WAN Technologies

❓ Tags	
⊙ Klaar	JA
☰ Week	Week 4

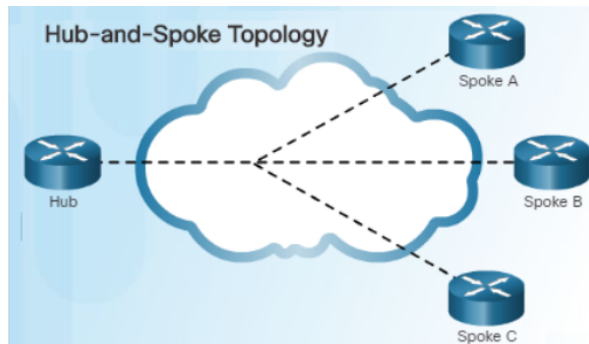# WAN Topologies

Point-to-Point
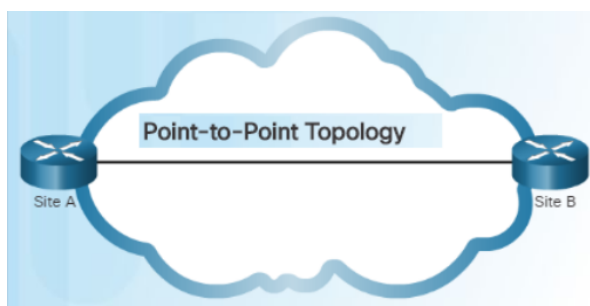
Employs a point-to-point circuit between two endpoints
Typically involves a dedicated leased-line connection such as a T1/E1 line.
Transparent to the customer network and appears to be a direct physical link between two endpoints
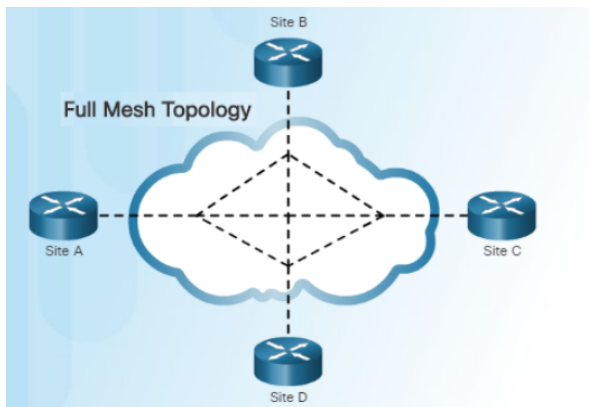
Hub-and-Spoke

Applicable when a private network connection between multiple sites is required

A single interface to the hub can be shared by all spoke circuits.

Spoke sites can be interconnected through the hub site using virtual circuits and routed subinterfaces at the hub.

Full Mesh

A disadvantage of the hub-and-spoke topology is that all communication has to go through the hub.

With a full mesh topology using virtual circuits, any site can communicate directly with any other site.

A disadvantage is the large number of virtual circuits that need to be configured and maintained.

Dual-homed
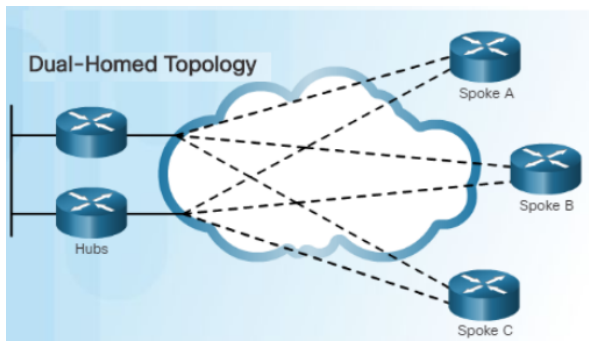
Provides redundancy and load balancing however they are more expensive to implement than single-homed topologies.

Requires additional networking hardware including routers and switches.

More difficult to implement since they require complex configurations.

Different Layer 1 WAN techniques

See Presentatie week4 les 1 dia 14-36

Broadband Connections

Two types of equipment are required to send signals upstream and downstream on a cable system:

- Cable Modem Termination System (CMTS) at the headend of the cable operator. The headend is a router with databases for providing Internet services to cable subscribers.

- Cable Modem (CM) on the subscriber end.

WAN Encapsulation Protocols

- HDLC - Default encapsulation on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices.

- PPP - Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Has built-in security mechanisms such as PAP and CHAP.

