Chapter 2: Point-to-Point Connections

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 2

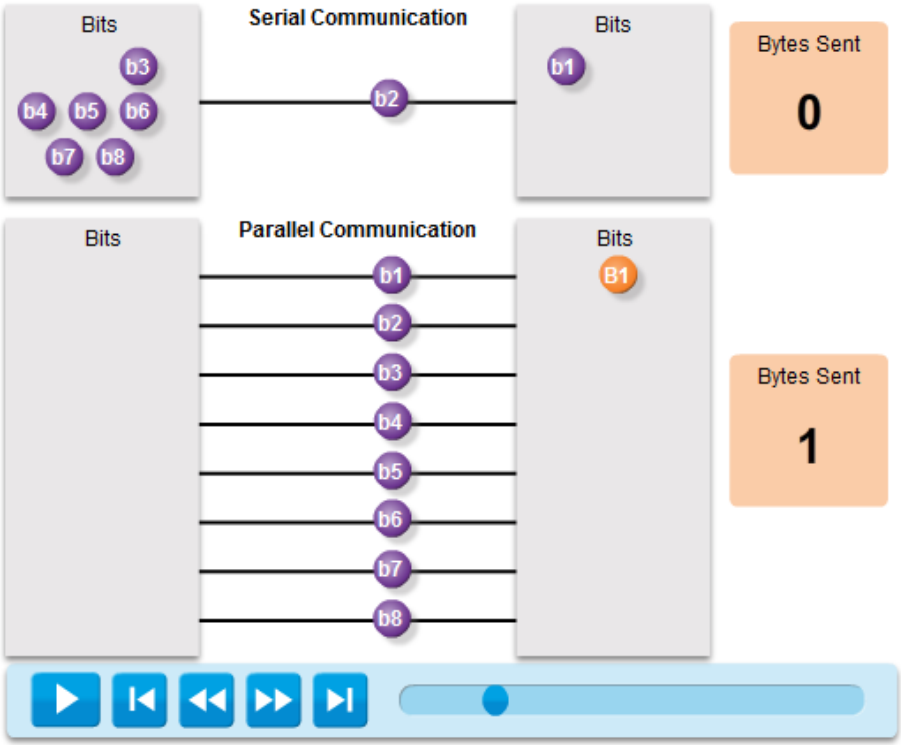
- 2.1 Serial Point-to-Point Overview
  - Configure HDLC encapsulation.
- 2.2 PPP Operation
- 2.3 PPP Implementation
- 2.4 Troubleshoot WAN Connectivity

2.1 Serial Point-to-Point Overview

Cisco | Networking Academy®
Mind Wide Open™

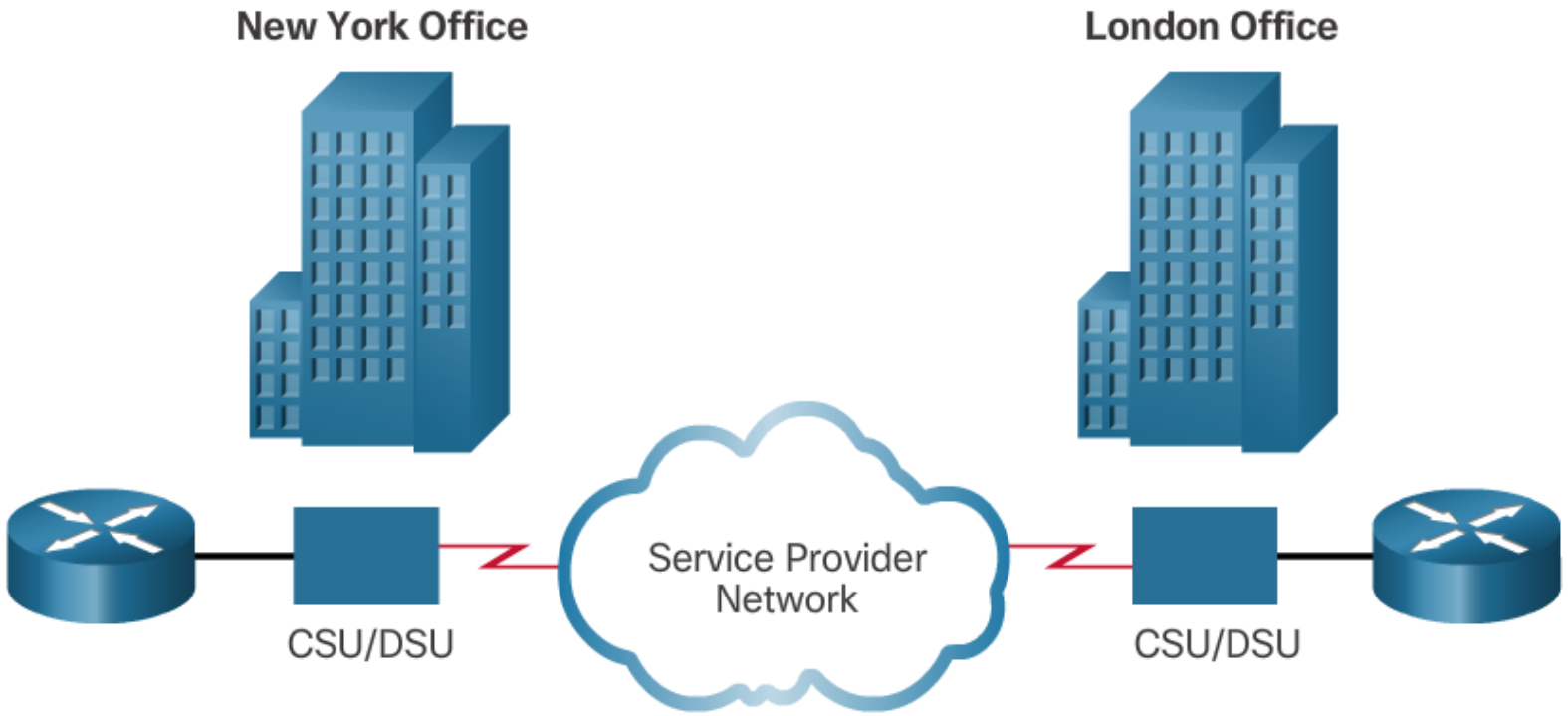
Serial and Parallel Ports

- Point-to-point connections are used to connect LANs to service provider WANs.
  - Also referred to as a serial connection or leased-line connection.
- Serial connection: bits transmitted sequentially over a single channel.
- Parallel communication: bits transmitted simultaneously over multiple wires
  - Cross talks, clock skews over longer distance



Point-to-Point Communications Links

- Point-to-point links can connect two geographically distant sites.
- Carrier dedicates specific resources for a line leased by the customer (leased-line).
- Point-to-point links are usually more expensive than shared services.
- Over fiber-optic cables, ATM lines, dial-up links, etc.



