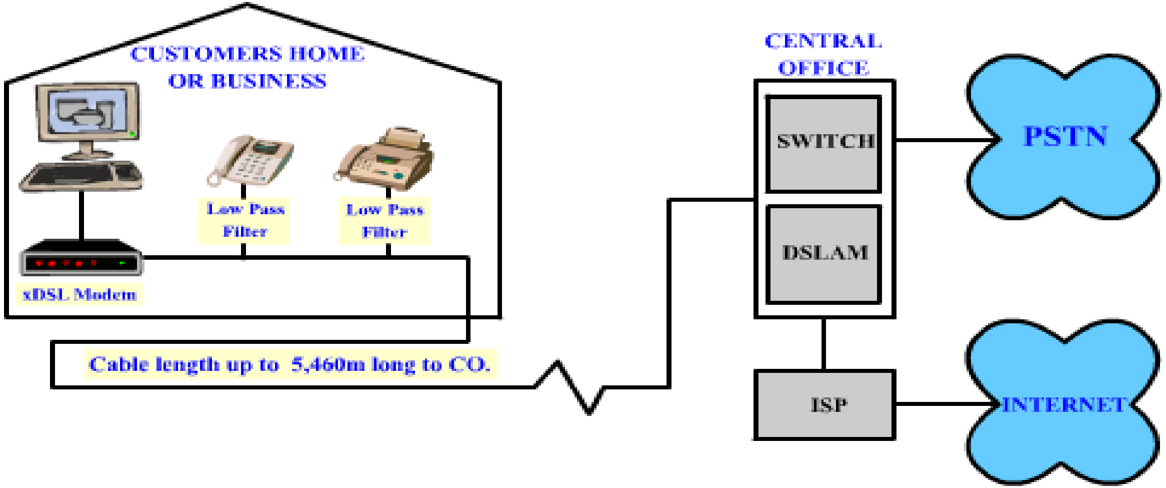
18CSC302J- Computer Networks

Unit-5

DSL Technology

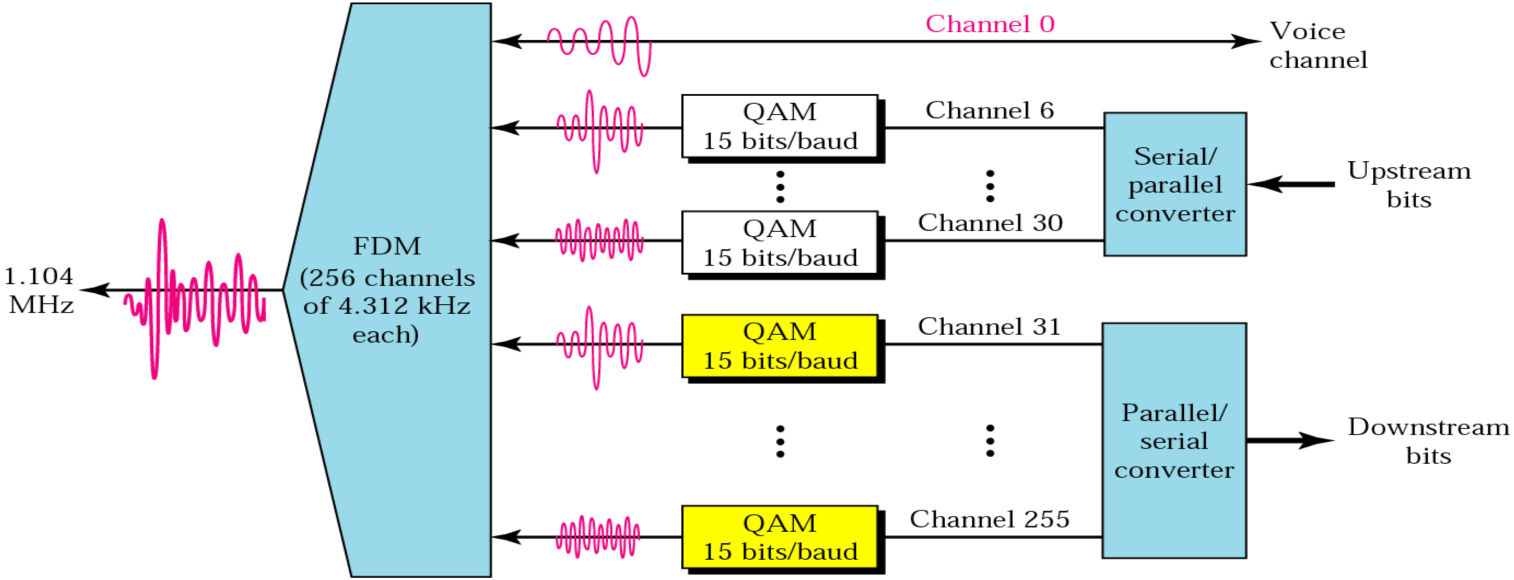


- Limited distance to central office (CO)
- Dedicated line from CO to home
- Asymmetric flow
- Typical speeds up to 1.5Mbits/s downstream

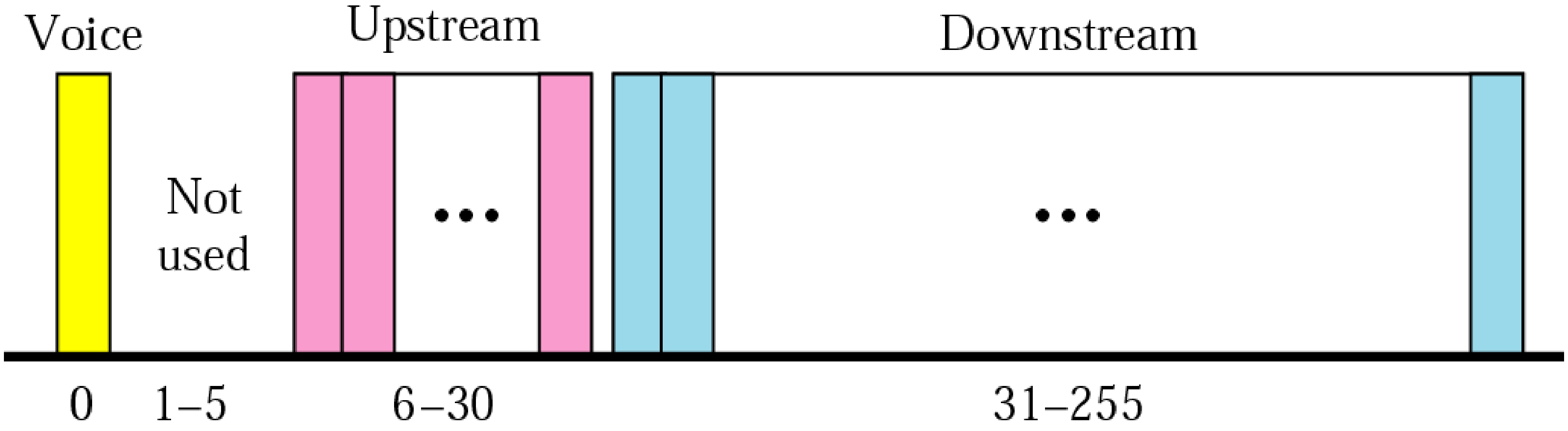
Digital Subscriber Line (DSL)

- Uses a newer technology that used the existing telecommunications networks such as the local loop telephone line.
- Is an asymmetric communication technology designed for residential users; it is not suitable for business.
- xDSL: where x can be replaced by A, V, H, or S
- The existing local loops can handle bandwidths up to 1.1 MHz
    - by removing the filter at the end of line of telephone company
    - but, limitation because of distance between the residence and the switching office, size of cable
- ADSL is an adaptive technology. The system uses a date rate based on the condition of the local loop line

- **DMT**
  - Modulation technique that has become standard for ADSL is called the discrete multi tone technique (DMT)



- voice : channel 0 is reserved for voice
- Idle : channel 1 to 5 are not used; gap between voice and data communicaiton
- Upstream data and control : channels 6 to 30 (25channels); one channel for control
- Downstream data and control : channels 31 to 255(225 channels); 13.4 Mbps; one channel for control

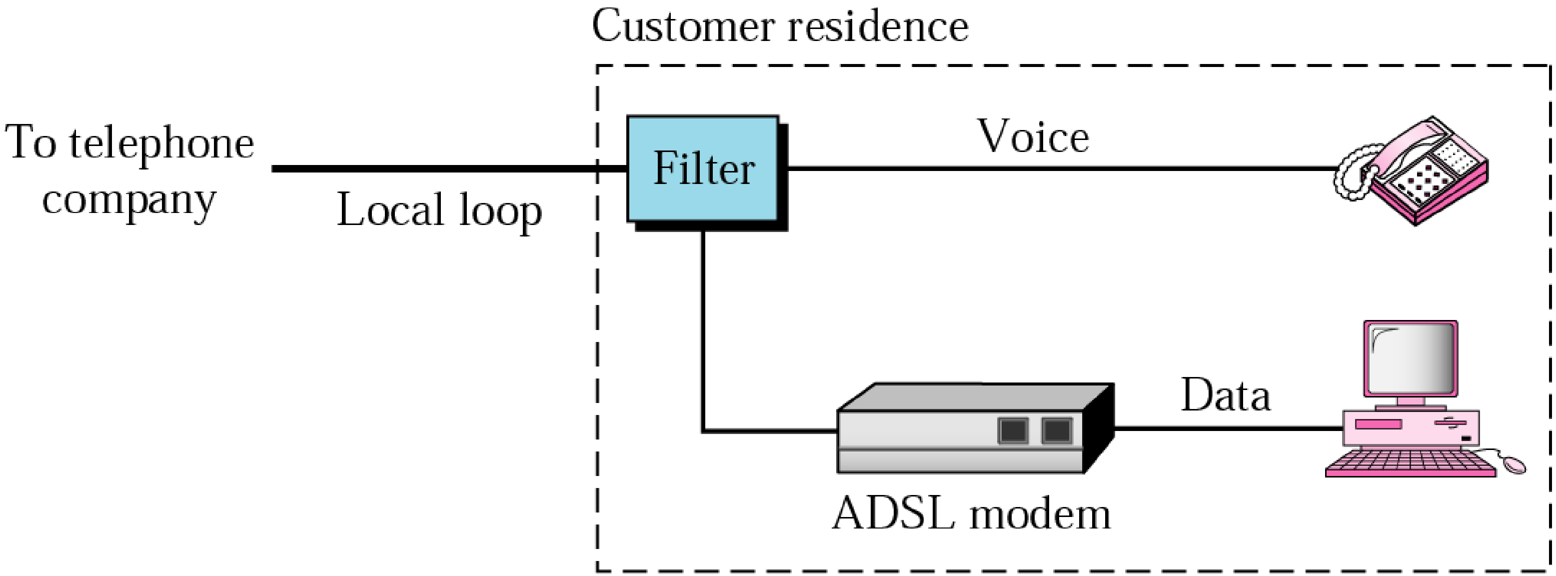


Source: Douglas E. Comer, Internetworking with TCP/IP, Principles, protocols, and architecture,Vol 1 5th Edition,2006