DSL:

Digital Subscriber Line (DSL) is a means of providing high-speed connections over installed copper wires.
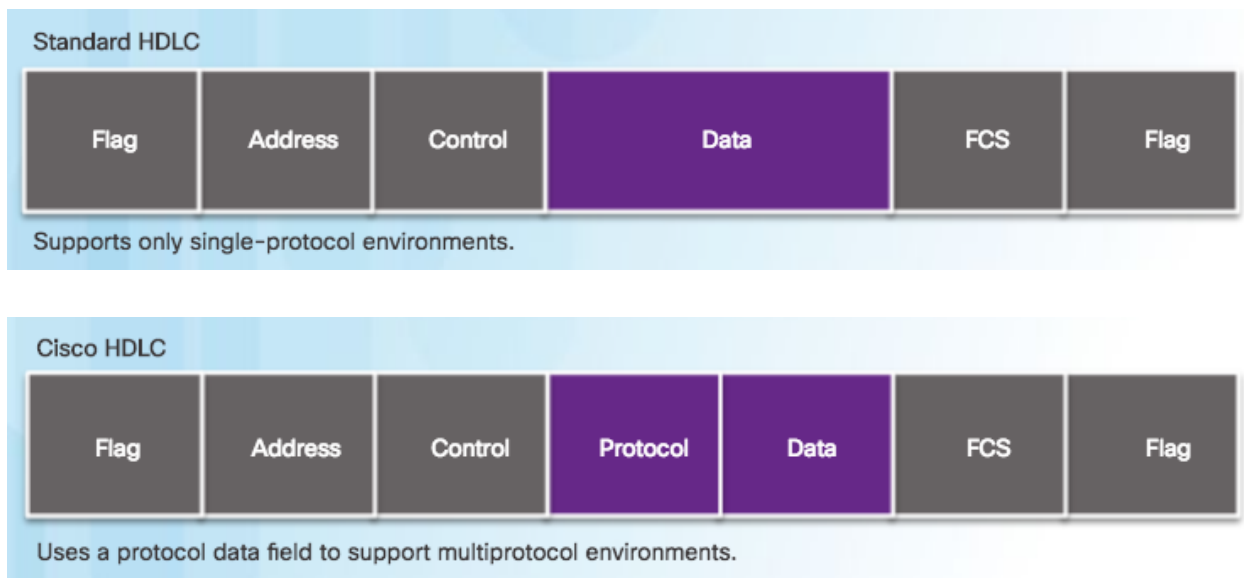Asymmetric DSL (ADSL) provides higher downstream bandwidth to the user than upload bandwidth.
Symmetric DSL (SDSL) provides the same capacity in both directions.
For satisfactory ADSL service, the local loop length must be less than 3.39 miles (5.46 km).

Advantage of DSL over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM.

HDLC Encapsulation

Standard HDLC

| Flag | Address | Control | Data | FCS | Flag |

Supports only single-protocol environments.

Cisco HDLC

| Flag | Address | Control | Protocol | Data | FCS | Flag |

Uses a protocol data field to support multiprotocol environments.

Cisco's HDLC is a point-to-point protocol that can be used on leased lines between two Cisco devices.

Protocol field makes it possible for a single serial link to accommodate multiple network-layer protocols.