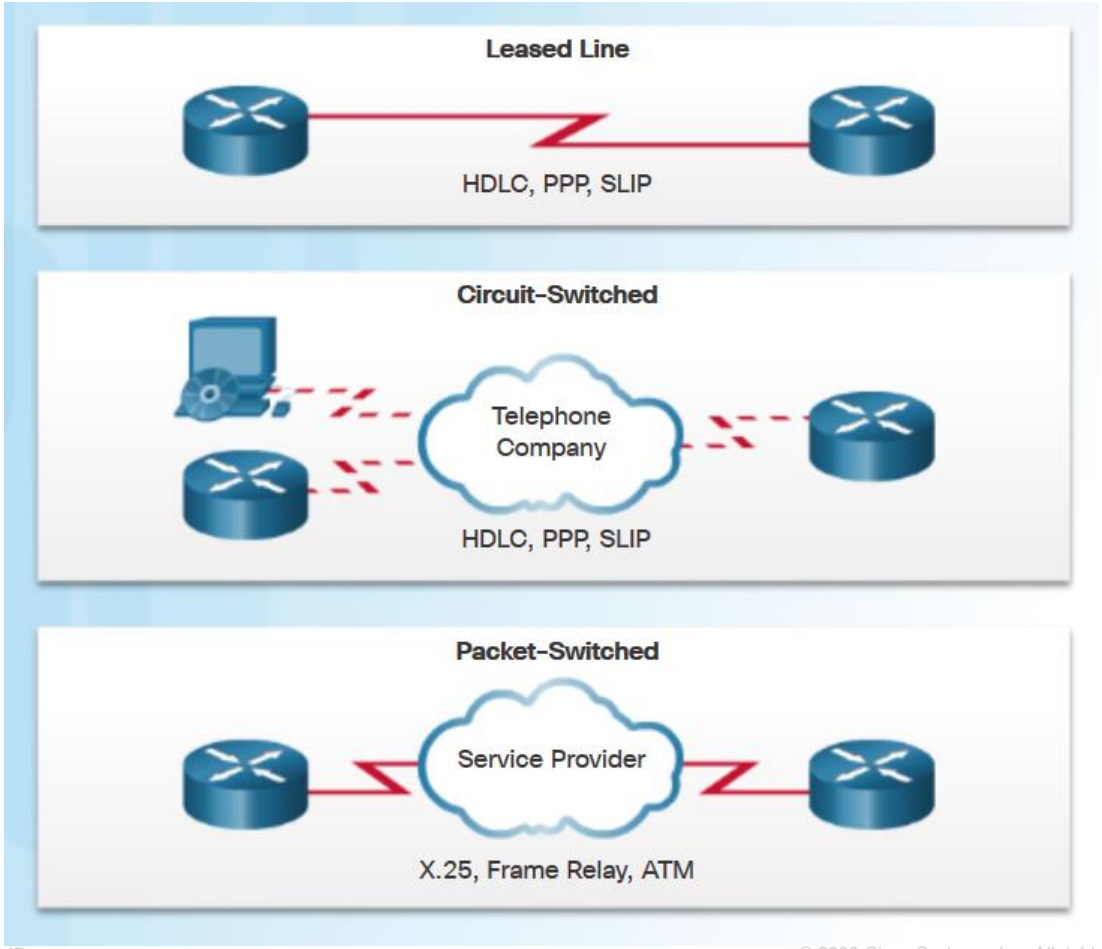
Serial Bandwidth

Bandwidth refers to the rate at which data is transferred over the communication link.

Line Type	Bit Rate Capacity	Line Type	Bit Rate Capacity
56	56 kb/s	OC-9	466.56 Mb/s
64	64 kb/s	OC-12	622.08 Mb/s
T1	1.544 Mb/s	OC-18	933.12 Mb/s
E1	2.048 Mb/s	OC-24	1.244 Gb/s
J1	1.544 Mb/s	OC-36	1.866 Gb/s
E3	34.368 Mb/s	OC-48	2.488 Gb/s
T3	44.736 Mb/s	OC-96	4.976 Gb/s
OC-1	51.84 Mb/s	OC-192	9.954 Gb/s
OC-3	155.52 Mb/s	OC-768	39.813 Gb/s

WAN Encapsulation Protocols

- Data is encapsulated into frames before crossing the WAN link
- An appropriate Layer 2 encapsulation type must be configured.

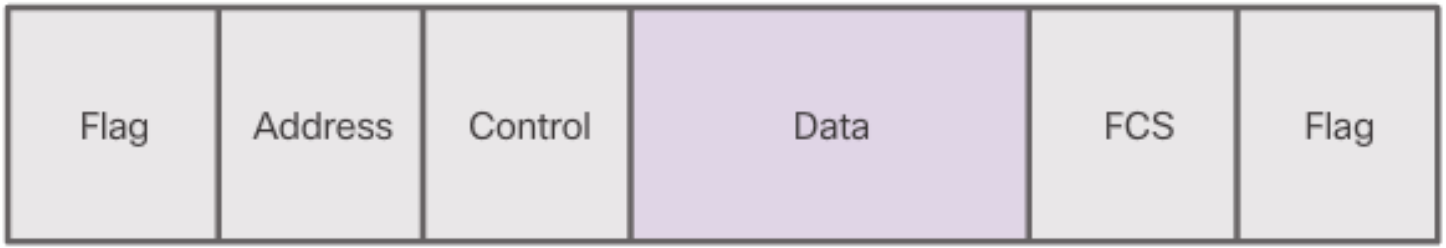


- HDLC
- PPP
- SLIP
- X.25 (LAPB)
- Frame Relay
- ATM

HDLC Encapsulation

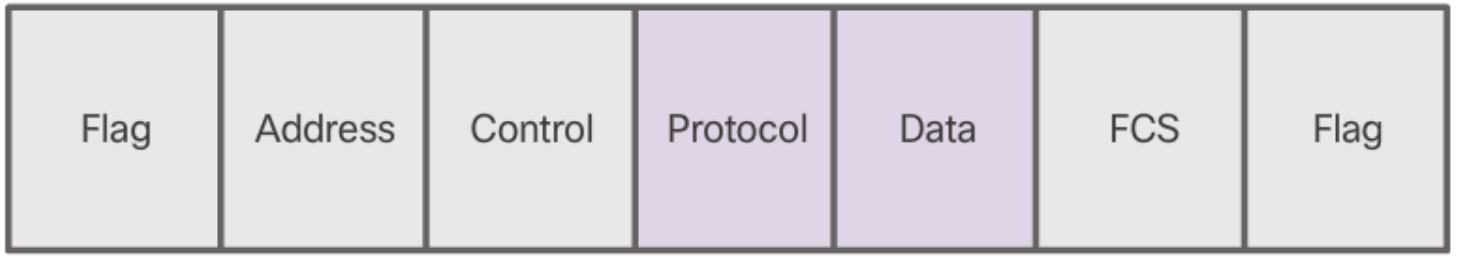
- Bit-oriented, synchronous data link layer protocol developed by the ISO
- Error-free communication between two points
- Flow control and error control through the use of acknowledgments
- Cisco HDLC (cHDLC) provides multiprotocol support

Standard HDLC



Supports only single-protocol environments.

Cisco HDLC



Uses a protocol data field to support multiprotocol environments.

Configuring HDLC Encapsulation

- Default encapsulation method used by Cisco devices on synchronous serial lines
- Point-to-point protocol on leased lines between two Cisco devices
- Connecting to a non-Cisco device, use synchronous PPP

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation hdlc
```

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

Troubleshooting a Serial Interface

```
R1# show interface 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 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:05, output 00:00:04, output hang
  never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
  output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold
  /drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 1017 bytes, 0 no buffer
     Received 5 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun,
         0 ignored, 0 abort
```

show interface s0/0/0

show controllers s0/0/0

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x0000064A,
CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000,
CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x0DBD2DB0, CTDP=0x0DBD31D0, FTDB=0x0DBD31D0
Main Routing Register=0x0003FE38 BRG Conf
Register=0x0005023F
Rx Clk Routing Register=0x76543818 Tx Clk
```

2.2 PPP Operation

Cisco | Networking Academy®
Mind Wide Open™

Introducing PPP

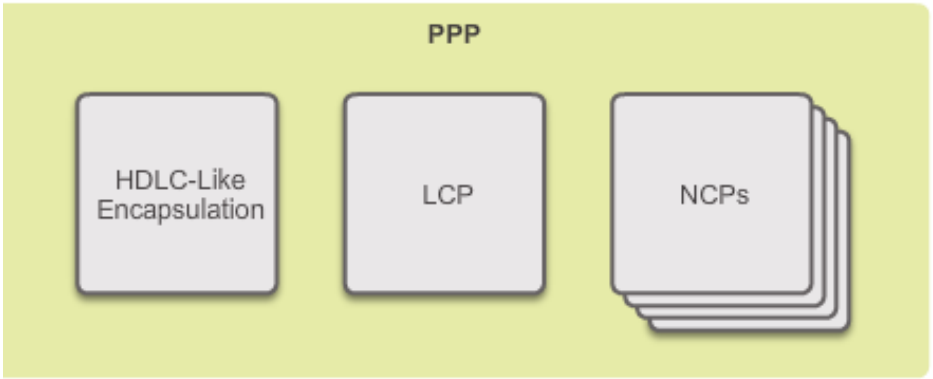
PPP defined by RFC 1661 (1994)

