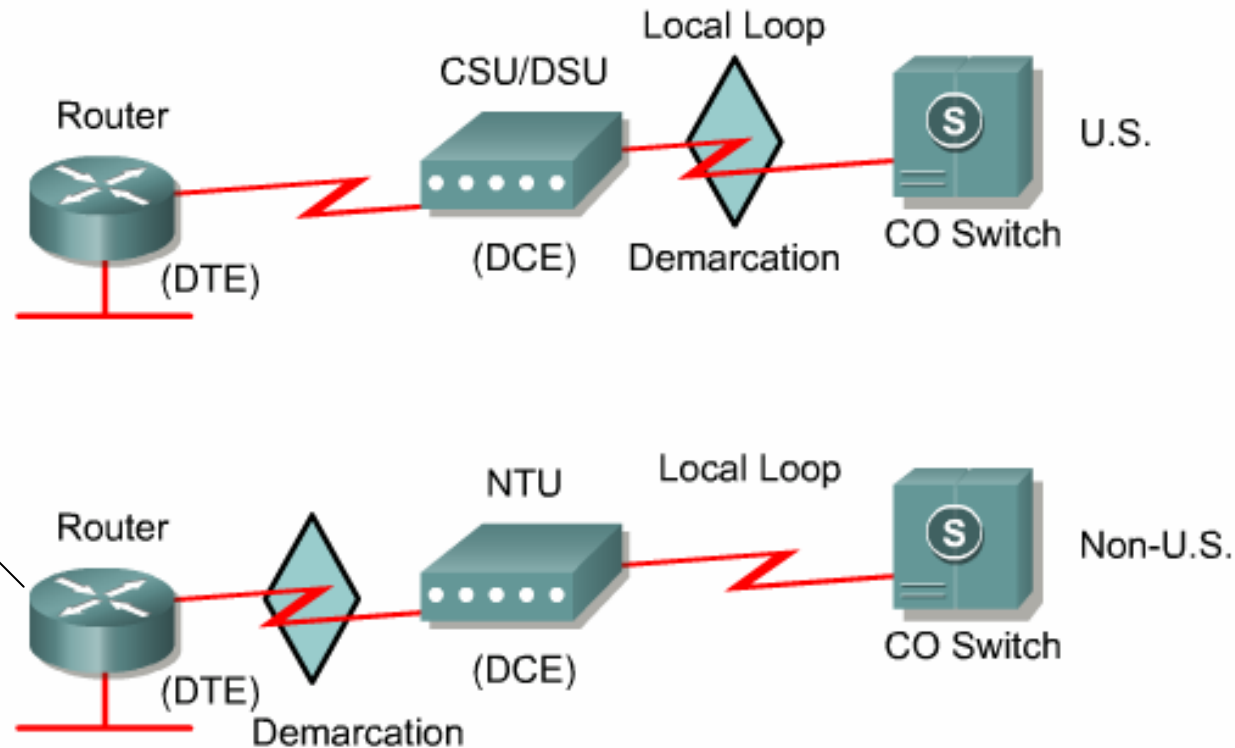
Výsledná rýchlosť: 2,048Mb/s



1. Kanál (spojenie)

64kbps

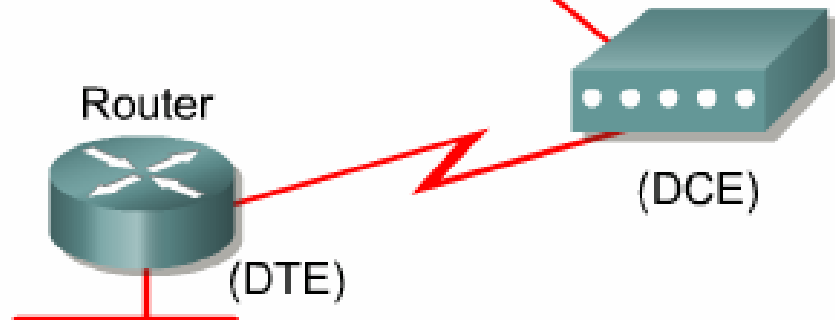
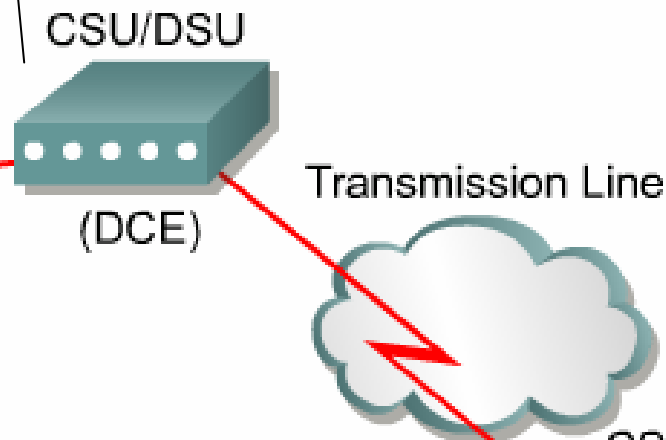
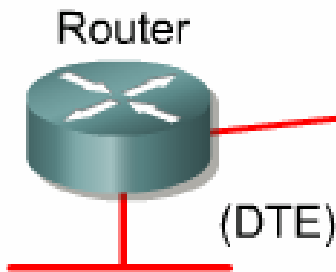
# Demarcation Point (Demarc)



**The point in the network where the responsibility of the service provider or "telco" ends.**

# DTE-DCE

•Source of a clocking signal



A serial connection has:

- DTE (Digital Terminal Equip.)
  - router, terminal, computer, printer, or fax machine
- DCE (Data Circuit Equip.)
  - modem or CSU/DSU
  - the device used to convert the user data from the DTE into a form acceptable to the WAN service provider transmission link.