Configuration example

Enable HDLC on the Serial 0/0/0 interface

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation hdlc
```

PPP Encapsulation

Advantages of PPP

- The link quality management feature (LQM) monitors the quality of the link. LQM can be configured with the interface command ppp quality percentage. If the error percentage falls below the configured threshold, the link is taken down and packets are rerouted or dropped.

- PPP supports PAP and CHAP authentication.

PPP contains three main components:

1. HDLC-like framing for transporting multiprotocol packets over point-to-point links.

2. Extensible Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

   a. LCP functions within the data link layer and has a role in establishing, configuring, and testing the data-link connection.

   b. LCP establishes the point-to-point link.

   c. LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.

   d. After the link is established, PPP also uses LCP to agree automatically on encapsulation formats such as authentication, compression, and error detection.

3. Network Control Protocols (NCPs) for establishing and configuring different network layer protocols (IPv4 and IPv6 Control Protocol).

   a. PPP permits multiple network layer protocols to operate on the same communications link. For every network layer protocol used, PPP uses a separate NCP, as shown in the figure. IPv4 uses IP Control Protocol and IPv6 uses IPv6 Control Protocol.

   b. NCPs include functional fields containing standardized codes to indicate the network layer protocol that PPP encapsulates.

      i. Value 8021 = IPCP

      ii. Value 8057 = IPv6CP

PPP compared to the OSI-model