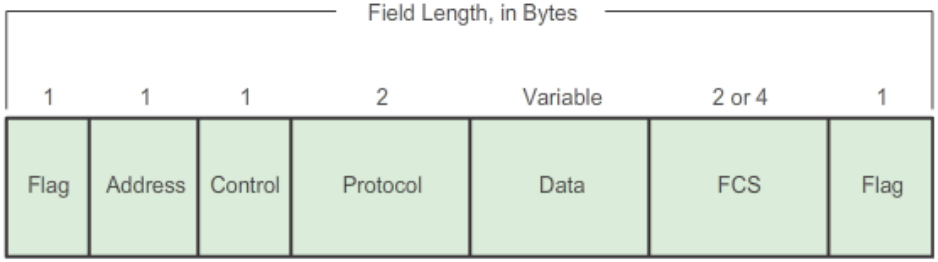
PPP contains 3 main components:

- HDLC-like framing
  - Encapsulating datagrams over point-to-point links
- Link Control Protocol (LCP)
  - Establish, configure, and test the data link connection
- Network Control Protocols (NCPs)
  - Establish and configure different network layer protocols
  - IPv4, IPv6, AppleTalk, Novell IPX, SNA Control Protocol (CP)

HDLC is the default encapsulation method on a serial link.

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



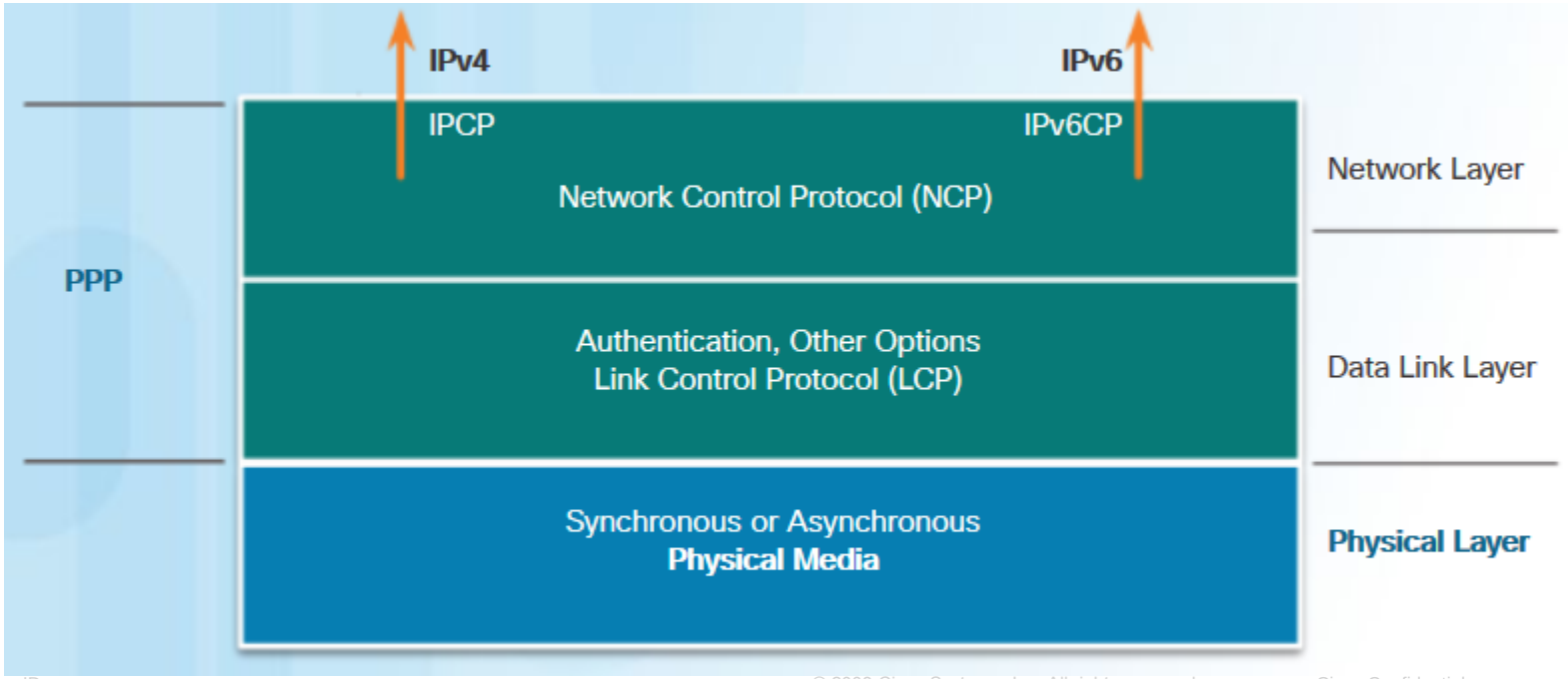


Benefits of PPP

- PPP is not proprietary
- PPP includes several features not available in HDLC:
  - Link quality management feature monitors the quality of the link.
  - Supports PAP and CHAP authentication.

PPP Layered Architecture

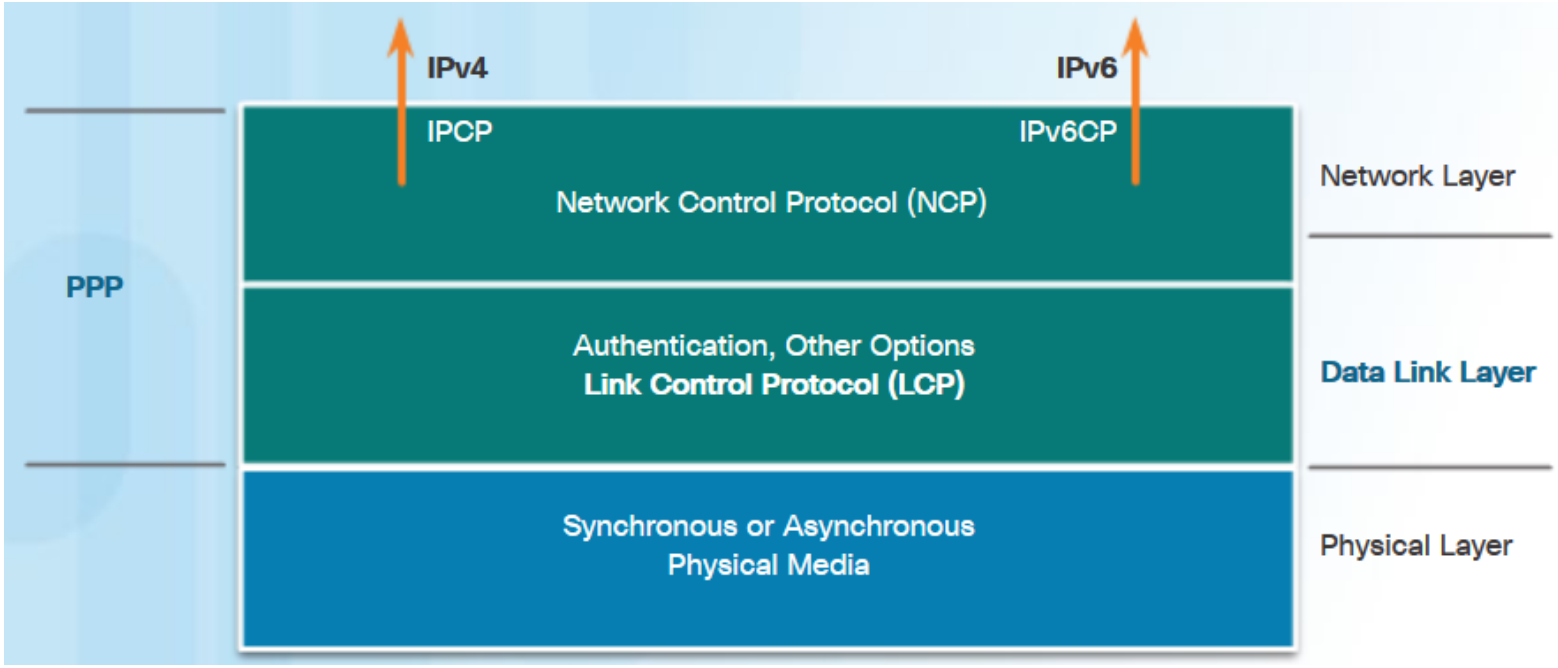
- LCP establishes the PPP connection
- LCP negotiates and sets up control options of the WAN link:
  - Authentication, compression, error detection
- NCP handle higher layer protocol configurations
- LCP terminates the PPP connection
- A the physical layer, PPP supports both synchronous and asynchronous media.