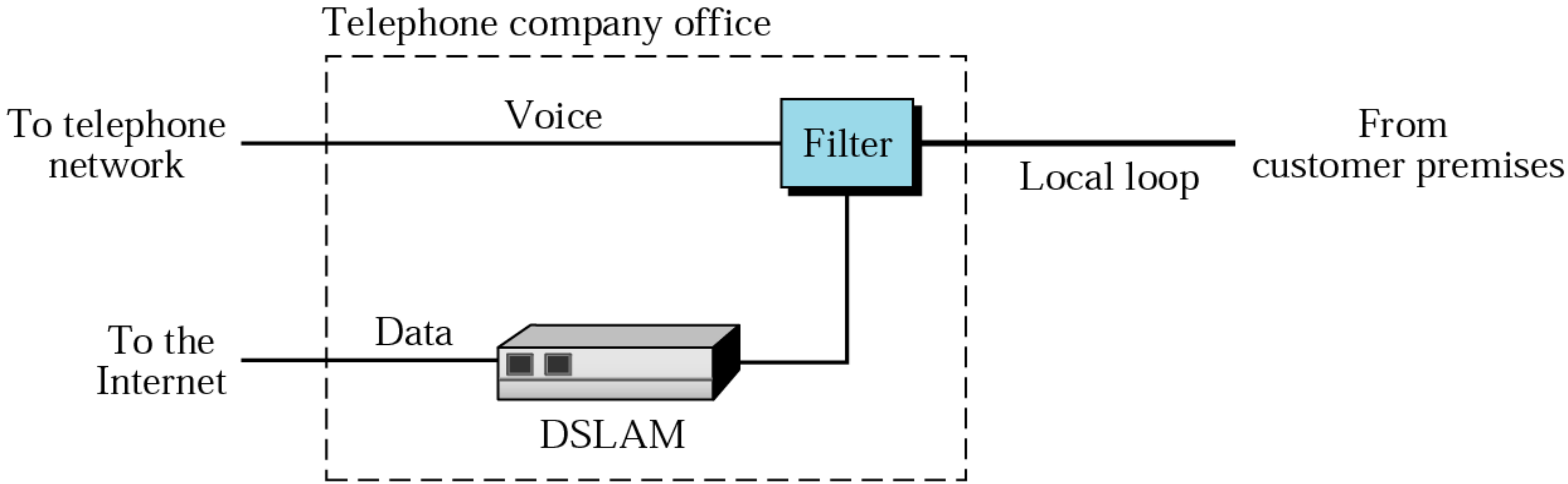
- Actual Bit Rate
    - Upstream : 64 Kbps to 1 Mbps
    - Downstream : 500 Kbps to 8 Mbps

  * Because of the high signal/noise ratio

Customer Site : ADSL Modem



Telephone Company Site : DSLAM

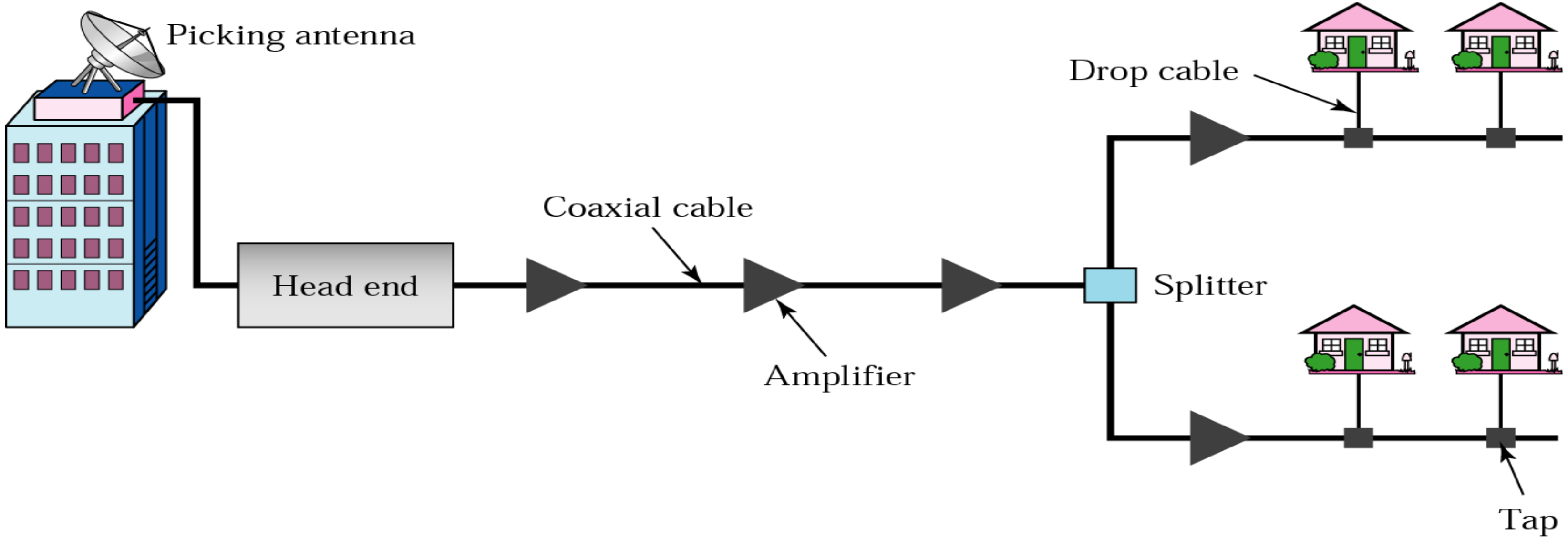


Other DSL Technologies

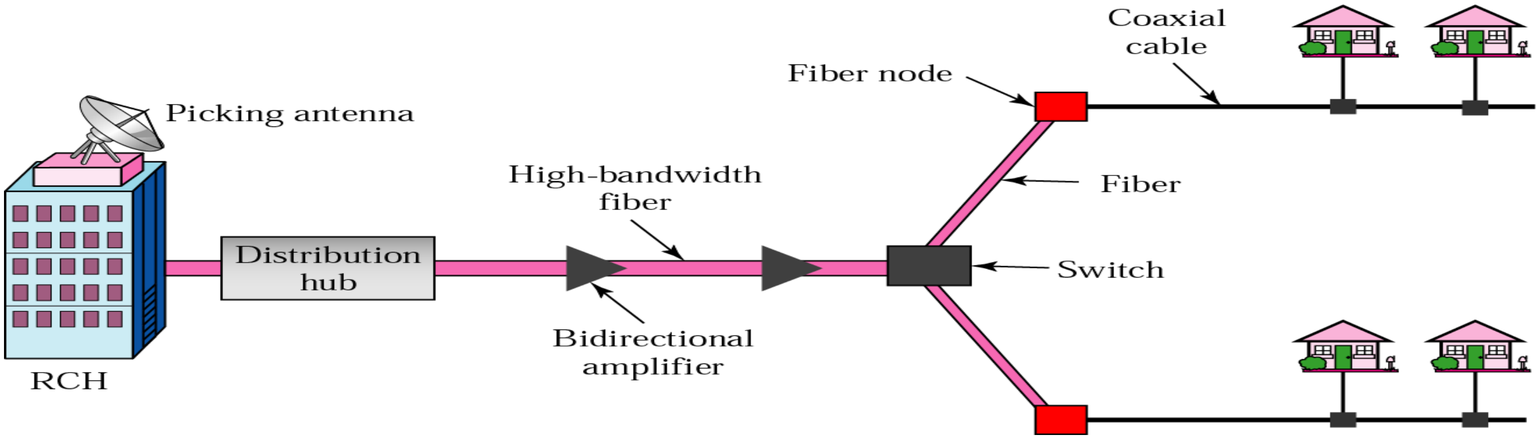
- SDSL: Symmetric Digital Subscriber Line
- HDSL: High-bit-rate digital subscriber line
  - an alternative to the T-line (1.544 Mbps)
  - using 2B1Q encoding
  - up to 3.6 Km
  - using 2 twisted-pair wires for full-duplex transmission
- VDSL : Very-high-rate digital subscriber
  - using coaxial cable, fiber-optic, or twisted pair cable for short distances (300 to 1800 m)
  - using DMT with a bit rate of 50 to 55 Mbps downstream and 1.5 to 2.5 Mbps upstream

Communication in the traditional cable TV network is unidirectional.