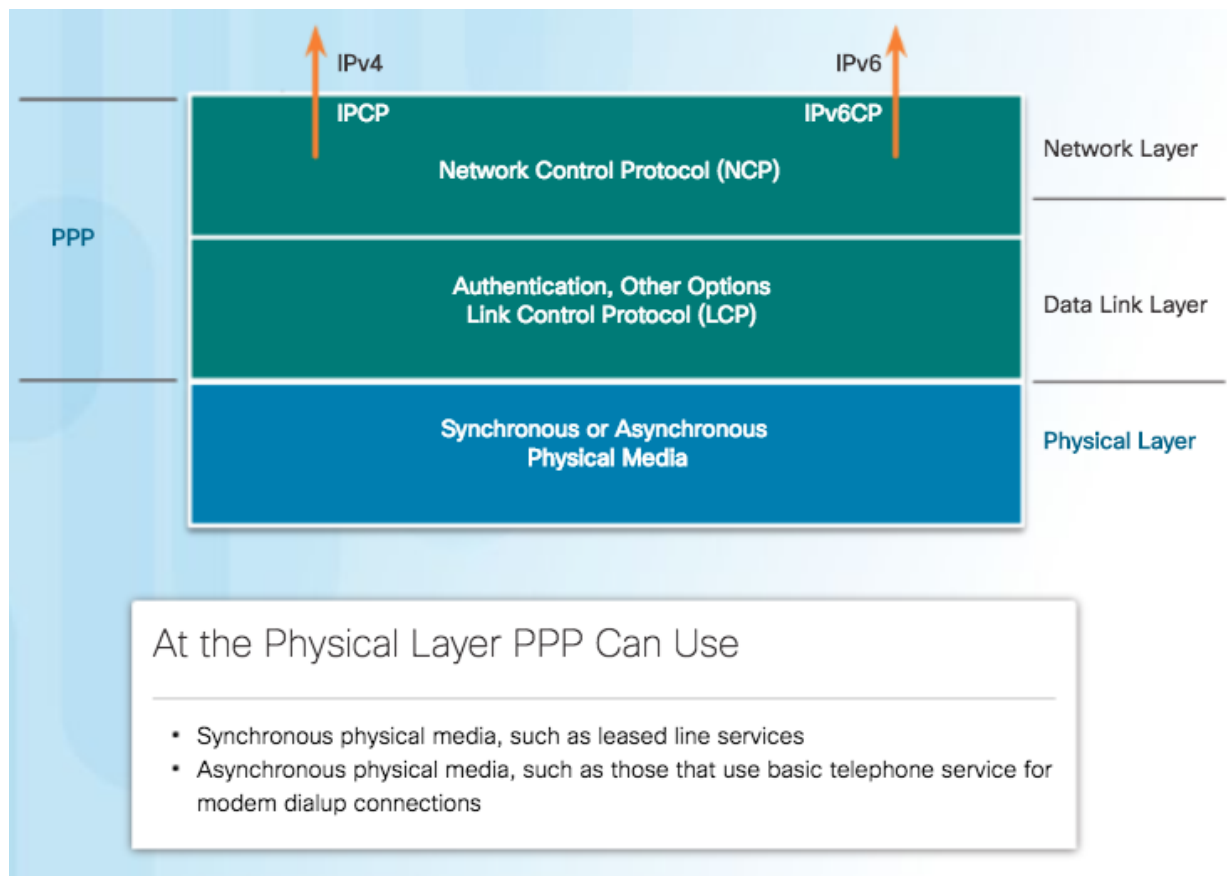
LCP Communnication
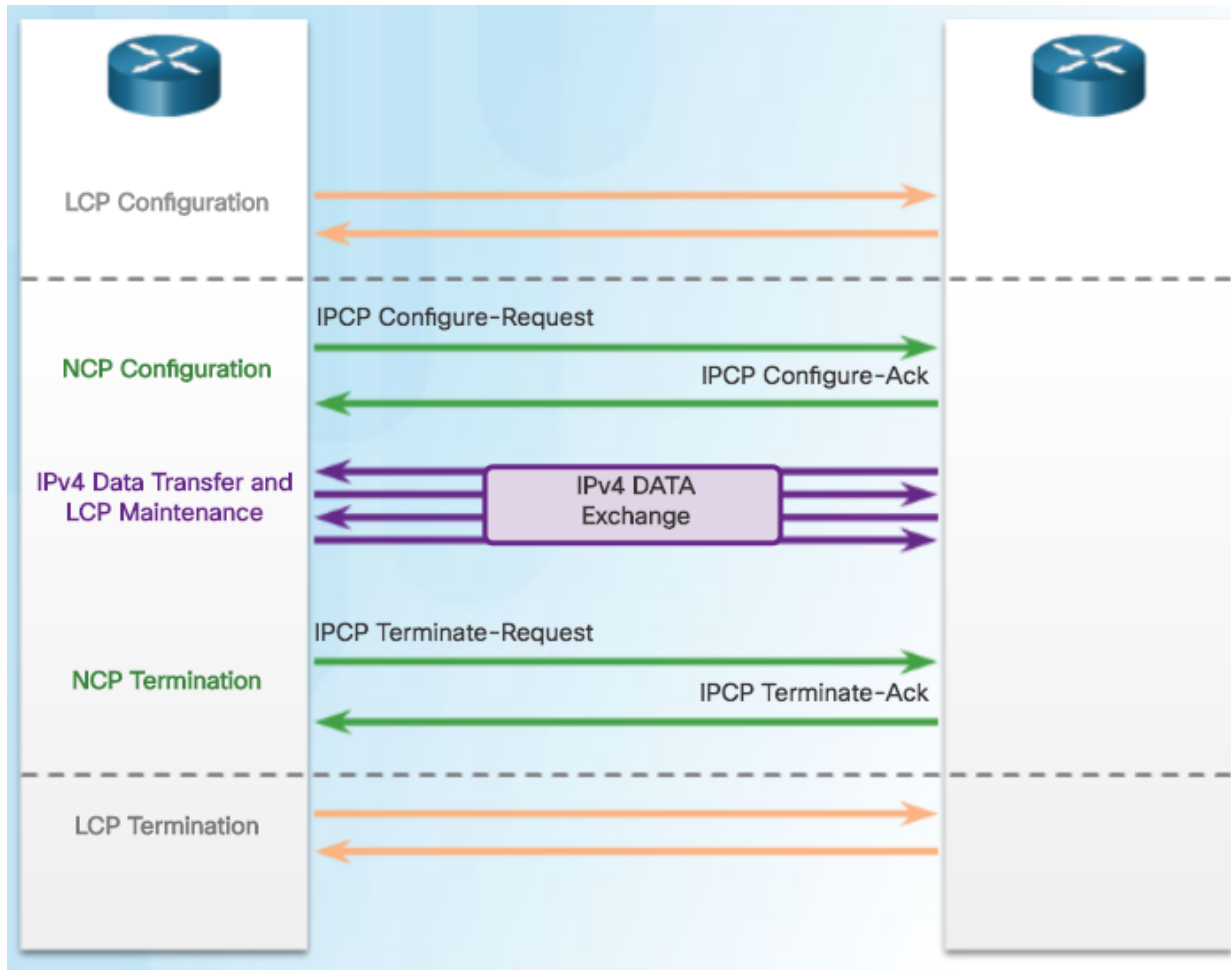
When data transfer is complete, NCP terminates the protocol link and LCP terminates the PPP connection.

After LCP has established the link, the routers exchange IPCP messages, negotiating options specific to IPv4.
IPCP is responsible for configuring, enabling, and disabling the IPv4 modules on both ends of the link.
IPCP negotiates two options:

- Compression - Allows devices to negotiate an algorithm to compress TCP and IP headers and save bandwidth.

- IPv4-Address - Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder.

After the NCP process is complete, the link goes into the open state and LCP takes over again in a link maintenance phase.

Configuration example

Use **PPP encapsulation**:

```
R1(config-if)# encapsulation ppp
```

Use **compression** (must be the same at both sides (both routers))

```
R1(config-if)# compress predictor
```

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.

The **PPP quality** percentage command ensures that the link meets the set quality requirement; otherwise, the link closes down

```
R1(config-if)# ppp quality 80
```

Configuration ppp quality 80, shown in the example, sets minimum quality to 80%

PPP Multilink

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
```

PPP Authentication

```
ppp authentication {chap | chap pap | pap chap | pap}
```

The ppp authentication Command

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP.

Verifying Configuration

Use the following commands to verify the PPP configuration

```
show ppp multilink
```

PPPoE Encapsulation

PPPoE creates a PPP tunnel over an Ethernet connection.

Configuration Example