Link Control Protocol (LCP)

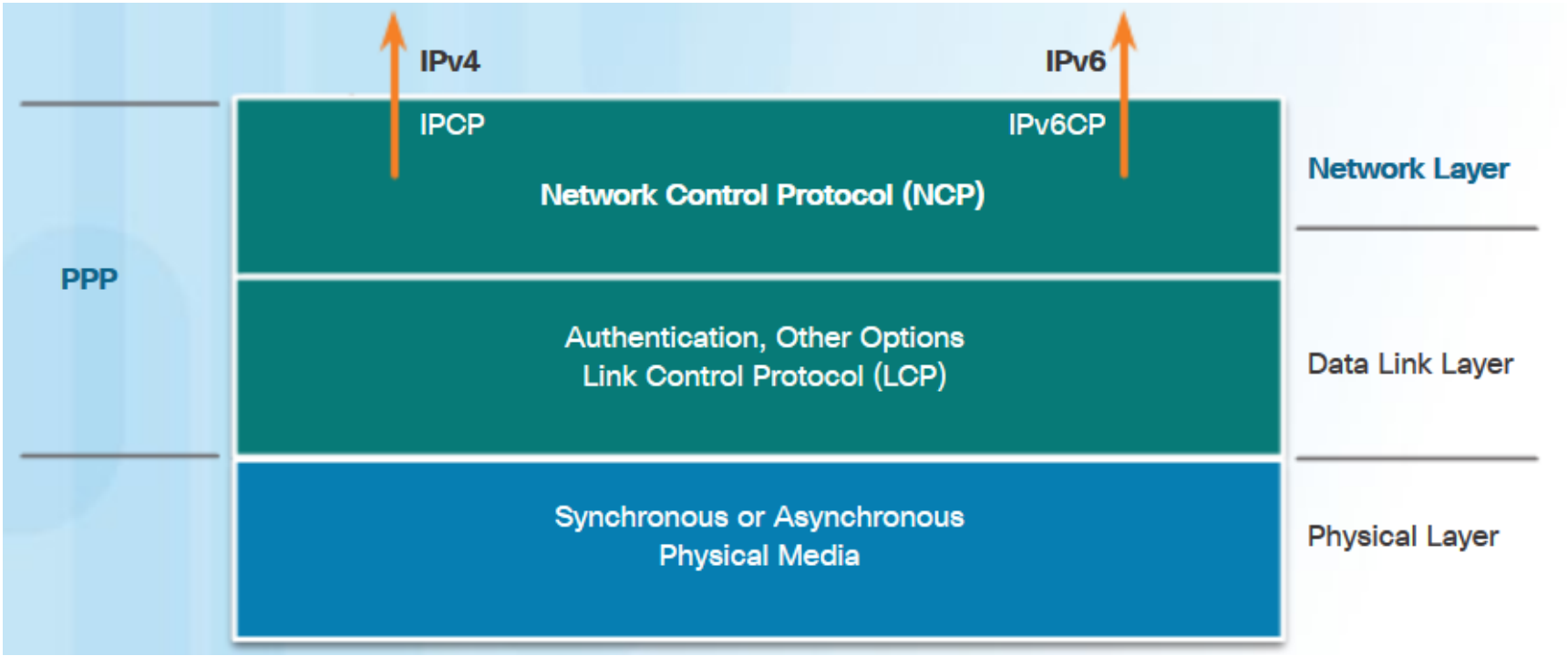
LCP provides automatic configuration of the interfaces at each end, including:

- Handling varying limits on packet size.
- Detecting common misconfiguration errors.
- Terminating the link.
- Determining when a link is functioning properly or when it is failing.



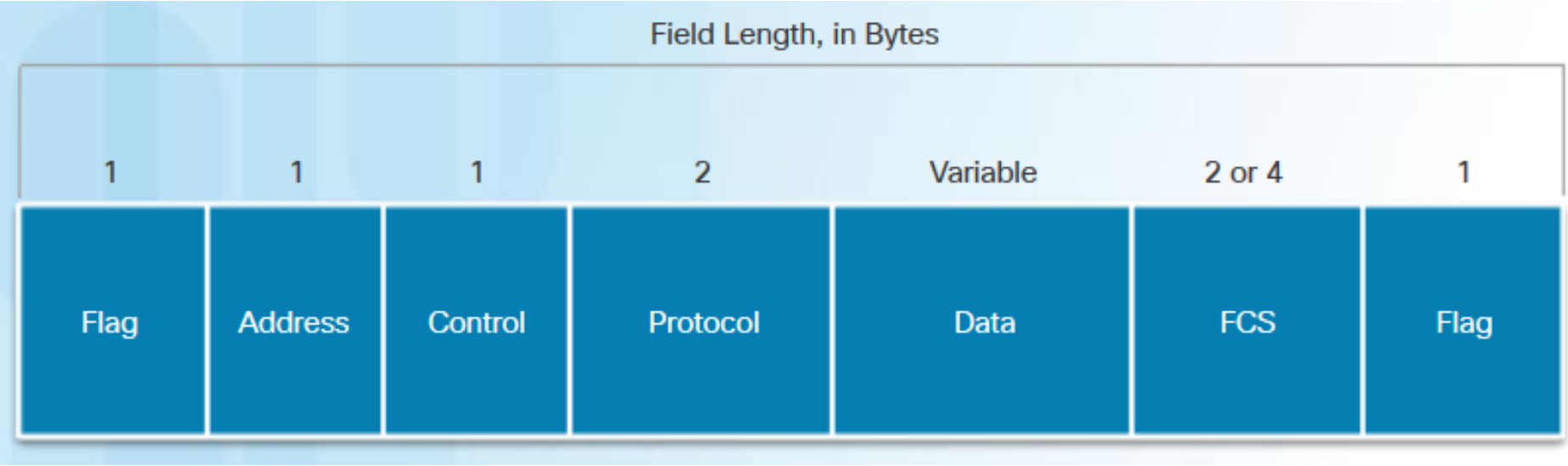
Network Control Protocol (NCP)

- PPP permits multiple network layer protocols to operate on the same communications link.
- For every network layer protocol used, PPP uses a separate NCP:
  - IPv4 CP (IPCP), CPD CP (CDPCP), IPv6 CP (IPv6CP)