- Traditional cable Networks
  - community antenna TV (CATV)



HFC Network



- RCH : Regional cable head; serving 400,000 subscribers;
- Distribution hub: serving 40,000 subscribers
- Coaxial cable : serving 1,000 subscribers
- Communication in HFC cable TV network can be bidireactional.

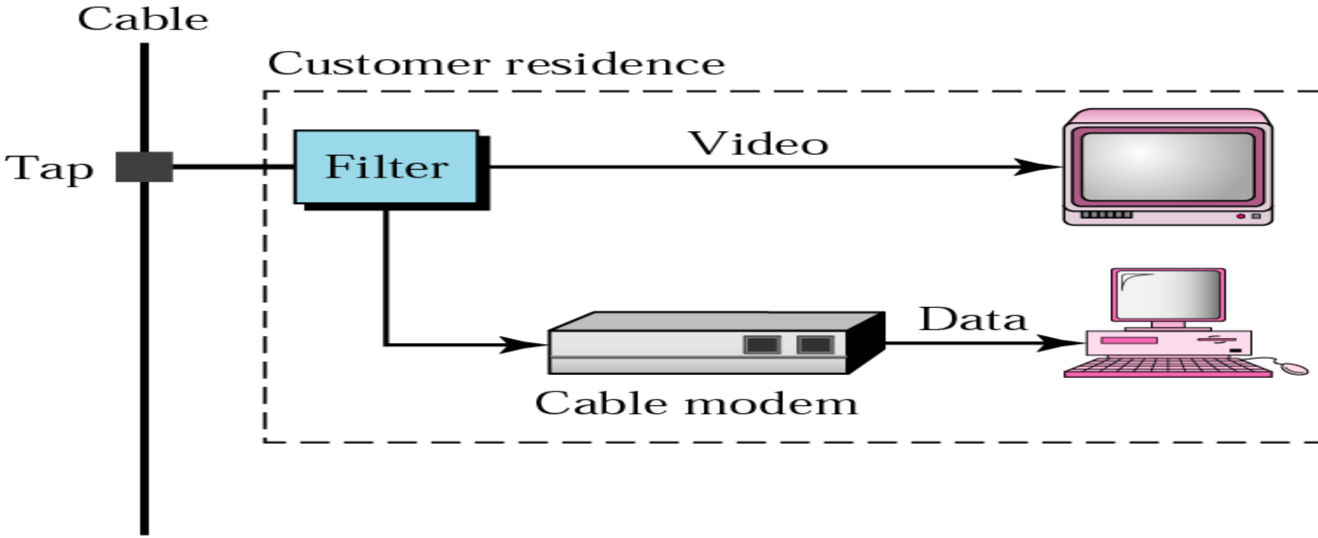
- ## Bandwidth

  - video band
    - 54 to 550 MHz
    - TV channels : 6 Mhz x 80 channels
  - Data downstream band : dividing into 6Mhz channels

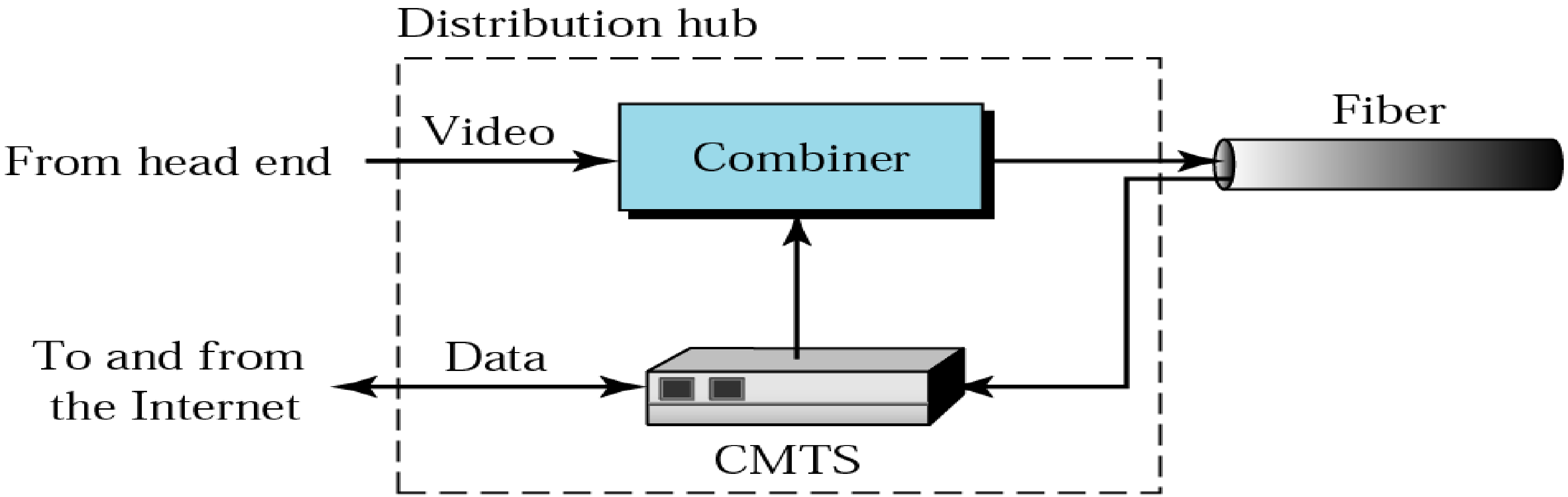
- Modulation
    - Downstream data are modulated using 64-QAM
- Data rate
    - 6 bits for each baud in 64-QAM (1bit : control bit)
    - Theoretically, 5bits/Hz x 6 Mhz = 30 Mbps

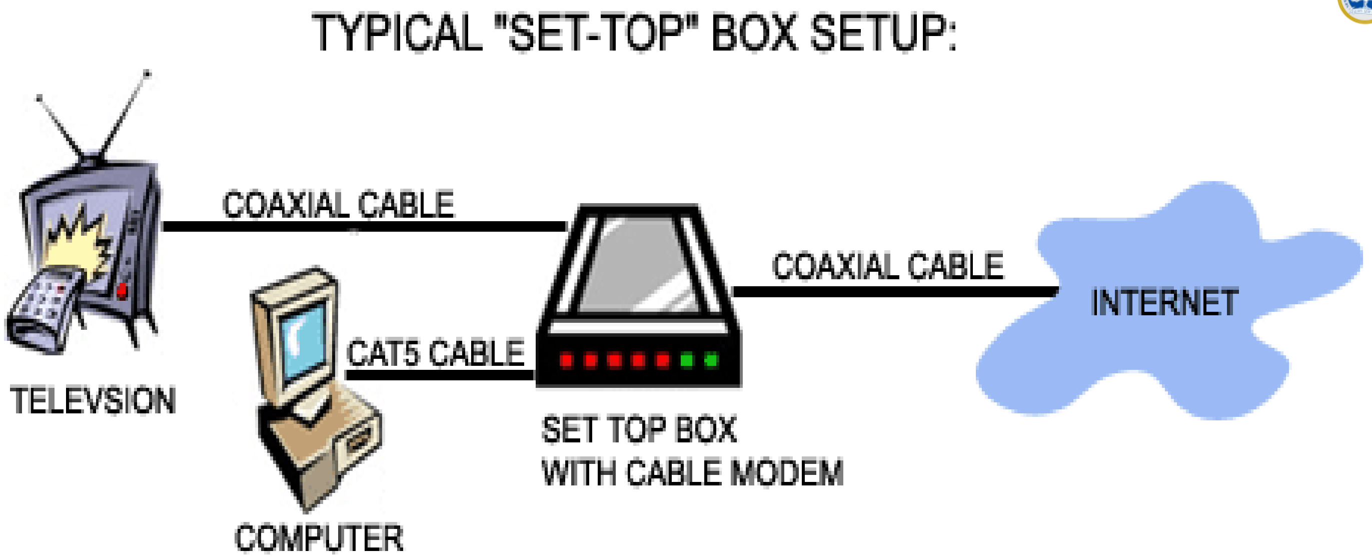
- Upstream data band
    - Modulation
        - upstream data band uses lower frequencies that are more susceptible to noise and interference
        - for this reason, using QPSK instead of QAM
    - Data rate : 2 bits/hz x 6 Mhz = 12 Mbps

- CM is installed inside the distribution hub by the cable company.



Cable modem transmission system(CMTS)





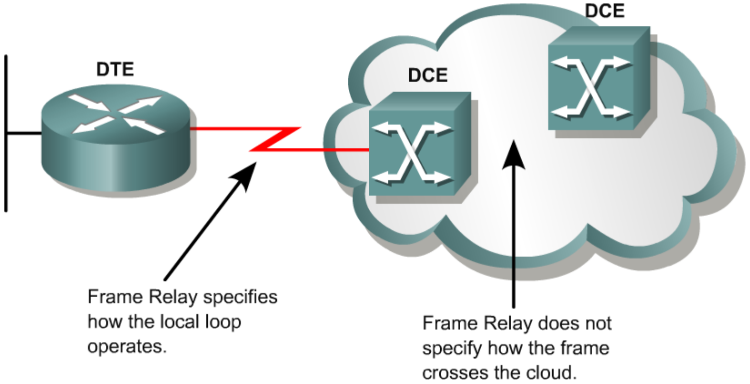
- Shared lines to the nearest splitter
- Generally higher speeds
- Reaches more households since distance limitation is removed
- Typical offering 4Mbits/s
- Last Mile advantage

Future Technology

- WiMax
  - Metropolitan Area Networks (MANs)
  - 3-5 miles range, no direct line of sight required
  - 2Mbits/s practical limit
  - Can use existing cell towers
- Broadband over Power Lines (BPL)
  - More pervasive infrastructure, but requires extra equipment
  - Up to 2.7Mbits/s
  - Superimposing analog signal over AC
  - Small deployments in operation (e.g. Manassas, Virginia 10MBits/s for $30.00 a month)