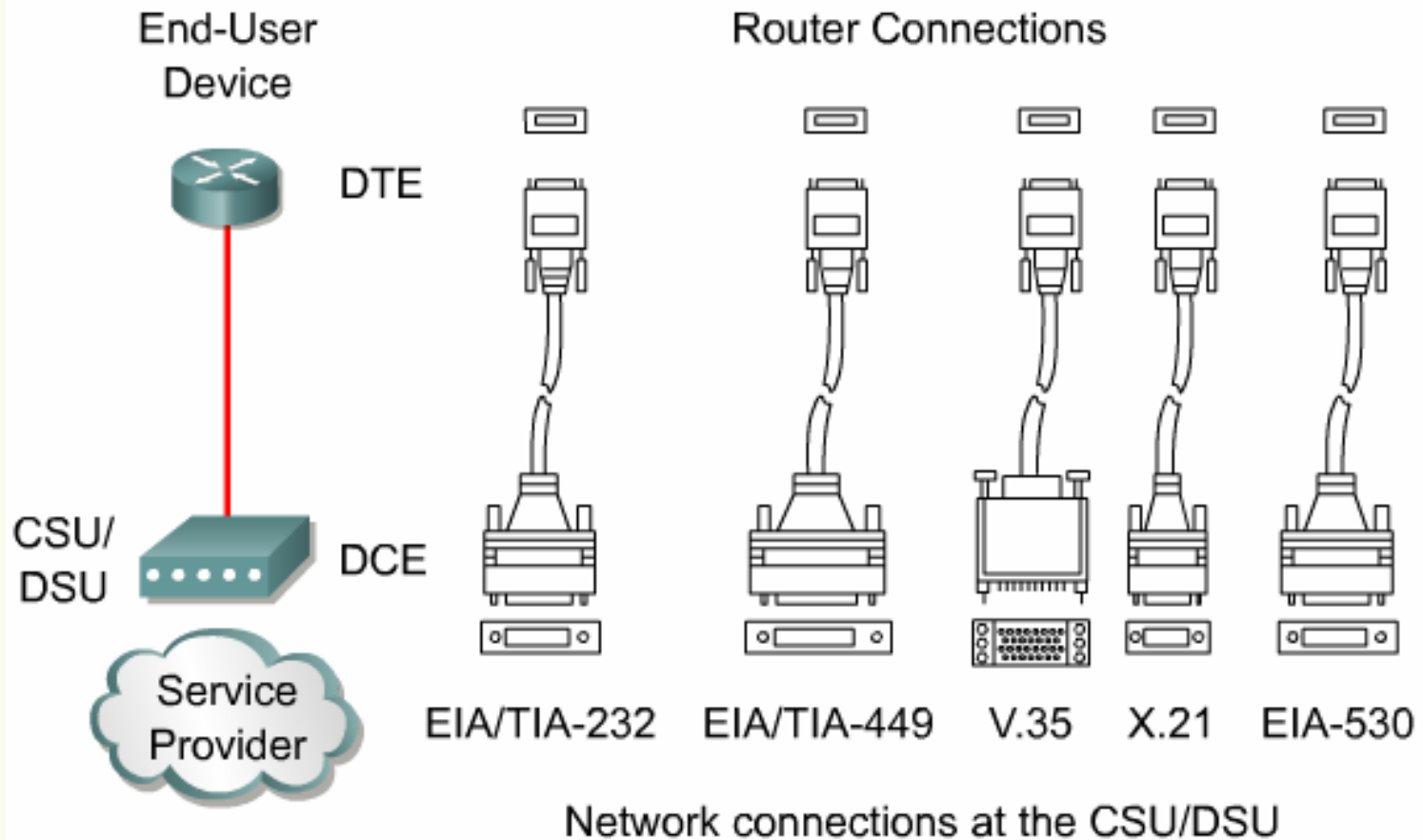
# DTE-DCE interface

- Communication standards by:
  - The Electronics Industry Association (EIA)
  - International Telecommunication Union Telecommunications Standardization Sector (ITU-T)
- The DTE/DCE interface for a particular standard defines the following specifications:
  - **Mechanical/physical** - Number of pins and connector type
  - **Electrical** - Defines voltage levels for 0 and 1
  - **Functional** - Specifies the functions that are performed by assigning meanings to each of the signaling lines in the interface
  - **Procedural** - Specifies the sequence of events for transmitting data

# DTE-DCE

- Synchronne sériové linky musia mať clock
  - Zvyčajne dodáva DCE zariadenie
- Ak prepájam dve DTE zariadenia (napr. routre v labe) cez synchronne rozhranie
  - Jeden musí byť zdrojom taktu
  - Default je router DTE zariadenie
  - Musím zmeniť konfiguráciou na DCE
    - Podľa typu pripojeného kábla
    - `Clock-rate 64000`

# Serial Connection Options



# Data link layer communication through serial lines

- Several data link communication protocols
  - HDLC, PPP, etc.
- **High-level data link control (HDLC) protocol**
  - Bit-oriented data link layer protocol
  - Point-to-point protocol
  - Define how to encapsulates data on synchronous serial data links
  - It allows flow control and error control through the use of acknowledgments and a windowing scheme