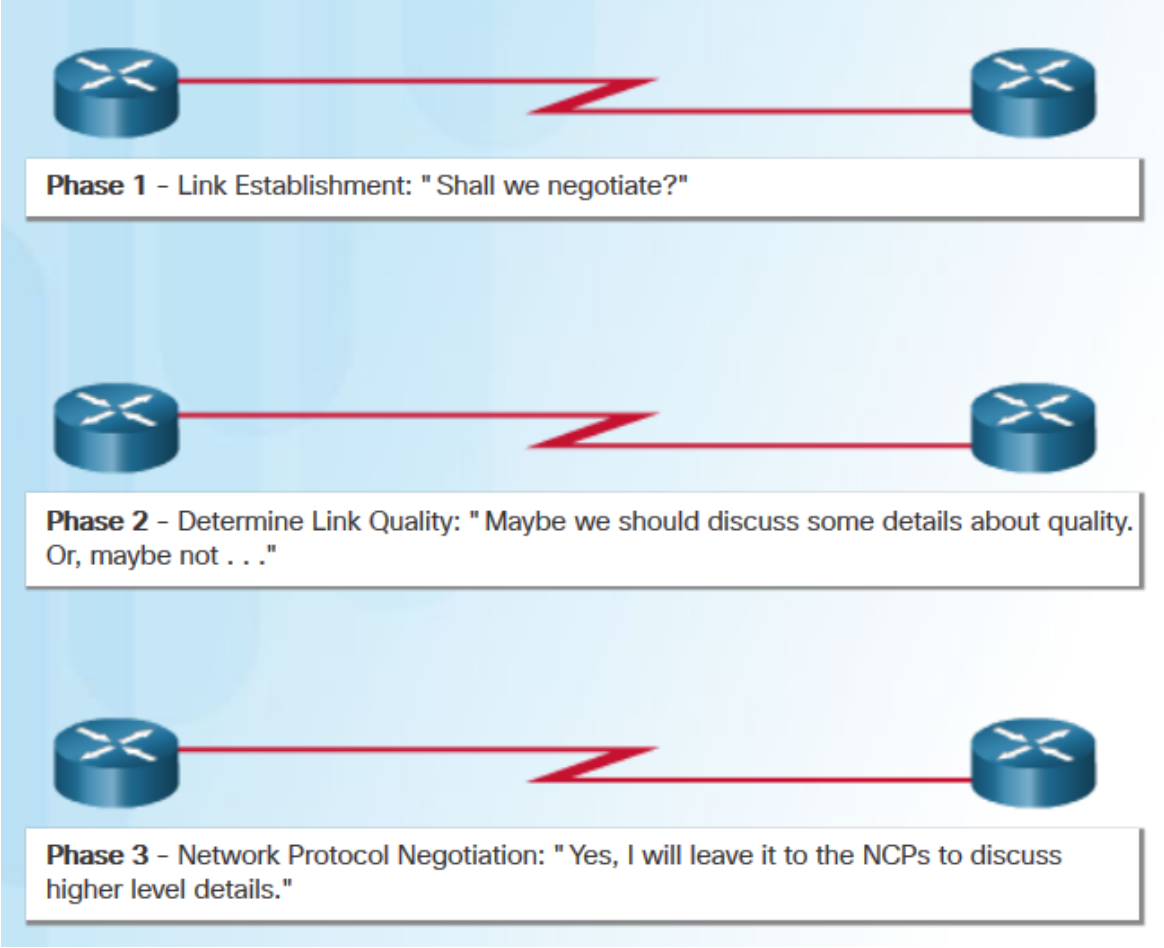


PPP Frame Structure

- A PPP frame consists of six fields:
  - Flag: the beginning or end of the frame: 01111110
  - Address: not used – 11111111
  - Control: unnumbered frames: 00000011
  - Protocol: 2-byte L3 protocol number
  - Data
  - Frame Check Sequence (FCS)



Establishing a PPP Session

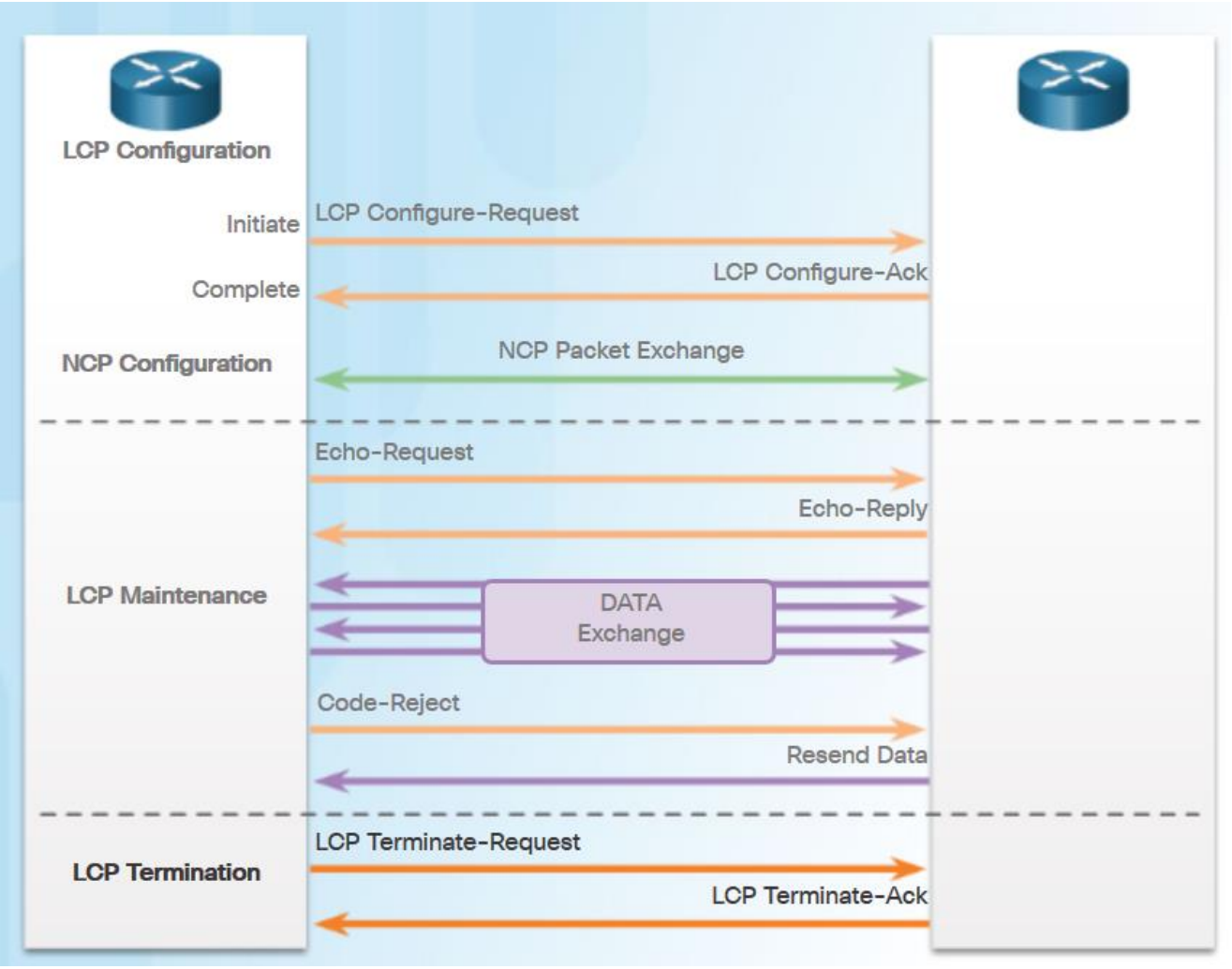


Phase 1 – LCP opens the connection, negotiate configuration options; completed when CFG-Ack frame comes

Phase 2 – LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.

Phase 3 – After the LCP finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time