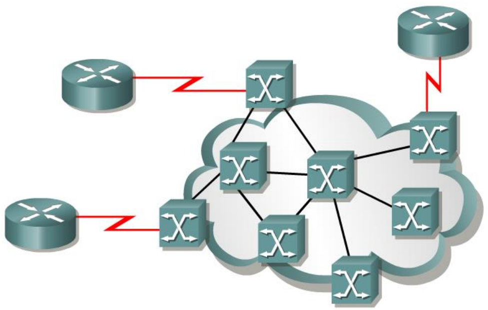
Frame Relay

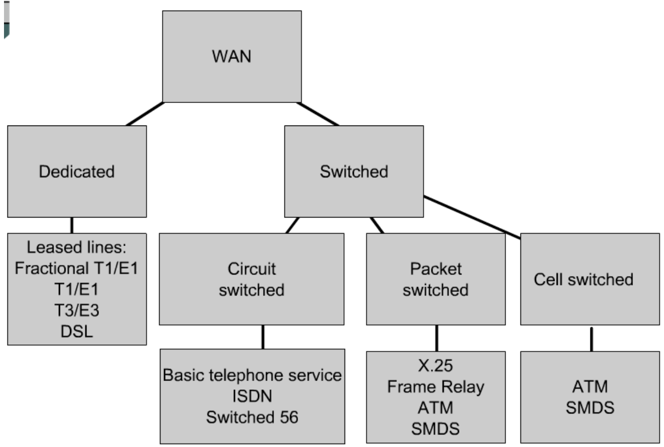
Introducing Frame Relay



- **Frame Relay** is a packet-switched, connection-oriented, WAN service.
- It operates at the data link layer of the OSI reference model.
- Frame Relay uses a subset of the high-level data link control (HDLC) protocol called Link Access Procedure for Frame Relay (LAPF).
- Frames carry data between user devices called data terminal equipment (DTE), and the data communications equipment (DCE) at the edge of the WAN.

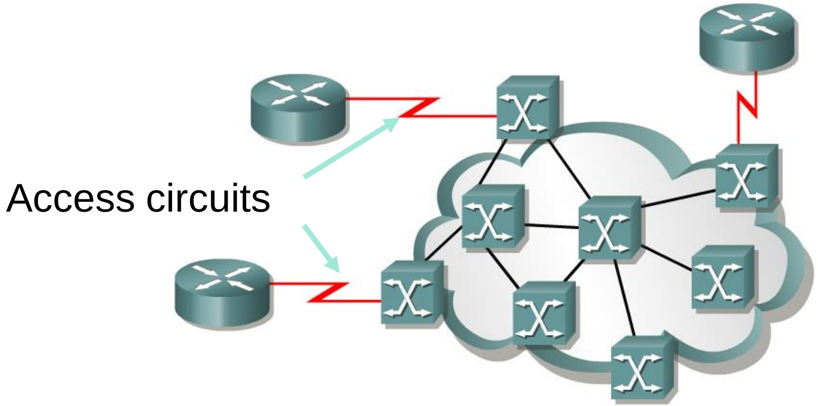
Frame Relay vs. X.25





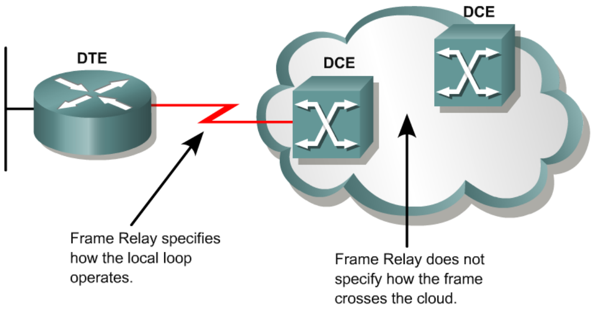
- Frame Relay does not have the sequencing, windowing, and retransmission mechanisms that are used by X.25.
- Without the overhead, the streamlined operation of Frame Relay outperforms X.25.
- Typical speeds range from 1.5 Mbps to 12 Mbps, although higher speeds are possible. (Up to 45 Mbps)
- The network providing the Frame Relay service can be either a carrier-provided public network or a privately owned network.
- Because it was designed to operate on high-quality digital lines, Frame Relay provides no error recovery mechanism.
- If there is an error in a frame it is discarded without notification.

Introducing Frame Relay



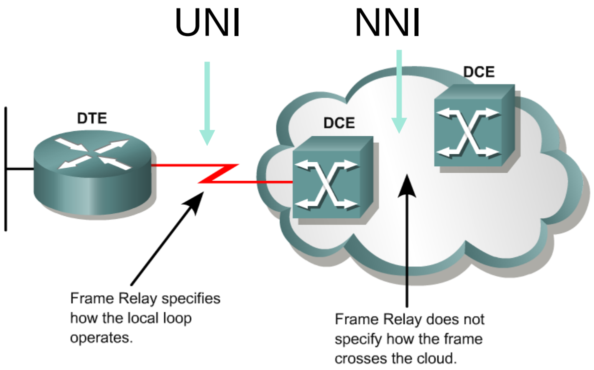
- A Frame Relay network may be privately owned, but it is more commonly provided as a service by a public carrier.
- It typically consists of many geographically scattered Frame Relay switches interconnected by trunk lines.
- Frame Relay is often used to interconnect LANs. When this is the case, a router on each LAN will be the DTE.
- **Access Circuit -** A serial connection, such as a T1/E1 leased line, will connect the router to a Frame Relay switch of the carrier at the nearest point-of-presence for the carrier.

DTE – Data Terminal Equipment



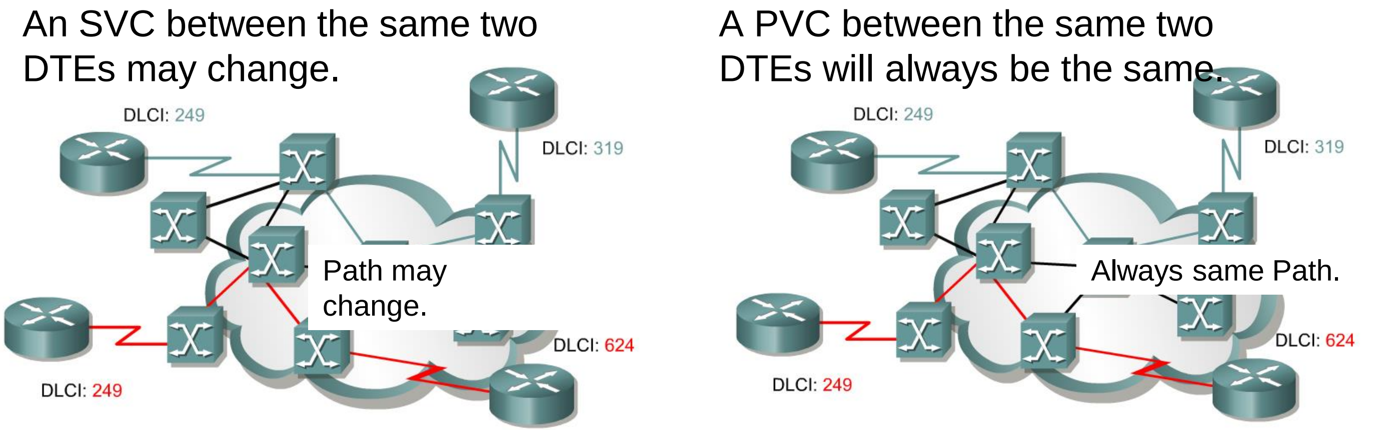
- DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of the customer.
- The customer may also own this equipment.
- Examples of **DTE** devices are routers and Frame Relay Access Devices (FRADs).
- A FRAD is a specialized device designed to provide a connection between a LAN and a Frame Relay WAN.

DCE – Data Communications Equipment



- **DCEs** are carrier-owned internetworking devices.
- The purpose of DCE equipment is to provide clocking and switching services in a network.
- In most cases, these are packet switches, which are the devices that actually transmit data through the WAN.
- The connection between the customer and the service provider is known as the **User-to-Network Interface (UNI).**
- The **Network-to-Network Interface (NNI)** is used to describe how Frame Relay networks from different providers connect to each other.

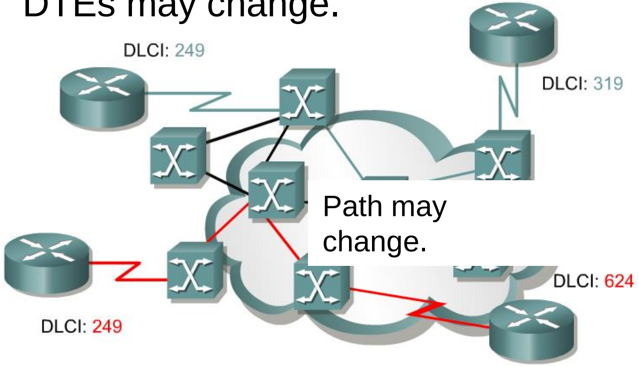
Frame Relay terminology



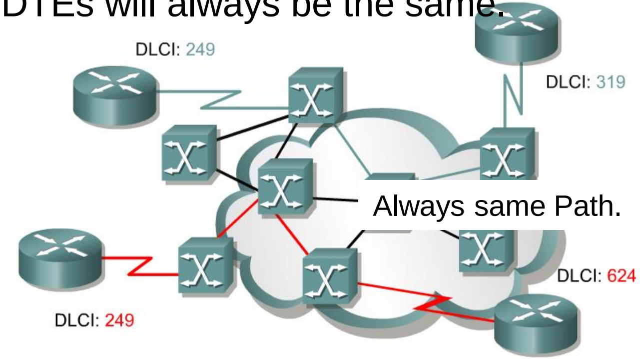
- The connection through the Frame Relay network between two DTEs is called a virtual circuit (VC).
- **Switched Virtual Circuits (SVCs)** are <u>Virtual circuits may be established dynamically by sending signaling messages to the network</u>.
  - However, SVCs are not very common.
- **Permanent Virtual Circuits (PVCs)** are more common.
  - PVC are <u>VCs that have been preconfigured by the carrier are used</u>

Frame Relay operation - SVC

An SVC between the same two DTEs may change.