# HDLC

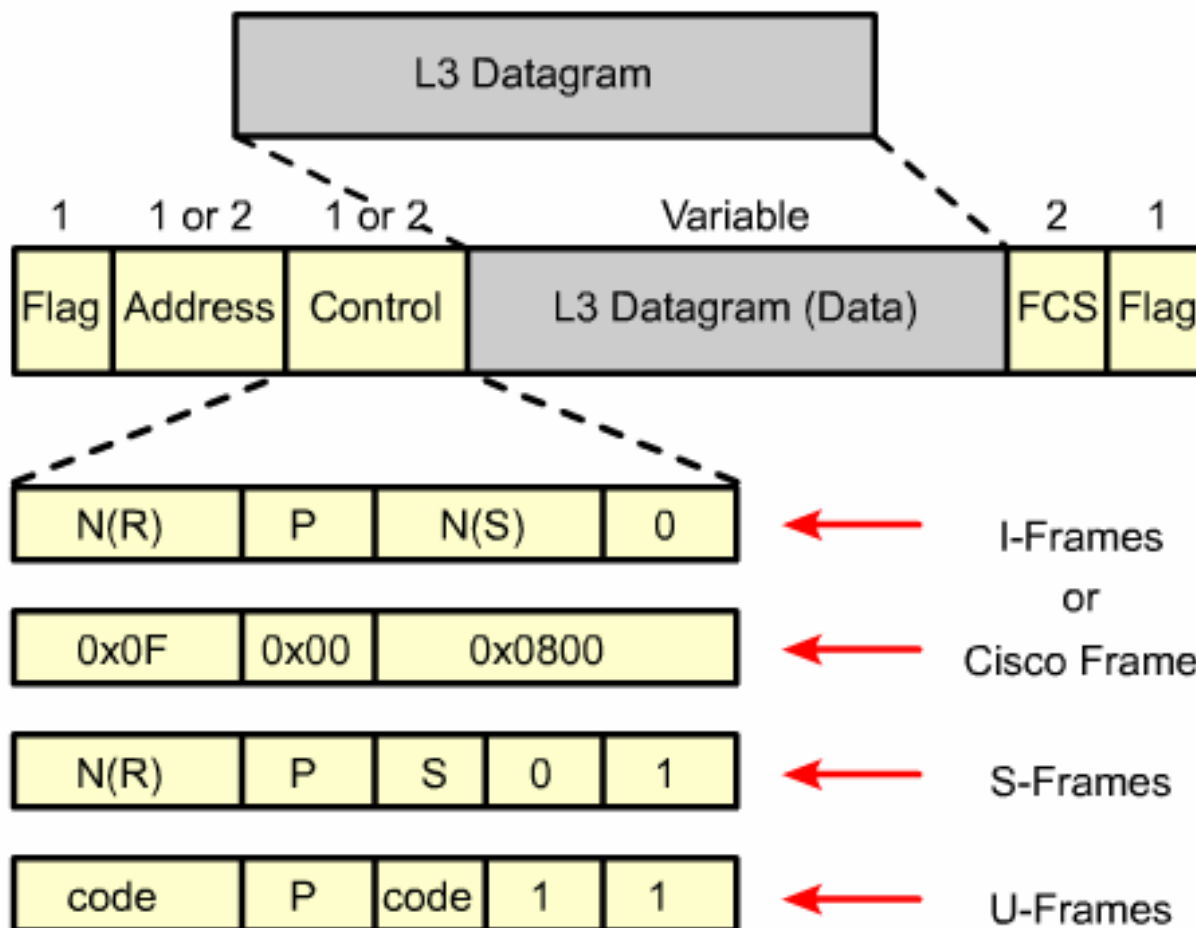
## ■ Standard HDLC

- Does not support multiple L3 protocols on a single link,
  - it does not know how to indicate which protocol is carried

## ■ Cisco

- Offers a proprietary version of HDLC.
- Frame is using a proprietary 'type' field that acts as a protocol field.
- The field enables multiple network layer protocols to share the same serial link.
- Cisco version of HDLC is the default Layer 2 protocol for Cisco router serial interfaces.

# HDLC Frame types



- **Information frames (I-frames)** – Carry the data to be transmitted for the station. Additional flow and error control data may be carried on an I-frame.

- **Supervisory frames (S-frames)** – Provide a request and response mechanisms when piggybacking is not used.

- **Unnumbered frames (U-frames)** – Provide supplemental link control functions such as connection setup. The code field identifies the U-frame type.

# Configuring HDLC Encapsulation

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

- Enable HDLC encapsulation
- HDLC is the default encapsulation on synchronous serial interfaces

# Troubleshooting a Serial Interface

```
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)
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 5762 drops; input queue 0/75, 301
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    38021 packets input, 5656110 bytes, 0 no buffer
    Received 23488 broadcasts, 0 runts, 0 giants, 0
```



# Troubleshooting a Serial Interface

- Five possible problem states can be identified in the interface status line of the `show interface serial` display:
  - Serial x is down, line protocol is down.
  - Serial x is up, line protocol is down.
  - Serial x is up, line protocol is up (looped).
  - Serial x is up, line protocol is down (disabled).
  - Serial x is administratively down, line protocol is down.

# show interface serial

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	<p>The router is not sensing a CD signal, which means the CD is not active.</p> <p>A WAN carrier service provider problem has occurred, which means the line is down or is not connected to CSU/DSU.</p> <p>Cabling is faulty or incorrect.</p> <p>Hardware failure has occurred (CSU/DSU).</p>	<p>1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal.</p> <p>2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation.</p> <p>3. Insert a breakout box and check all control leads.</p> <p>4. Contact the leased-line or other carrier service to see whether there is a problem.</p> <p>5. Swap faulty parts.</p> <p>6. If faulty router hardware is suspected, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.</p>

# show interface serial

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (DTE mode)	A local or remote router is misconfigured.	<ol style="list-style-type: none"><li>1. Put the modem, CSU, or DSU in local loopback mode and use the <b>show interfaces serial</b> command to determine whether the line protocol comes up. If the line protocol comes up, a WAN carrier service provider problem or a failed remote router is the</li><li>2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU.</li><li>3. Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct WAN carrier service provider network termination point. Use the <b>show controllers exec</b> command to determine which cable is attached to which interface.</li><li>4. Enable the debug <b>serial interface exec</b> command.</li><li>5. If the line protocol does not come up in local loopback mode, and if the output of the <b>debug serial interface exec</b> command shows</li></ol>
	Keepalives are not being sent by the remote router.	
	A leased-line or other carrier service problem has occurred, which means a noisy line or misconfigured or failed switch.	
	A timing problem has occurred on the cable, which means serial clock transmit external (SCTE) is not set on CSU/DSU. SCTE is designed to	

# show interface serial

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (DCE mode)	<p>The clockrate interface configuration command is missing.</p> <p>The DTE device does not support or is not set up for SCTE mode (terminal timing).</p> <p>The remote CSU or DSU has failed.</p>	<p>1. Add the clockrate interface configuration command on the serial interface.</p> <p>Syntax: <b>clockrate</b> <i>bps</i></p> <p>Syntax Description: bps - Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000</p> <p>2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU.</p> <p>3. Verify that the correct cable is being used.</p> <p>4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads.</p> <p>5. Replace faulty parts as necessary.</p>

# show interface serial

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (disabled)	A high error rate has occurred due to a WAN service provider problem.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals.
	A CSU or DSU hardware problem has occurred.	2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a WAN service provider problem.
	Router hardware (interface) is bad.	3. Swap out bad hardware as required (CSU, DSU, switch, local or remote router).