LCP Operation

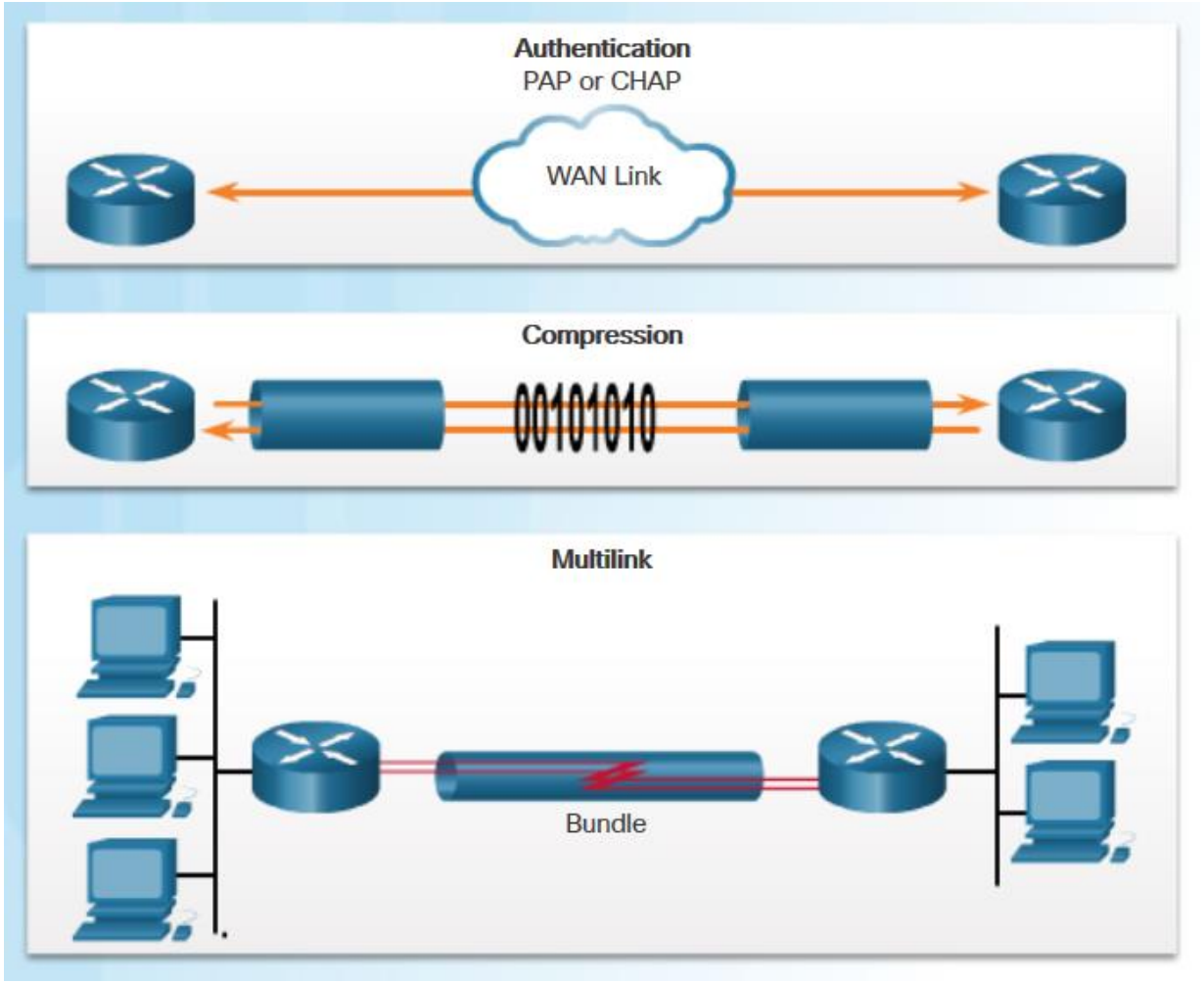


1. **Link establishment**
   - Configure-Request
   - Configure-Ack
   - Configure-Nak
   - Configure-Reject
2. **Link maintenance**
   - Echo-Request
   - Echo-Reply
   - Code-Reject
   - Protocol-Reject
   - Discard-Request
3. **Link termination**
   - Terminate-Request
   - Terminate-Ack

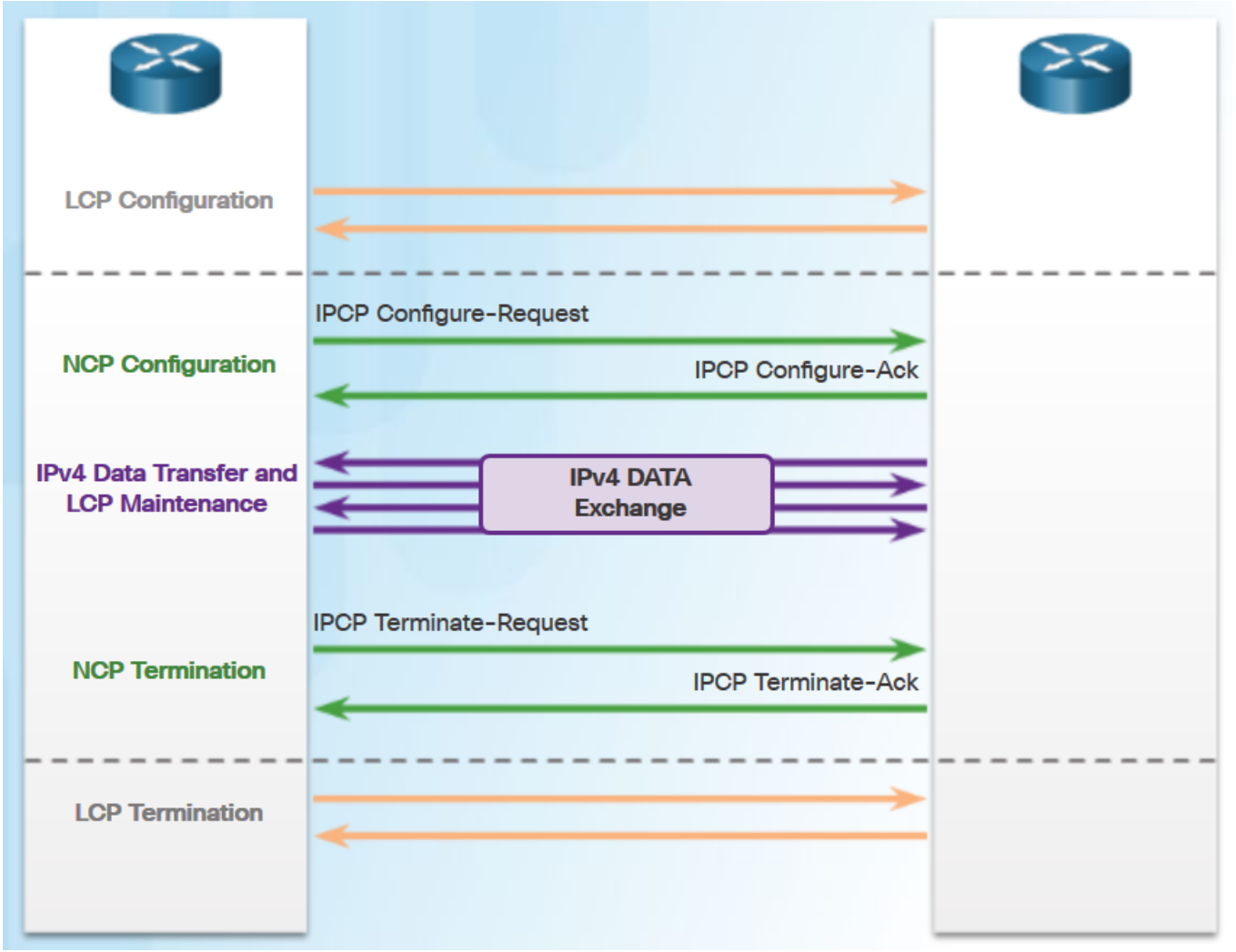
PPP Configuration Options

Optional functions include:

- Authentication using either PAP or CHAP
- Compression using either Stacker or Predictor
- Multilink that combines two or more channels to increase the WAN bandwidth