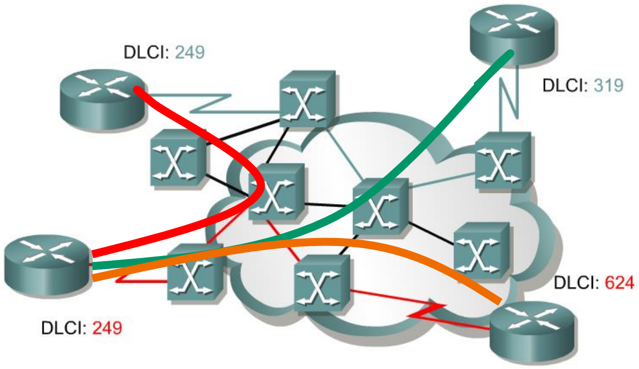


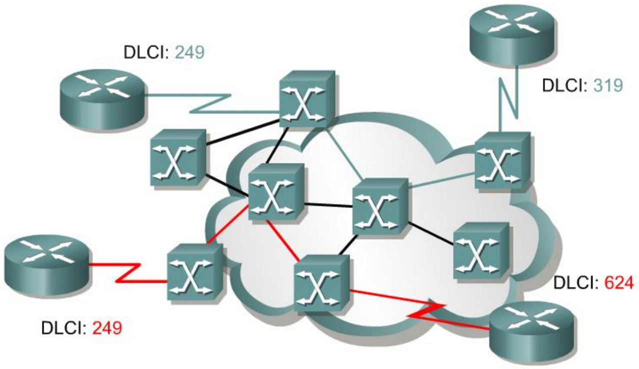
A PVC between the same two DTEs will always be the same.



- **SVCs are temporary connections** that are only used when there is sporadic data transfer between DTE devices across the Frame Relay network.
- Because they are temporary, SVC connections require call setup and termination for each connection supported by Cisco IOS Release 11.2 or later.
- Before implementing these temporary connections, determine whether the service carrier supports SVCs since **many Frame Relay providers only support PVCs.**

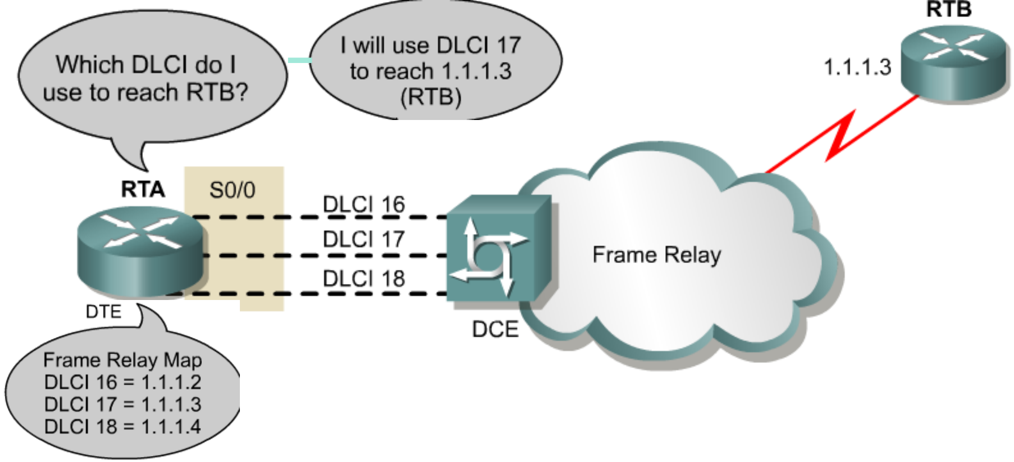
Access Circuits and Cost Savings





- The **FRAD or router** connected to the Frame Relay network may have multiple virtual circuits connecting it to various end points.
- This makes it a very cost-effective replacement for a full mesh of access lines.
- Each end point needs only a single access circuit and interface.

DLCI



- A **data-link connection identifier (DLCI)** identifies the logical VC between the CPE and the Frame Relay switch.
- The Frame Relay switch maps the DLCIs between each pair of routers to create a PVC.
- DLCIs have local significance, although there some implementations that use global DLCIs.
- **DLCIs 0 to 15** and **1008 to 1023** are **reserved** for special purposes.
- Service **providers assign** DLCIs in the range of **16 to 1007**.
  - DLCI 1019, 1020: Multicasts
  - DLCI 1023: Cisco LMI
  - DLCI 0: ANSI LMI

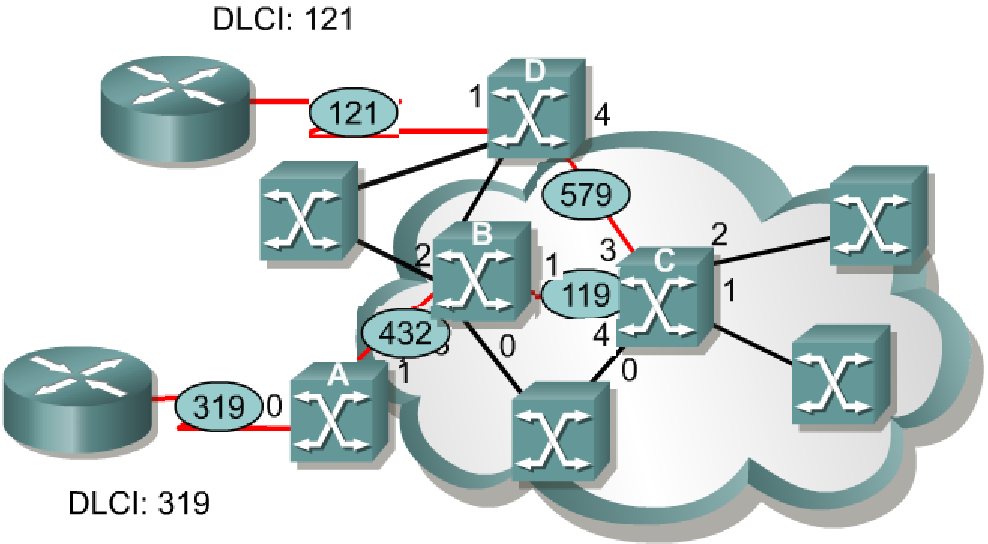
DLCI

A			
VC	Port	VC	Port
319	0	432	1

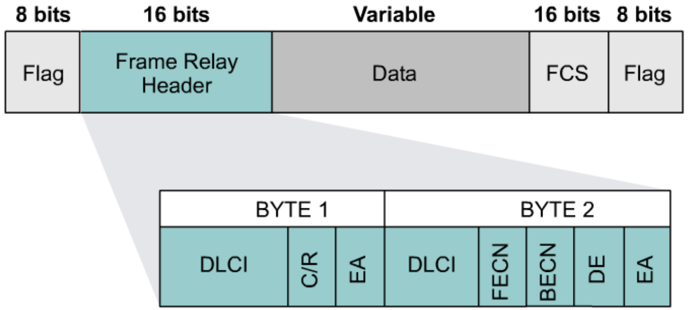
B			
VC	Port	VC	Port
432	3	119	1

C			
VC	Port	VC	Port
119	4	579	3

D			
VC	Port	VC	Port
579	0	121	1



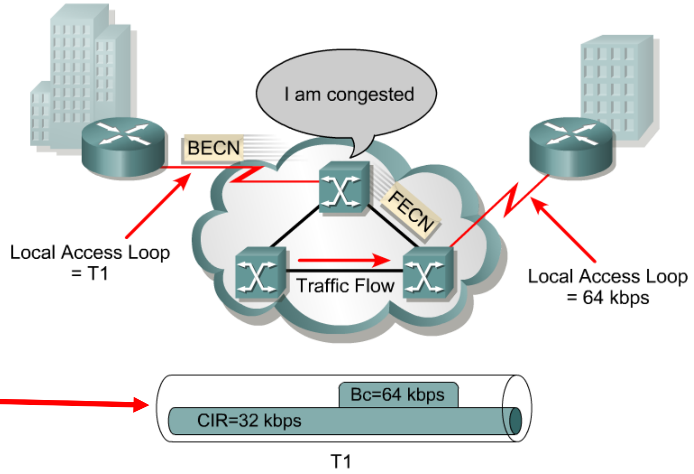
Frame Relay IETF Frame Format



- Inside the cloud, your Frame Relay provider sets up the DLCI numbers to be used by the routers for establishing PVCs.

Frame Relay bandwidth and flow control

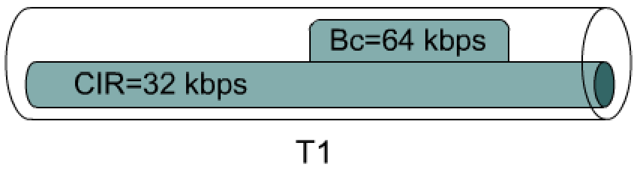
The first thing we need to do is become familiar with some of the terminology.