# show interface serial

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up (looped)	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	<ol style="list-style-type: none"><li>1. Use the <code>show running-config</code> privileged exec command to look for any <code>loopback</code> interface configuration command entries.</li><li>2. If there is a <code>loopback</code> interface configuration command entry, use the <code>no loopback</code> interface configuration command to remove the loop.</li><li>3. If there are no conflicting loopback interfaces configured, then physically examine the CSU/DSU to determine whether it can be manually set to loopback mode. If it has, then disable manual loopback.</li><li>4. After disabling loopback mode on the CSU/DSU, reset the CSU/DSU, and inspect the line status. If the line protocol comes up, no other action is needed.</li><li>5. If upon inspection, that the CSU or DSU cannot be manually set, then contact the leased-line or other carrier service for line troubleshooting assistance.</li></ol>

# show interface serial

Serial x is administratively down, line protocol is down

The router configuration includes the shutdown interface configuration command.

A duplicate IP address exists.

1. Check the router configuration for the **shutdown** command.

2. Use the **no shutdown interface configuration** command to remove the **shutdown** command.

3. Verify that there are no identical IP addresses using the **show running-config** privileged exec command or the **show interfaces exec** command.

4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.



# Sh controllers INT INT\_ID

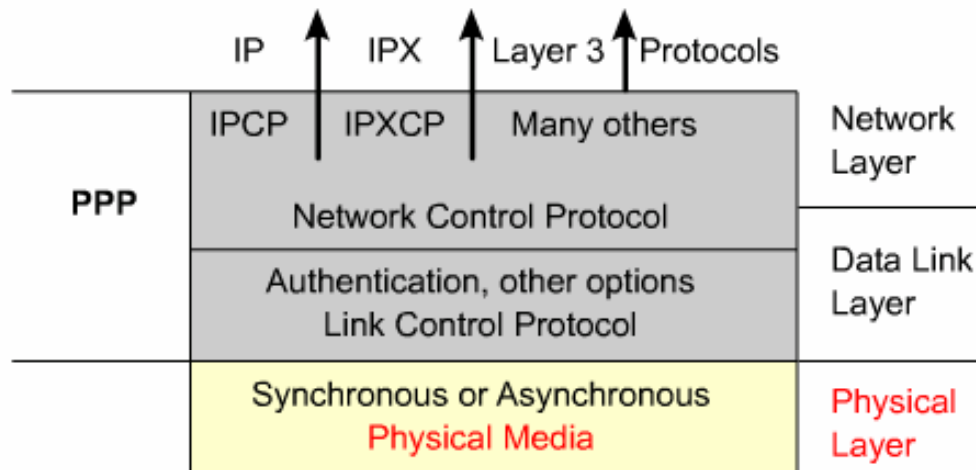
```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific
[PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```