NCP Operation



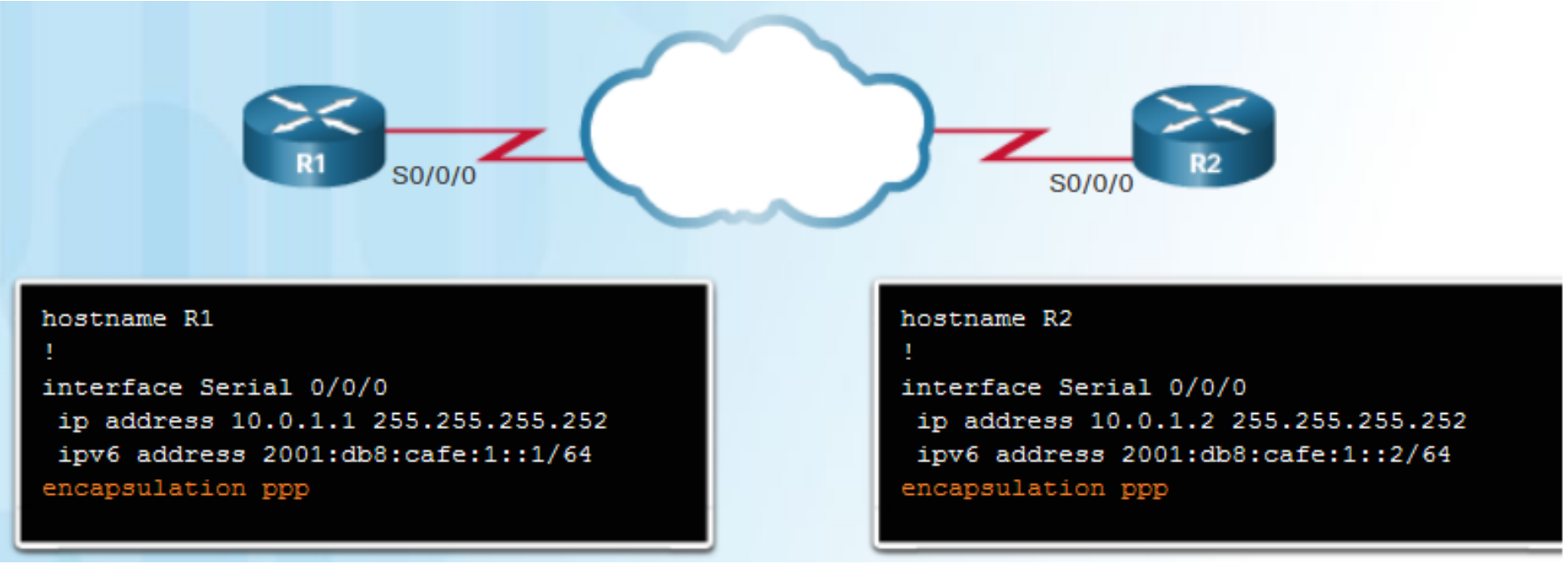
IPCP Example

- Compression
  - Stacker
  - Predictor
- IPv4-Address

2.3 PPP Implementation

Cisco | Networking Academy®
Mind Wide Open™

PPP Basic Configuration




```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
encapsulation ppp
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
encapsulation ppp
```

PPP Compression


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
compress predictor
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
compress predictor
```

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

Keyword	Description
predictor	(Optional) Specifies that a predictor compression algorithm will be used.
stac	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used.

PPP Link Quality Monitoring

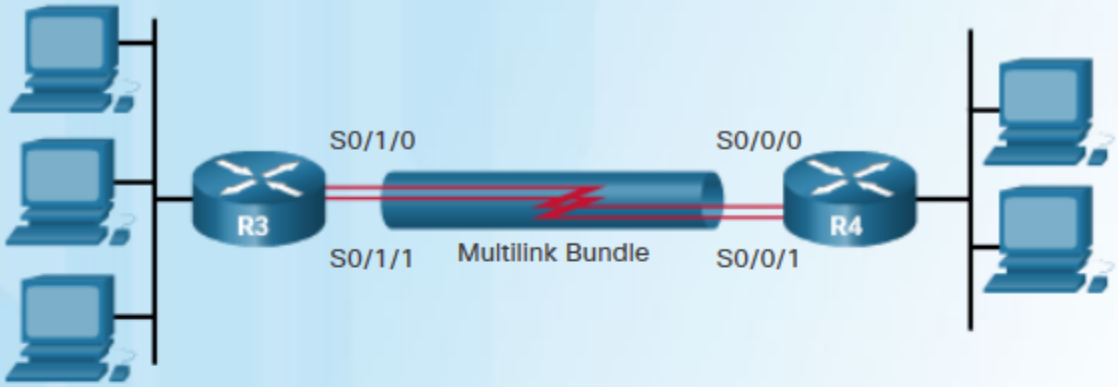

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 ppp quality 80
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp quality 80
```

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

Keyword	Description
percentage	Specifies the link quality threshold. Range is 1 to 100.

PPP Multilink




```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Verifying PPP Configuration

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show interfaces serial	Displays information about a serial interface.
show ppp multilink	Displays information about a PPP multilink interface.

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
```

show interfaces serial 0/0/0

show ppp multilink

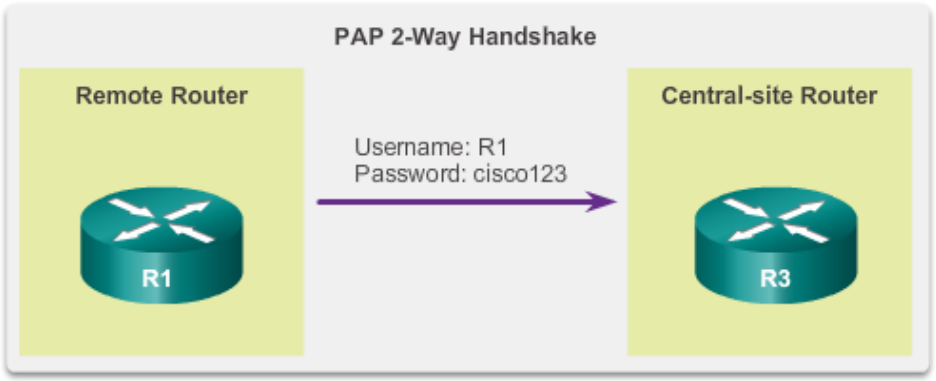
```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

Password Authentication Protocol (PAP)

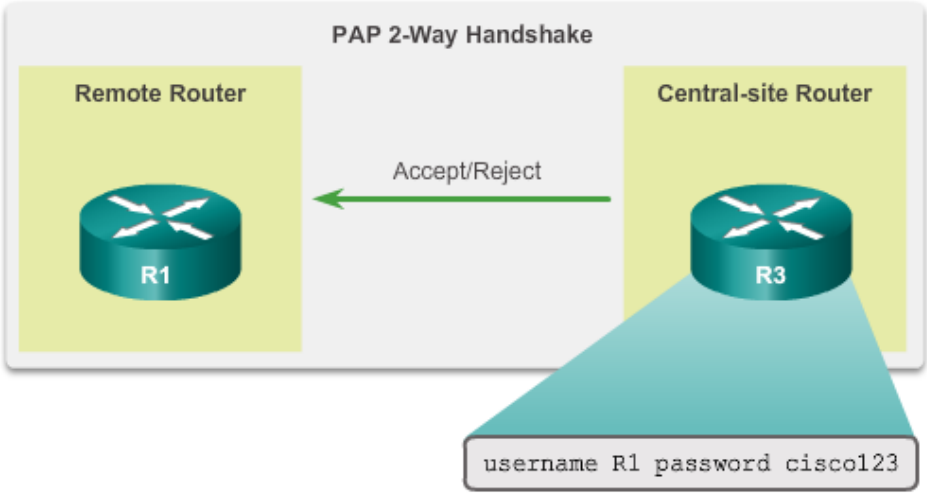
1. Initiating PAP

R1 sends its PAP username and password to R3.

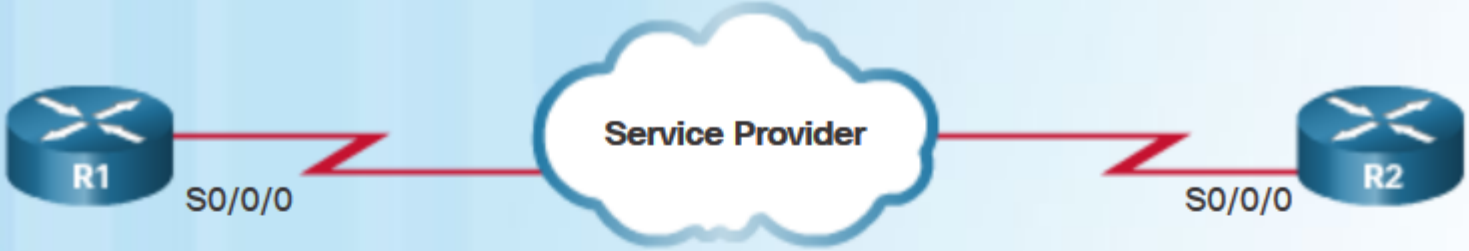


2. Completing PAP

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



Configuring PPP PAP Authentication

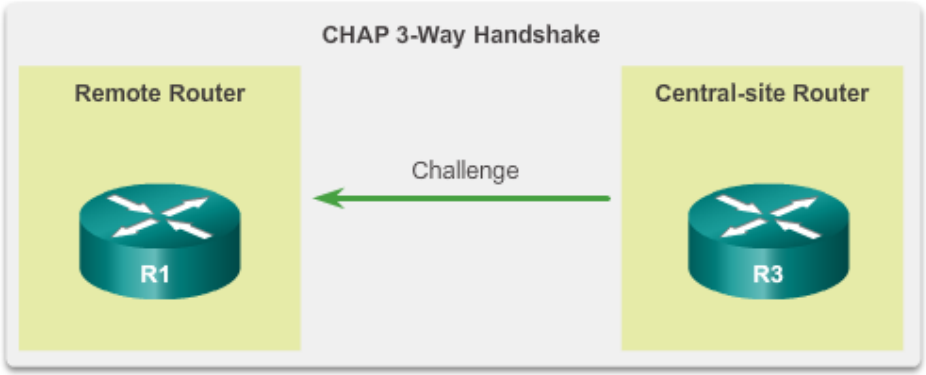