- **Local access rate** – This is the clock speed or port speed of the connection or local loop to the Frame Relay cloud.
    - It is the rate at which data travels into or out of the network, regardless of other settings.
- **Committed Information Rate (CIR)** – This is the rate, in bits per second, at which the Frame Relay switch agrees to transfer data.
    - The rate is usually averaged over a period of time, referred to as the **committed rate measurement interval (Tc).**

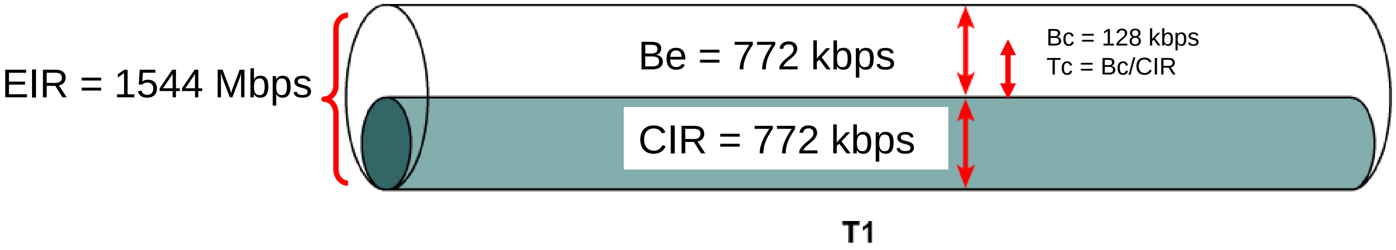
Frame Relay bandwidth and flow control

Tc = 2 seconds
Bc = 64 kbps
CIR = 32 kbps



- **Committed burst (Bc)** – The maximum number of bits that the switch agrees to transfer during any Tc.
  - The higher the Bc-to-CIR ratio, the longer the switch can handle a sustained burst.
  - The DE (Discard Eligibility) bit is set on the traffic that was received after the CIR was met. (coming)
  - (FYI) For example, if the Tc is 2 seconds and the CIR is 32 kbps, the Bc is 64 kbps.
  - (FYI) The Tc calculation is Tc = Bc/CIR.
- **Committed Time Interval (Tc)** – Tc is not a recurrent time interval. It is used strictly to measure inbound data, during which time it acts like a sliding window. Inbound data triggers the Tc interval.

Frame Relay bandwidth and flow control



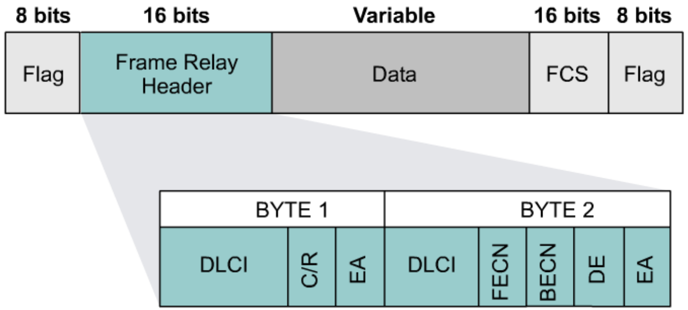
- **Excess burst (Be)** – This is the <u>maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR.</u>

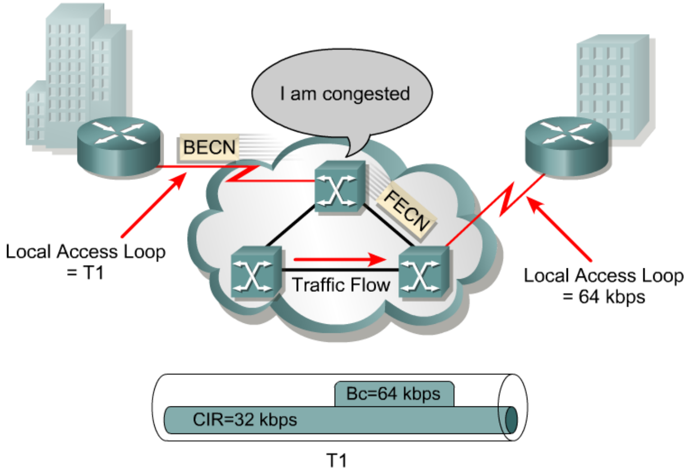
    - Excessive Burst (Be) is <u>dependent on the service offerings</u> available from your vendor, but it is <u>typically limited to the port speed of the local access loop.</u>

- **Excess Information Rate (EIR)** – This defines the <u>maximum bandwidth available to the customer, which is the CIR plus the Be.</u>

    - <u>Typically, the EIR is set to the local access rate.</u>

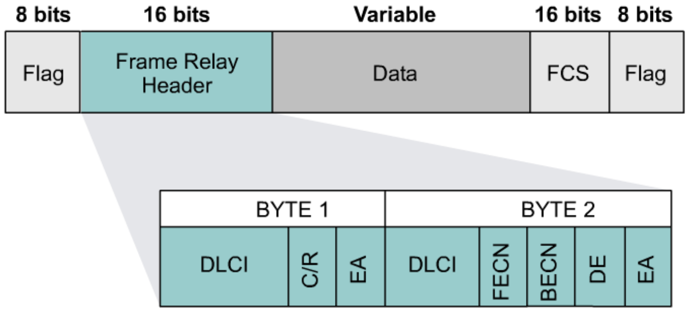
Frame Relay bandwidth and flow control

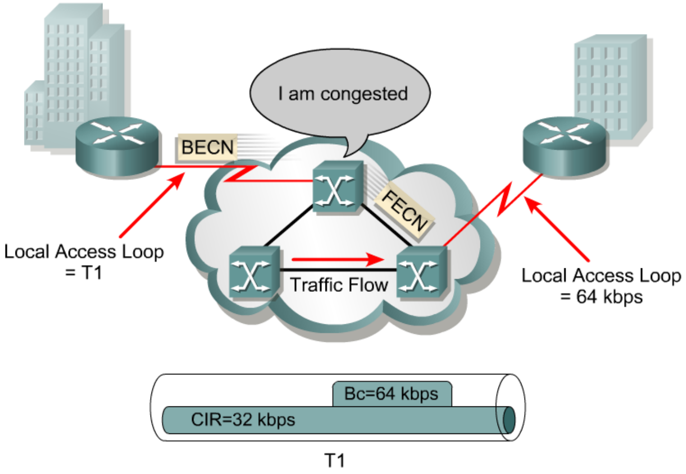




- **Forward Explicit Congestion Notification (FECN)** – When a Frame Relay switch recognizes congestion in the network, it sends an FECN packet to the destination device.
  - This indicates that congestion has occurred.
- **Backward Explicit Congestion Notification (BECN)** – When a Frame Relay switch recognizes congestion in the network, it sends a BECN packet to the source router.
  - This instructs the router to reduce the rate at which it is sending packets.
  - With Cisco IOS Release 11.2 or later, Cisco routers can respond to BECN notifications.

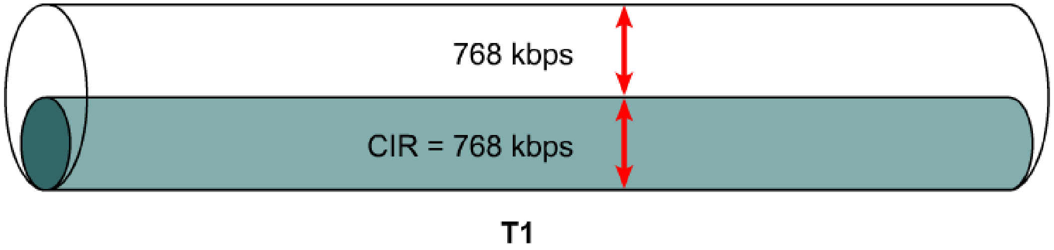
Frame Relay bandwidth and flow control





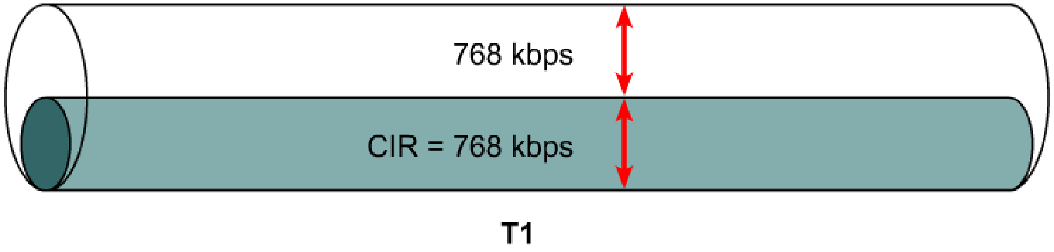
- **Discard eligibility (DE) bit** – When the router or switch detects network congestion, it can mark the packet "Discard Eligible".
  - The DE bit is set on the traffic that was received after the CIR was met.
  - These packets are normally delivered.
  - However, in periods of congestion, the Frame Relay switch will drop packets with the DE bit set first.

Frame Relay bandwidth



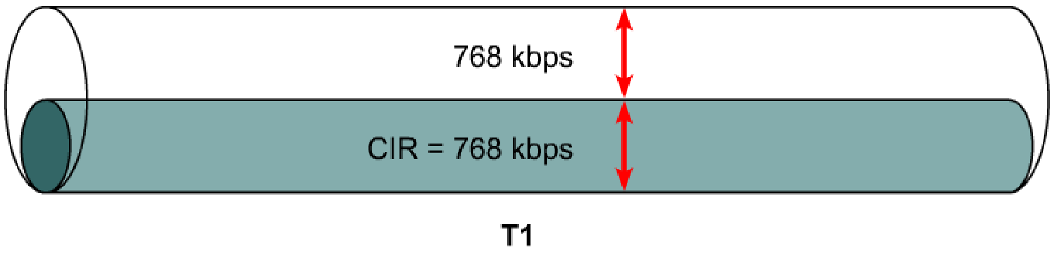
- **Several factors determine the rate** at which a customer can send data on a Frame Relay network.
  - Foremost in limiting the maximum transmission rate is the capacity of the local loop to the provider.
    - If the local loop is a T1, no more than 1.544 Mbps can be sent.
    - In Frame Relay terminology, the speed of the local loop is called the local access rate.
  - Providers use the CIR parameter to provision network resources and regulate usage.
    - For example, a company with a T1 connection to the packet-switched network (PSN) may agree to a CIR of 768 Kbps.
    - This means that the provider guarantees 768 Kbps of bandwidth to the customer's link at all times.