# PPP protocol



# PPP Layered Architecture – Physical Layer

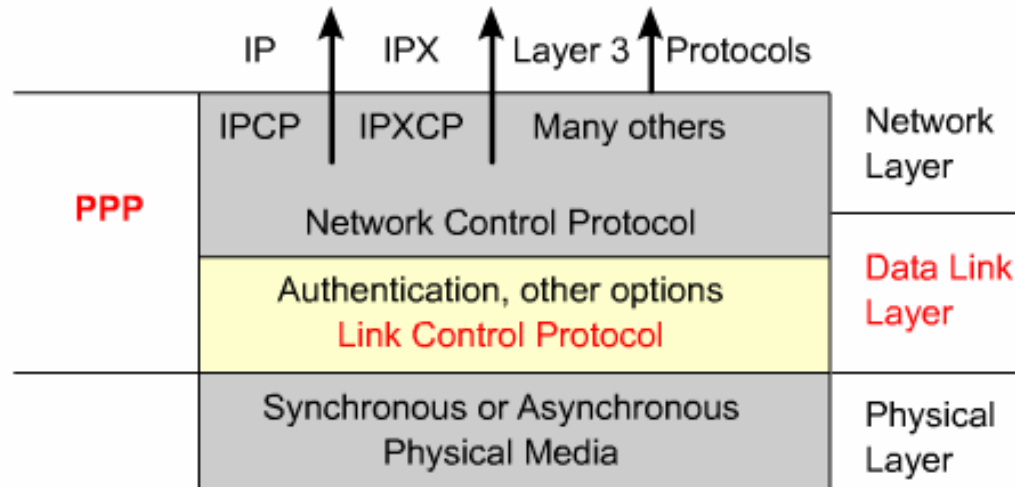


- PPP can be configured on:
  - Asynchronous serial
  - Synchronous serial
  - High-Speed Serial Interface (HSSI)
  - Integrated Services Digital Network (ISDN)

With its lower-level functions, PPP can use:

- Synchronous physical media
- Asynchronous physical media like those that use basic telephone service for modem dialup connections.

# PPP and the Data Link Layer - LCP



## ■ LCP

- Sits on top of the physical layer
- Is used to establish, configure, and test the data-link connection

- PPP offers a rich set of services that control setting up a data link.
- These services are options in LCP and are primarily negotiation and checking frames to implement the point-to-point controls an administrator specifies for the call.

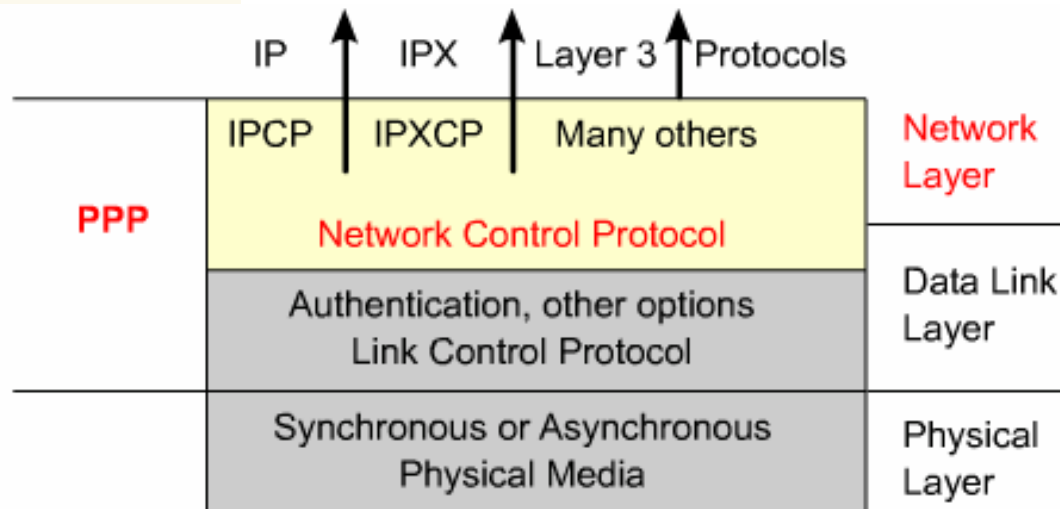
# PPP and the Data Link Layer - LCP

- LCP other functions
  - **Authentication**
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP).
  - **Compression**
    - increase the effective throughput on PPP connections The protocol decompresses the frame at its destination.
    - Two compression protocols available in Cisco routers:
      - Stacker
      - Predictor.
  - **Error detection**
    - Allow to identify fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link.
  - **Multilink**
  - **PPP Callback**
    - Cisco router can act as a callback client or as a callback server.
    - The client makes the initial call, requests that it be called back, and terminates its initial call.
    - The callback router answers the initial call and makes the return call to the client based on its configuration statements.

# PPP and the Data Link Layer - LCP

- LCP other functions
  - Handle varying limits on packet size
  - Detect common misconfiguration errors
  - Terminate the link