```
hostname R1
username R2 password someone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password someone
```

```
hostname R2
username R1 password someone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password someone
```

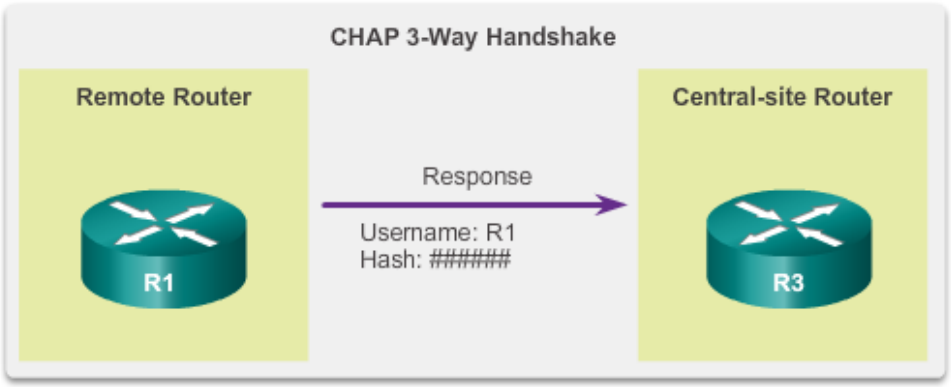
Challenge Handshake Authentication Protocol (CHAP)

R3 initiates the 3-way handshake and sends a challenge message to R1.



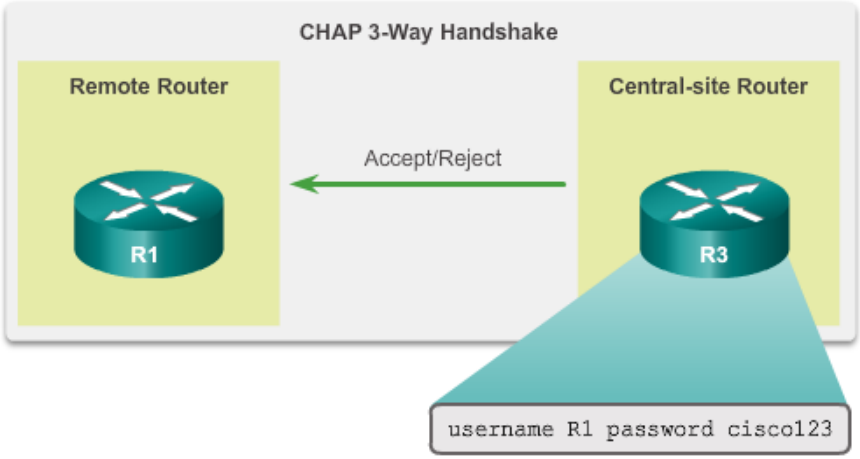
1. Initiating CHAP

R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.



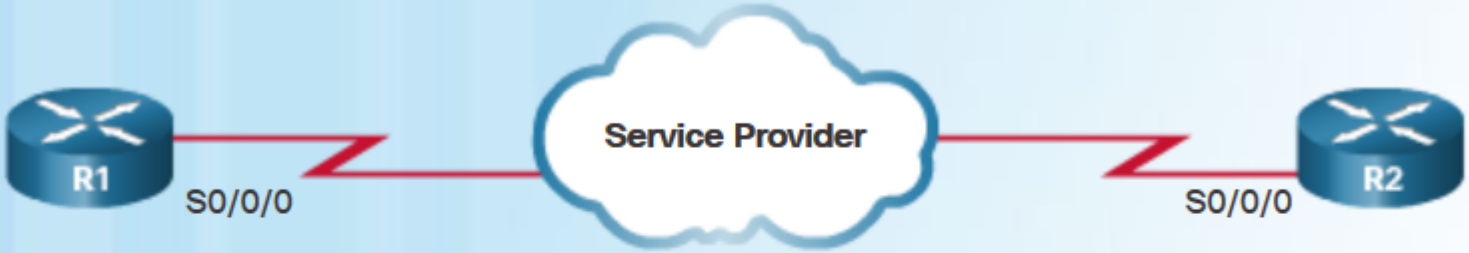
2. Responding CHAP

Using the username and password for R1 in it's local database, R3 compares its calculated hash value with the one sent from R1.



3. Completing CHAP

Configuring PPP CHAP Authentication




```
hostname R1
username R2 password someone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

```
hostname R2
username R1 password someone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```

2.4 Troubleshoot WAN Connectivity

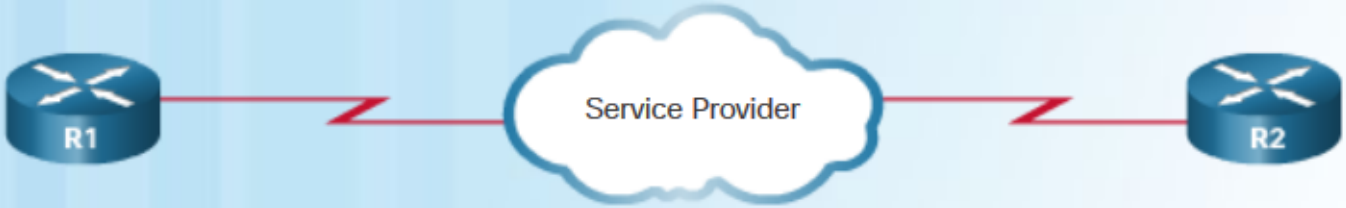
Cisco | Networking Academy®
Mind Wide Open™

Troubleshooting PPP Serial 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 Microsoft Callback Control (MSCB) protocol.

Debug PPP Negotiation




```
R1# debug ppp negotiation
PPP protocol negotiation debugging is on
R1#
*Apr  1 18:42:29.831: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to up
*Apr  1 18:42:29.831: Se0/0/0 PPP: Sending cstate UP notification
*Apr  1 18:42:29.831: Se0/0/0 PPP: Processing CstateUp message
*Apr  1 18:42:29.835: PPP: Alloc Context [66A27824]
*Apr  1 18:42:29.835: ppp2 PPP: Phase is ESTABLISHING
*Apr  1 18:42:29.835: Se0/0/0 PPP: Using default call direction
*Apr  1 18:42:29.835: Se0/0/0 PPP: Treating connection as a
dedicated line
*Apr  1 18:42:29.835: Se0/0/0 PPP: Session handle[4000002]
Session id[2]
*Apr  1 18:42:29.835: Se0/0/0 LCP: Event[OPEN]
State[Initial to Starting]
*Apr  1 18:42:29.835: Se0/0/0 LCP: O CONFREQ [Starting]
id 1 len 23
*Apr  1 18:42:29.835: Se0/0/0 LCP:    AuthProto
CHAP (0x0305C22305)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    QualityType 0xC025
period 1000 (0x0408C025000003E8)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    MagicNumber 0x1E887DD3
```

Debug PPP Authentication

- Always verify your configuration with the **show interfaces serial** command, in the same way as you did without authentication.
- Never assume your authentication configuration works without testing it using the previously covered show commands
- For debugging PPP authentication, use the **debug ppp authentication** command.

```
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
```