Frame Relay bandwidth



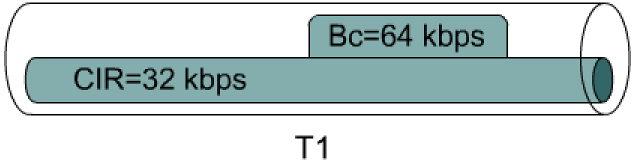
- Typically, the higher the CIR, the higher the cost of service.
- Customers can choose the CIR that is most appropriate to their bandwidth needs, as long as the CIR is less than or equal to the local access rate.
- If the CIR of the customer is less than the local access rate, the customer and provider agree on whether bursting above the CIR is allowed.
- If the local access rate is T1 or 1.544 Mbps, and the CIR is 768 Kbps, half of the potential bandwidth (as determined by the local access rate) remains available.

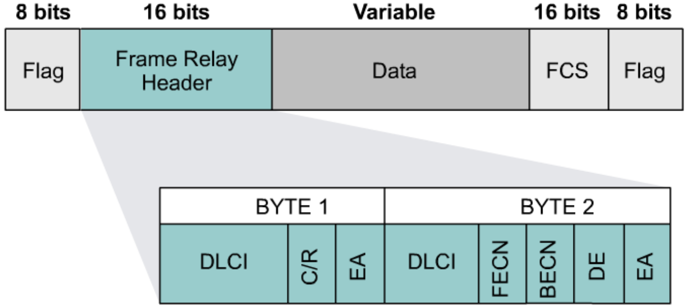
Frame Relay bandwidth



- Many providers allow their customers to purchase a CIR of 0 (zero).
- This means that the provider does not guarantee any throughput.
- In practice, customers usually find that their provider allows them to burst over the 0 (zero) CIR virtually all of the time.
- If a CIR of 0 (zero) is purchased, carefully monitor performance in order to determine whether or not it is acceptable.
- Frame Relay allows a customer and provider to agree that under certain circumstances, the customer can “burst” over the CIR.
- Since burst traffic is in excess of the CIR, the provider does not

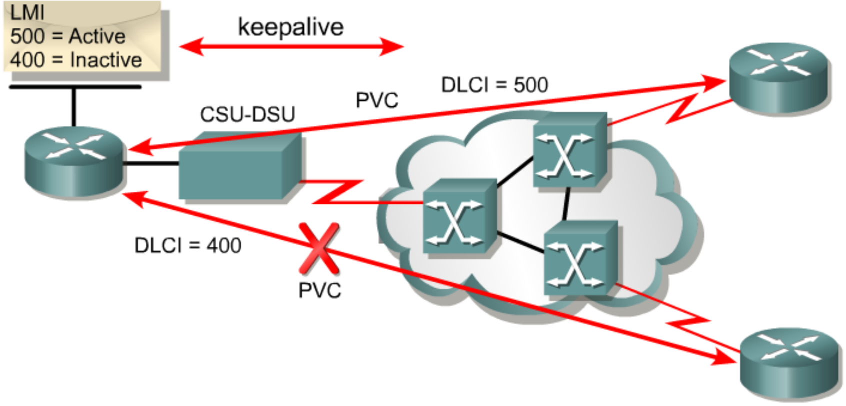
Frame Relay bandwidth





- Either a router or a Frame Relay switch tags each frame that is transmitted beyond the CIR as eligible to be discarded.
- When a frame is tagged DE, a single bit in the Frame Relay frame is set to 1.
- This bit is known as the discard eligible (DE) bit.
- The Frame Relay specification also includes a protocol for congestion notification.
- This mechanism relies on the FECN/ BECN bits in the Q.922 header of the frame.
- The provider's switches or the customer's routers can selectively set the DE bit in frames.
- These frames will be the first to be dropped when congestion occurs.

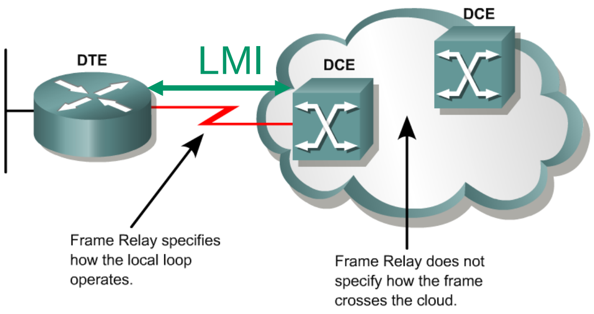
LMI – Local Management Interface



- LMI is a signaling stand
  the DTE and the Frame R
- LMI is responsible for m
  the status between devic
- LMI includes:
  - **A keepalive mechanism**, which verifies that data is flowing
  - **A multicast mechanism**, which provides the network server (router) with its local DLCI.
  - **The multicast addressing**, which can give DLCIs global rather than local significance in Frame Relay networks (not common).
  - **A status mechanism**, which provides an ongoing status on the DLCIs known to the switch

LMI

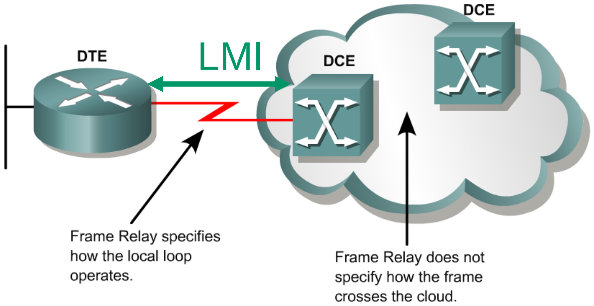
Cisco IOS Keyword	Description
ansi	Annex D defined by American National Standards Institute (ANSI) standard T1.617.
cisco	LMI type defined jointly by Cisco and three other companies.
q933a	ITU-T Q.933 Annex A.



- In order to deliver the **first LMI services** to customers as soon as possible, vendors and standards committees worked separately to develop and deploy LMI in early Frame Relay implementations.
- The **result** is that there are three types of LMI, none of which is compatible with the others.
- **Cisco, StrataCom, Northern Telecom, and Digital Equipment Corporation (Gang of Four)** released one type of LMI, while the **ANSI** and the **ITU-T** each released their own versions.
- The LMI type must match between the provider Frame Relay switch and the customer DTE device.

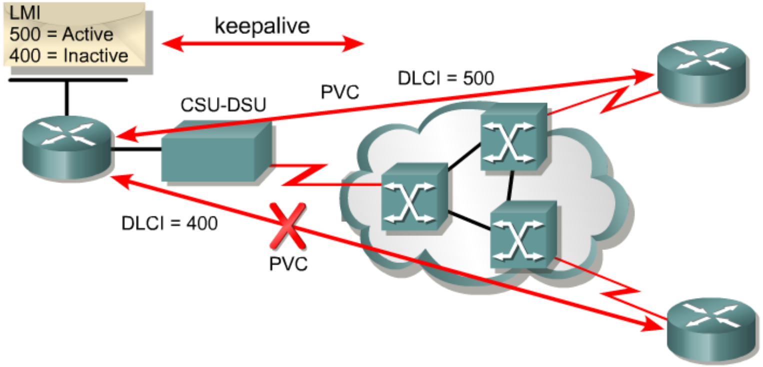
LMI

Cisco IOS Keyword	Description
ansi	Annex D defined by American National Standards Institute (ANSI) standard T1.617.
cisco	LMI type defined jointly by Cisco and three other companies.
q933a	ITU-T Q.933 Annex A.



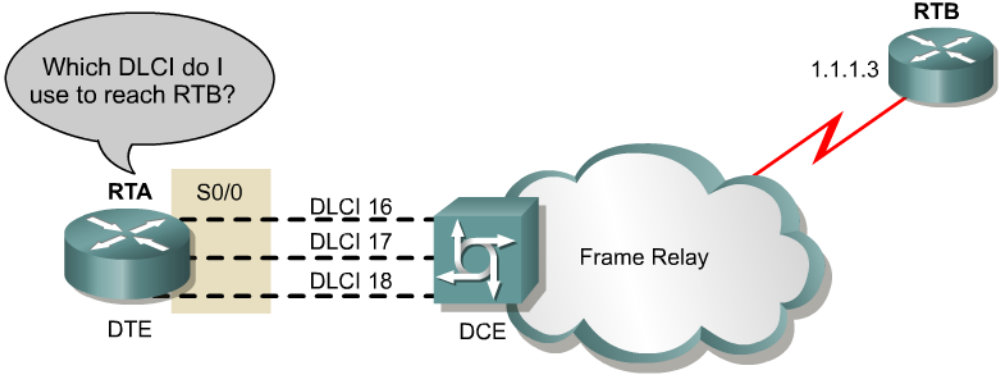
- In Cisco IOS releases **prior to 11.2**, the Frame Relay interface must be manually configured to use the correct LMI type, which is furnished by the service provider.
- If using Cisco IOS Release **11.2 or later**, the router attempts to automatically detect the type of LMI used by the provider switch.
- This automatic detection process is called **LMI autosensing**.
- No matter which LMI type is used, when LMI autosense is active, it sends out a full status request to the provider switch.