  - Determine when a link is functioning properly or when it is failing

# PPP and the Network Layer - NCP



■ Allows to use multiple L3 protocols

- With its higher-level functions, PPP carries packets from several network-layer protocols in NCPs.
- These are functional fields containing standardized codes to indicate the network-layer protocol type that PPP encapsulates.

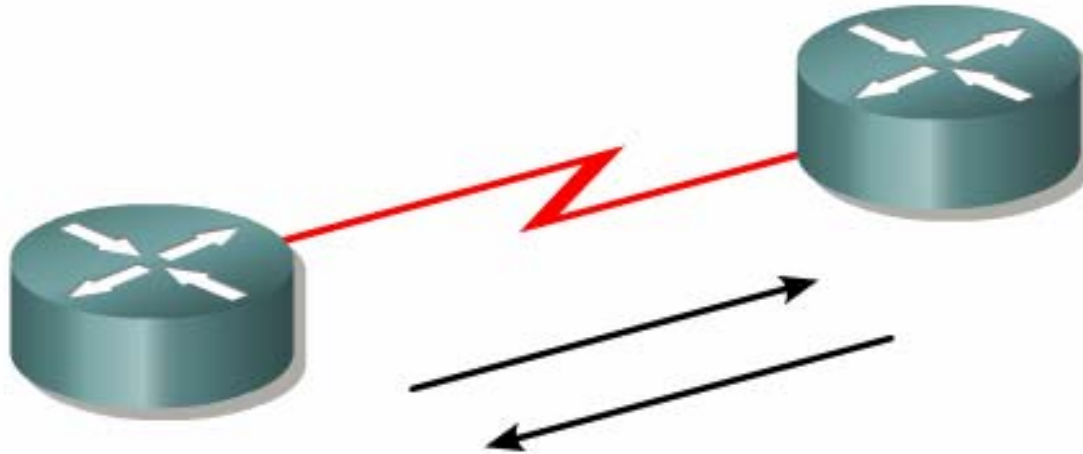
# PPP frame

# Establishing a PPP Session - Phases

- The three PPP session establishment phases are:
  - **Link-establishment phase**
    - LCP is used to configure and test the data link.
    - LCP frames contain a configuration option which allows devices to negotiate the use of options such as the maximum transmission unit (MTU), compression of certain PPP fields, and the link-authentication protocol.
    - This phase is complete when a configuration acknowledgment frame has been sent and received.
  - **Authentication phase (optional)**
    - It takes place before the network layer protocol phase is entered.
    - Optionaly link-quality determination test is made.
    - The link is tested to determine whether the link quality is good enough to bring up network layer protocols.
  - **Network layer protocol phase**
    - NCP is used to choose and configure one or more network layer protocols, such as IP, IPX, etc.



# PPP Operation



## LCP

- LCP listen
- Option negotiation
- Link Quality is determined (optional)
- Network layer configuration begins (IPCP, IPXCP, ATCP)
- Link establishment (LCP Open)
- LCP termination

# PPP Configuration Options

Features	How It Operates	Protocol
Authentication	Require a password and Perform Challenge Handshake	PAP CHAP
Compression	Compress data at source; 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)

Cisco routers that use PPP encapsulation may include the LCP options shown in this table.

