PPP & HDLC
Serial connection
Serial connection
Serial connection

At higher frequencies, crosstalk causes bytes to be dropped.
Smart Serial

Smart Serial Connector
Smart Serial connector
Wan encapsulation protocol

[Diagram showing Wan Encapsulation Protocols, including HDLC, PPP, SLIP, X.25, Frame Relay, ATM, Leased Line, Circuit-Switched, Packet-Switched, Telephone Company, Service Provider]
HDLC

Standard and Cisco HDLC Frame Format

- Supports only single-protocol environments.

Cisco HDLC

- Uses a protocol data field to support multiprotocol environments.
HDLC

Configuring HDLC Encapsulation

Router(config-if)#encapsulation hdlc

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

Troubleshooting a Serial Interface

R1#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 172.16.0.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:03, output 00:00:04, output hang never
Last clearing of "show interface" counters 1w0d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  219 packets input, 15632 bytes, 0 no buffer
  Received 218 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  217 packets output, 14919 bytes, 0 underruns
  0 output errors, 0 collisions, 107 interface resets
  0 output buffer failures, 0 output buffers swapped out
12 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
PPP

What is PPP?

HDLC is the default encapsulation method between Cisco routers.

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

PPP Layered Architecture: Physical Layer

- IP
- IPX
- Layer 3
- Protocols

- IPCP
- IPXCP
- Many others

Network Control Protocol

Authentication, other options
Link Control Protocol

Synchronous or Asynchronous
Physical Media

Network Layer
Data Link Layer
Physical Layer
LCP
NCP
PPP
Establishing a PPP Session

Phase 1 - Link Establishment: "Let’s negotiate."

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

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

The LCP does all the talking.
PPP components

1- Frame Format:

<table>
<thead>
<tr>
<th>Flag</th>
<th>address</th>
<th>control</th>
<th>type</th>
<th>data</th>
<th>FCS</th>
<th>flag</th>
</tr>
</thead>
</table>

2- Link control protocol (LCP):

- It negotiates:
  1. Link establishment → open session
  2. Link management → options
  3. Link termination.

3- Network control protocol (NCP):

Negotiates the upper layer protocols that will be transmitted across the PPP connection.
PPP LCP Features

- Compression
- Multilink PPP
- Call Back
  - Authentication
1- Compression

- To improve the throughput on slower links.
2- Multilink

- B.W aggregation by combining multiple physical interfaces into one link (logically) like load sharing.
- Splitting L3 packets into small parts called fragments and send them over parallel links.
- This can improve throughput and reduce latency between systems.
3- Call back

- Enable a router to place a call and request call back (Like missed calls).
- Once the request is made, the call disconnect and the other router (server) dial the router (client) back.
  - By that way a central site can pay all the bills of the calls with the other sides.
4- 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

PPP Configuration Commands

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictor</td>
<td>(Optional) Specifies that a predictor compression algorithm will be used.</td>
</tr>
<tr>
<td>Stac</td>
<td>(Optional) Specifies that a Stacker (LZS) compression algorithm will be used.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>Specifies the link quality threshold. Range is 1 to 100.</td>
</tr>
</tbody>
</table>
PPP AUTHENTICATION

PPP Authentication Protocols

PAP
2-Way Handshake

Username: R1
Password: cisco123
Accept/Reject

CHAP
3-Way Handshake
Challenge

Username: R1
Password: cisco123
Accept/Reject

Central-site router

Remote Router

Central-site Router

Remote Router
AUTHENTICATION PROCESS
PAP

Initiating PAP

Central-site router

PAP
2-Way Handshake

Remote router

Username: R1
Password: cisco123

Router R1 sends its PAP username and password to router R3.
PAP

Completing PAP

Router R3 evaluates R1's username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.
Router R3 initiates the 3-way handshake and sends a challenge message to router R1.
CHAP

Central-site router

CHAP
3-Way Handshake
Response

Username: R1
Password: cisco123

Remote router

R1 responds to R3's CHAP challenge by sending its CHAP username and password.
CHAP

Router R3 evaluates R1’s username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.
CHAP PROCESS

Example - CHAP Authentication Process

1. Establish Link
CHAP PROCESS

Example - CHAP Authentication Process

Establish Link

01 id random R2

2
CHAP PROCESS

Example - CHAP Authentication Process

Establish Link

R1

R2

user
pass
R2
boardwalk

01 id random R2

MD5
hash
CHAP PROCESS

Example - CHAP Authentication Process

Establish Link

01 | id | random | R2

02 | id | hash | R1

user | pass |
R2 | boardwalk

[Diagram showing the CHAP process with R1 and R2, user and pass, random, and hash values.]
CHAP PROCESS
The `ppp authentication` Command

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default] [callin]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chap</code></td>
<td>Enables CHAP on a serial interface.</td>
</tr>
<tr>
<td><code>pap</code></td>
<td>Enables PAP on a serial interface.</td>
</tr>
<tr>
<td><code>chap pap</code></td>
<td>Enables both CHAP and PAP, and performs CHAP authentication before PAP.</td>
</tr>
<tr>
<td><code>pap chap</code></td>
<td>Enables both CHAP and PAP, and performs PAP authentication before CHAP.</td>
</tr>
<tr>
<td><code>if-needed</code></td>
<td>Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if</td>
</tr>
<tr>
<td></td>
<td>the user has already provided authentication. This option is available only</td>
</tr>
<tr>
<td></td>
<td>on asynchronous interfaces.</td>
</tr>
<tr>
<td><code>list-name</code></td>
<td>Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of</td>
</tr>
<tr>
<td></td>
<td>authentic list name is specified, the system uses the default. Lists are</td>
</tr>
<tr>
<td></td>
<td>created with the <code>aaa authentication</code> <code>ppp</code> command.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Used with AAA/TACACS+. Created with the <code>aaa authentication</code> <code>ppp</code> command.</td>
</tr>
<tr>
<td><code>callin</code></td>
<td>Specifies authentication on incoming (received) calls only.</td>
</tr>
</tbody>
</table>
PAP AUTHENTICATION

A sample PAP configuration.

```
hostname R1
username R3 password sameone
!
int serial 0/0
ip address 128.0.1.1 255.255.255.255
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R1 password sameone

hostname R3
username R1 password sameone
!
int serial 0/0
ip address 128.0.1.2 255.255.255.255
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R3 password sameone
```
CHAP AUTHENTICATION

A sample CHAP configuration.

```
hostname R1
username R3 password sameone
!
int serial 0/0
ip address 128.0.1.1 255.255.255.255
encapsulation ppp
ppp authentication CHAP

hostname R3
username R1 password sameone
!
int serial 0/0
ip address 128.0.1.2 255.255.255.255
encapsulation ppp
ppp authentication CHAP
```
CHAP DEBUG

Troubleshooting a PPP Configuration with Authentication

R2# debug ppp authentication
Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
# show int s0/0.

The status of interface, encapsulation, LCP state, NCP state.

#debug ppp negotiation.

#debug ppp authentication.