# Network Control Protocol



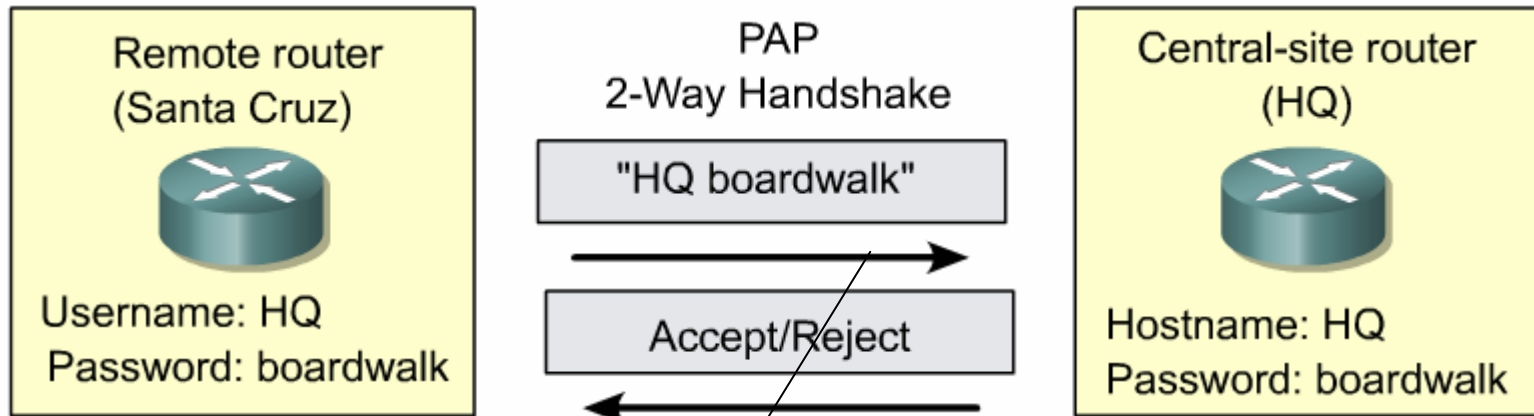
## NCP Characteristics:

- Responsible for configuring enabling and disabling the L3 protocol.
- Uses L2 protocol field 0x8021 to identify the payload as IPCP
- Address Assignment (DHCP)
- NetBios Name Servers
- Domain Name System

# PPP authentication

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

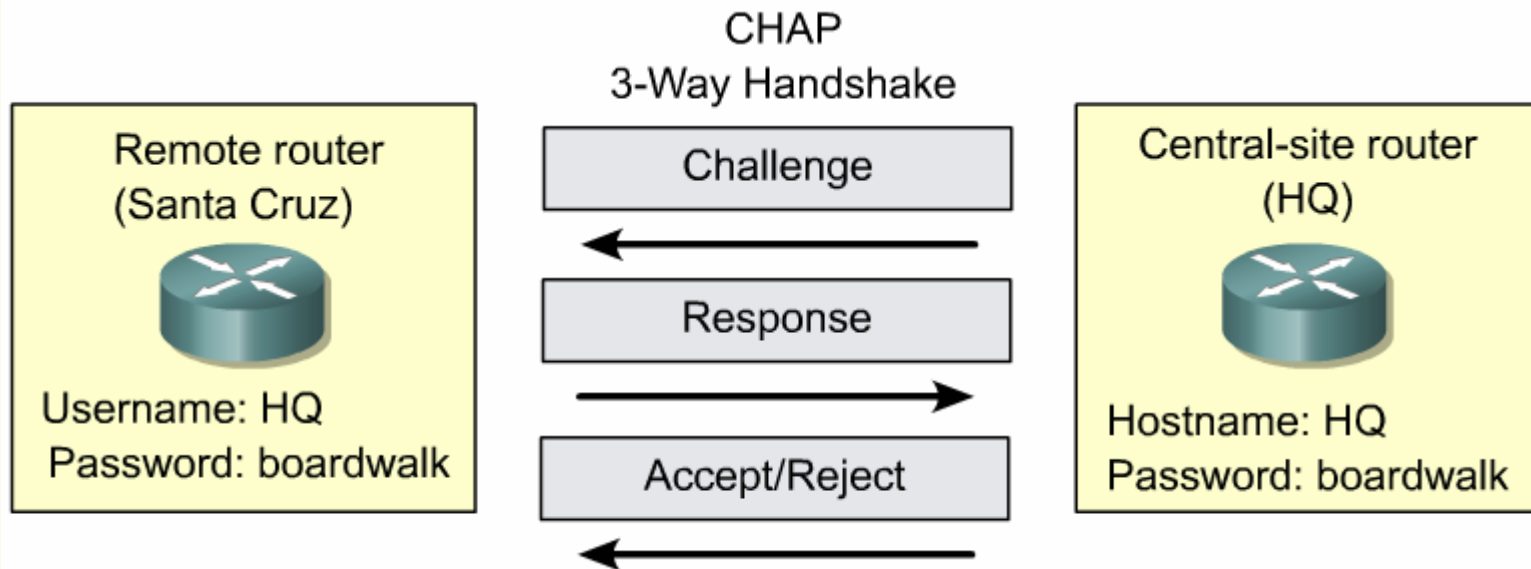
# Password Authentication Protocol (PAP)



- Passwords sent in clear text
- Peer in control of attempts

- Heslo posielané ako text
- Opakovane posielané až kým druhá strana nepotvrdí = **PROBLÉM (trial-and-error attacks)**

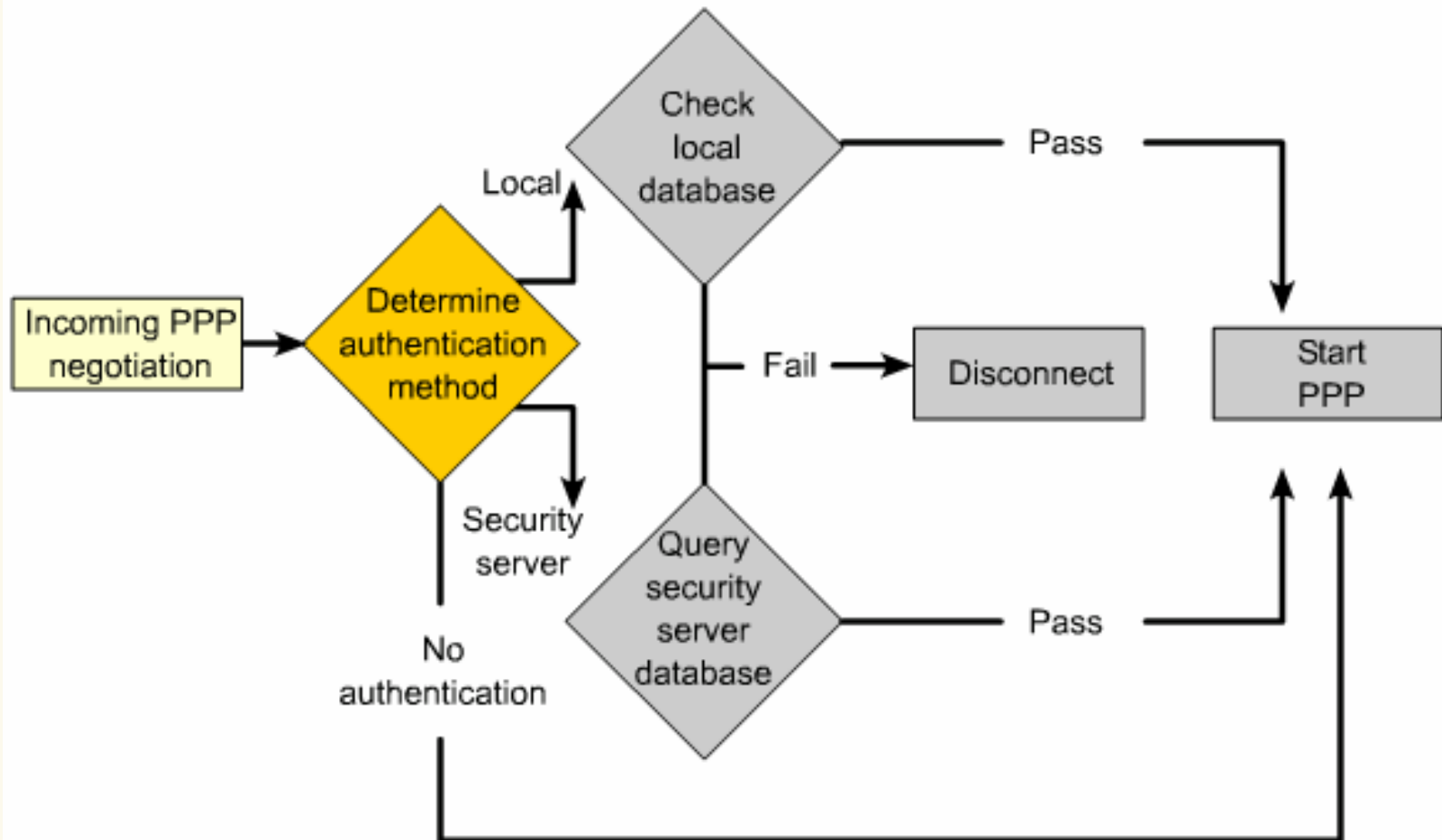
# Challenge Handshake Authentication Protocol (CHAP)



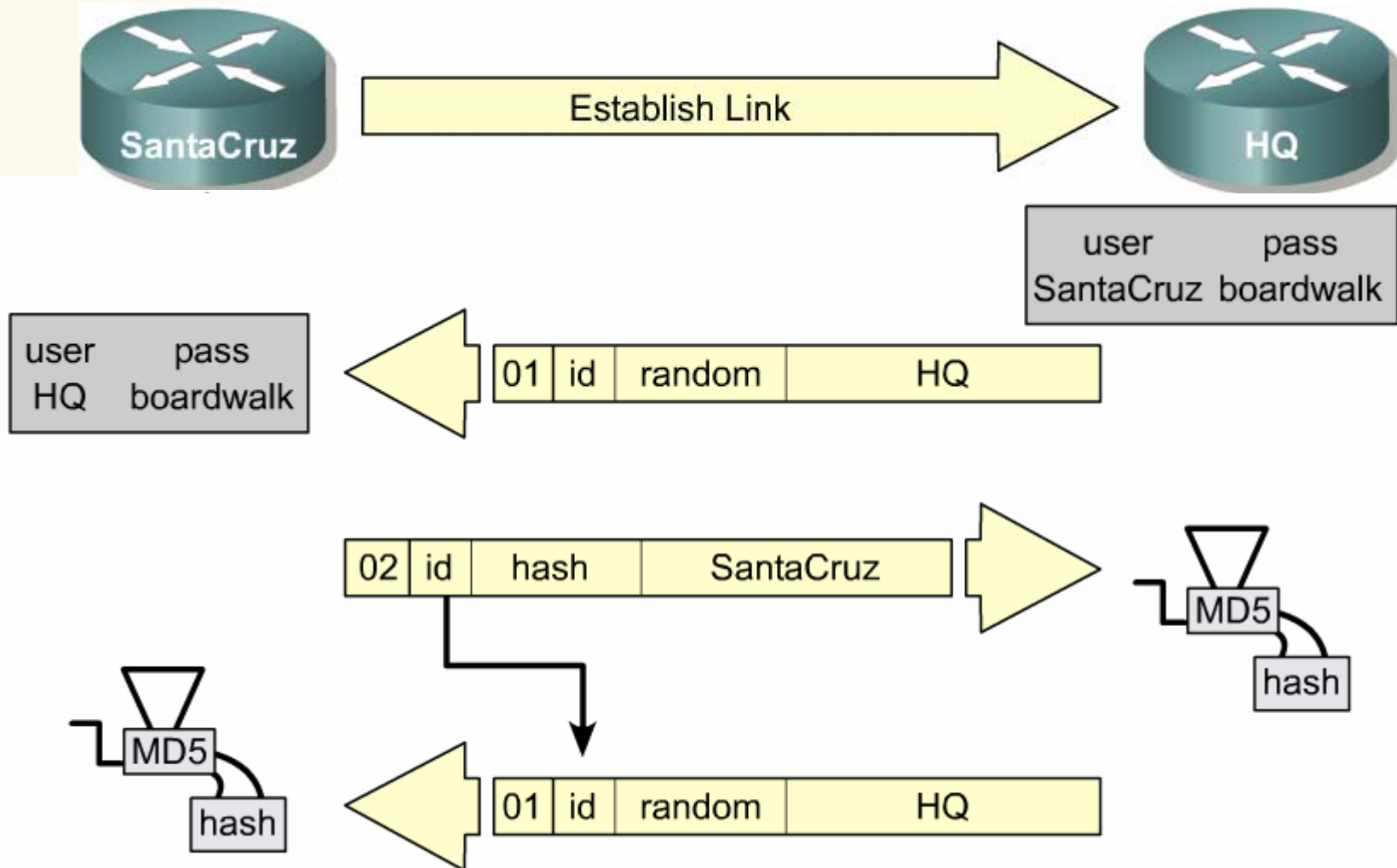
Uses a secret password known only to authenticator and peer.

- CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable
- password is not send

# PPP Encapsulation and Authentication Process



# CHAP Authentication Process





# Configuring PPP

Router#**configure terminal**

Router(config)#**interface serial 0/0**

Router(config-if)#**encapsulation ppp**

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

Keyword	Description
<i>Predictor</i>	(Optional) Specifies that a predictor compression algorithm will be used.
<i>Stac</i>	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used.

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

Keyword	Description
<i>Percentage</i>	Specifies the link quality threshold. Range is 1 to 100.

# Configuring PPP Authentication



## Enabling PPP

- ☒ ppp encapsulation

## Enabling PPP Authentication

- ☒ hostname
- ☒ username/password
- ☒ ppp authentication

## Enabling PPP

- ☒ ppp encapsulation

## Enabling PPP Authentication

- ☒ hostname
- ☒ username/password
- ☒ ppp authentication

# PAP Configuration



```
hostname Left
username Right password
sameone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication PAP
ppp pap sent-username
Left
password sameone
```

```
hostname Right
username Left password
sameone
!
int serial 0/0
ip address 128.0.1.2
255.255.255.0
encapsulation ppp
ppp authentication PAP
ppp pap sent-username
Right
password sameone
```

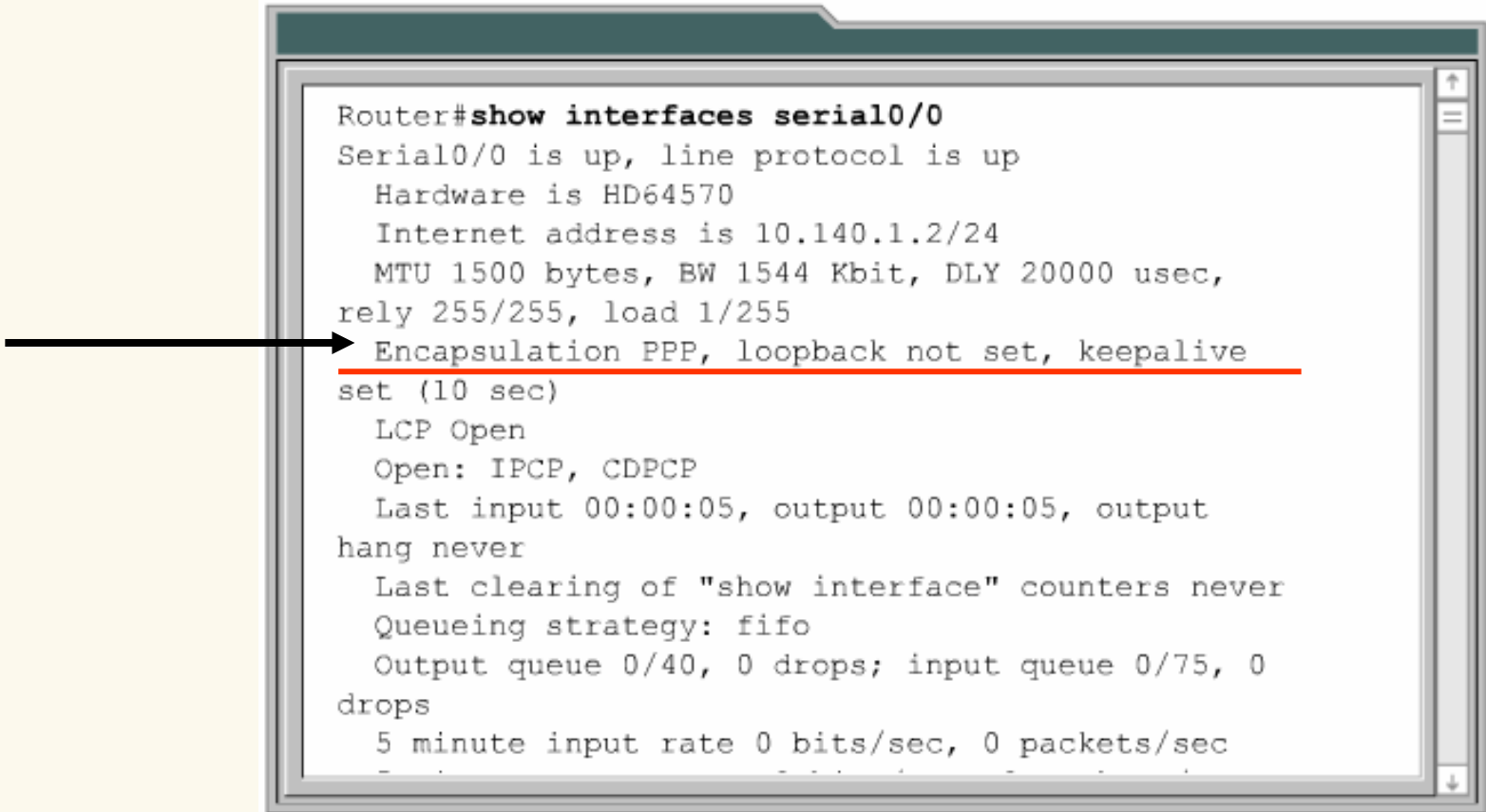
# CHAP Configuration



```
hostname Left
username Right password
someone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

```
hostname Right
username Left password
someone
!
int serial 0/0
ip address 128.0.1.2
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
  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
  Output queue 0/40, 0 drops; input queue 0/75, 0
  drops
  5 minute input rate 0 bits/sec, 0 packets/sec
```

# PPP Configuration Commands

Command	Description
<code>encapsulation ppp</code>	Enables PPP on an interface
<code>ppp authentication pap</code>	Enables PAP authentication on an interface
<code>ppp authentication chap</code>	Enables CHAP authentication on an interface
<code>username <i>username</i></code> <code>password <i>password</i></code>	Establishes a username-based authentication system
<code>show interfaces</code>	Displays statistics for all interfaces configured on the router or access server
<code>debug ppp</code> <code>authentication</code>	Debugs the PAP or CHAP authentication process
<code>undebug all</code>	Turns off all debugging displays

# 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

Command	Description
<b>packet</b>	Used with the <b>debug ppp</b> command to display PPP packets being sent and received
<b>negotiation</b>	Used with the <b>debug ppp</b> command to display PPP packets transmitted during PPP startup, where PPP options are negotiated
<b>error</b>	Used with the <b>debug ppp</b> command to display protocol errors and error statistics associated with PPP connection negotiation and operation
<b>chap</b>	Used with the <b>debug ppp</b> command to display Challenge Authentication Protocol (CHAP) packet exchanges