LMI



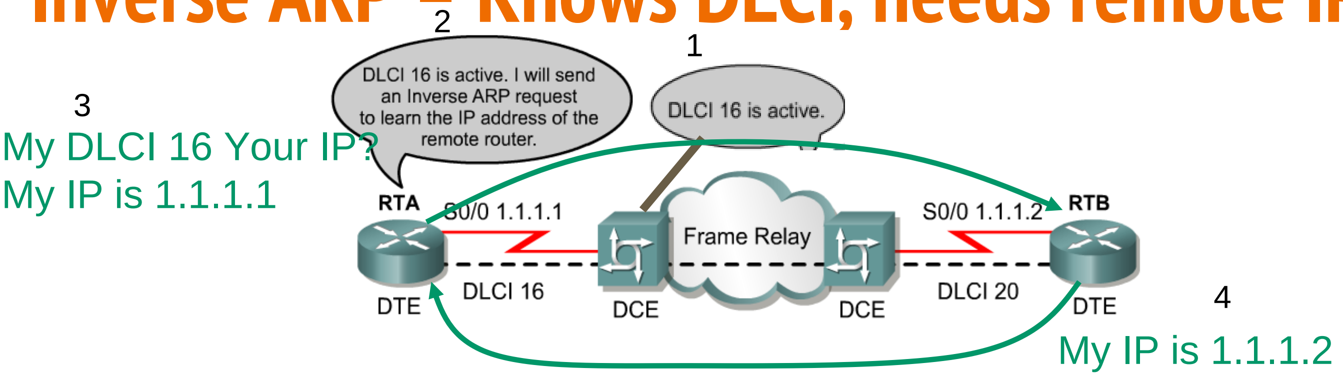
- The Frame Relay switch uses **LMI** to report the status of configured PVCs.
- The three possible PVC states are as follows:
  - **Active state** – Indicates that the connection is active and that routers can exchange data.
  - **Inactive state** – Indicates that the local connection to the Frame Relay switch is working, but the remote router connection to the Frame Relay switch is not working.
  - **Deleted state** – Indicates that no LMI is being received from the Frame Relay switch, ***or*** that there is no service

DLCI Mapping to Network Address



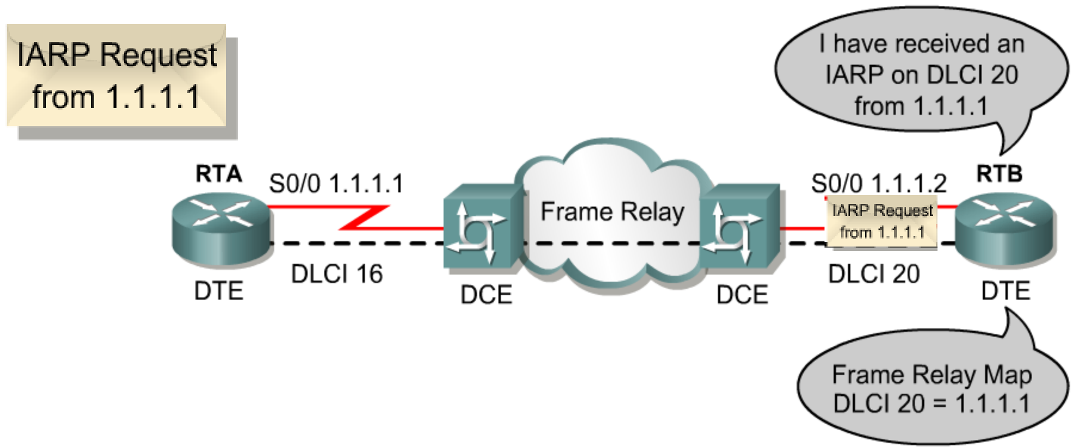
- **Manual**
  - Manual: Administrators use a **frame relay map** statement.
- **Dynamic**
  - **Inverse Address Resolution Protocol** (**I-ARP**) provides a given DLCI and requests next-hop protocol addresses for a specific connection.
  - The router then updates its mapping table and uses the information in the table to forward packets on the correct

Inverse ARP – Knows DLCI, needs remote IP



- Once the router learns from the switch about available PVCs and their corresponding DLCIs, the router can send an **Inverse ARP** request to the other end of the PVC. (*unless statically mapped – later*)
- For each supported and configured protocol on the interface, the router sends an Inverse ARP request for each DLCI. (unless statically mapped)
- In effect, the Inverse ARP request asks the remote station for its Layer 3 address.
- At the same time, it provides the remote system with the Layer 3 address of the local system.
- The return information from the Inverse ARP is then used to build the Frame Relay map.

Inverse ARP – Knows DLCI, needs remote IP



- Inverse Address Resolution Protocol (Inverse ARP) was developed to provide a mechanism for dynamic DLCI to Layer 3 address maps.
- **Inverse ARP** works much the same way Address Resolution Protocol (ARP) works on a LAN.
- However, with **ARP**, the device knows the Layer 3 IP address and needs to know the remote data link MAC address.
- With **Inverse ARP**, the router knows the Layer 2 address which is the DLCI, but needs to know the remote Layer 3 IP address.

Configuring Frame Relay maps

```
Router(config-if)#frame-relay map protocol protocol-
    address dlci [broadcast] [ietf | cisco]
```

- If the environment does not support LMI autosensing and Inverse ARP, a Frame Relay map must be manually configured.
- Use the **`frame-relay map`** command to configure static address mapping.
- Once a **static map** for a given DLCI is configured, Inverse ARP is disabled on that DLCI.
- The **`broadcast`** keyword is commonly used with the **`frame-relay map`** command.
- The **`broadcast`** keyword:
    - Forwards broadcasts when multicasting is not enabled.

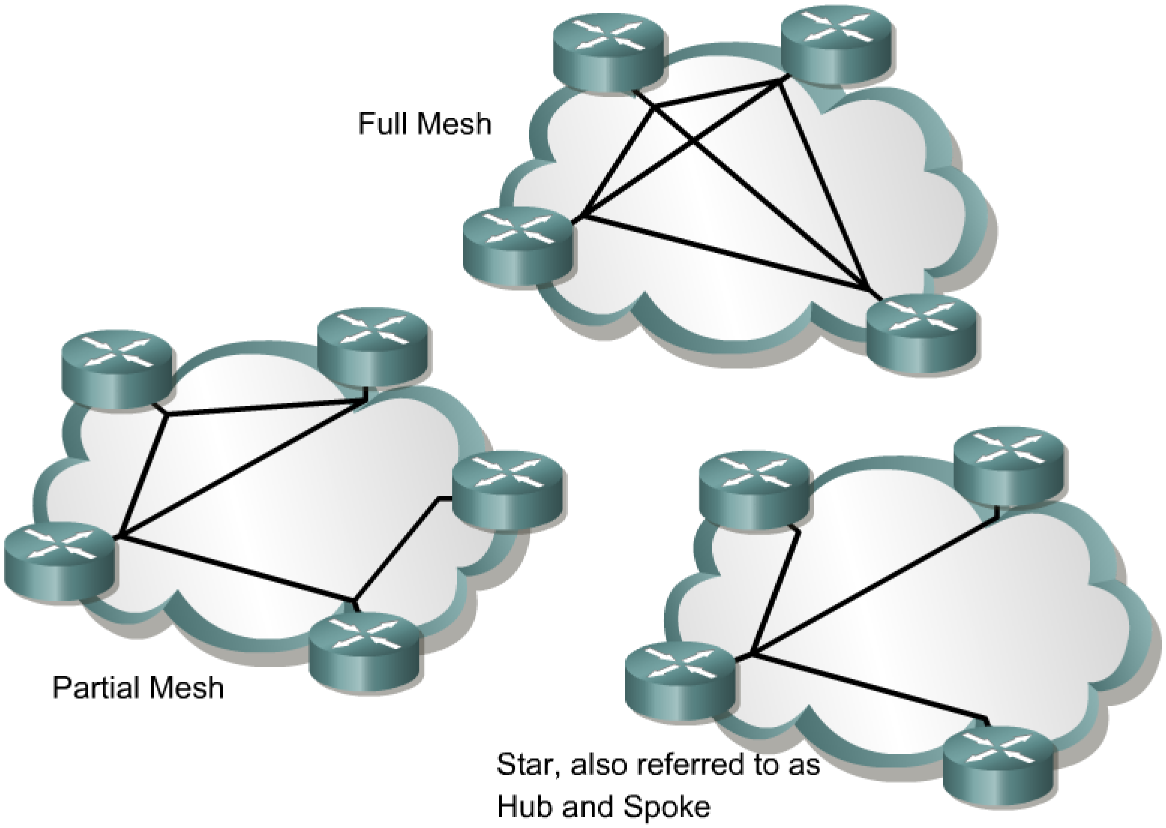
`debug frame-relay lmi` (continued)

```
1w2d: Serial0/0 (in): Status, myseq 142
1w2d: RT IE 1, length 1 type 0
1w2d: KA IE 3, length 2 yourseq 142, myseq 142
1w2d: PVC IE 0x7, length 0x6, dlci 100, status 0x2, bw0
```

FYI ONLY

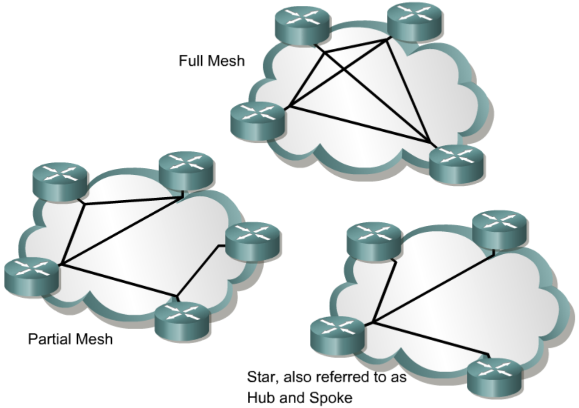
- The possible values of the status field are as follows:
- **0x0** – Added/inactive means that the switch has this DLCI programmed but for some reason it is not usable. The reason could possibly be the other end of the PVC is down.
- **0x2** – Added/active means the Frame Relay switch has the DLCI and everything is operational.
- **0x4** – Deleted means that the Frame Relay switch does not have this DLCI programmed for the router, but that it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the service provider in the Frame Relay cloud.

Frame Relay Topologies



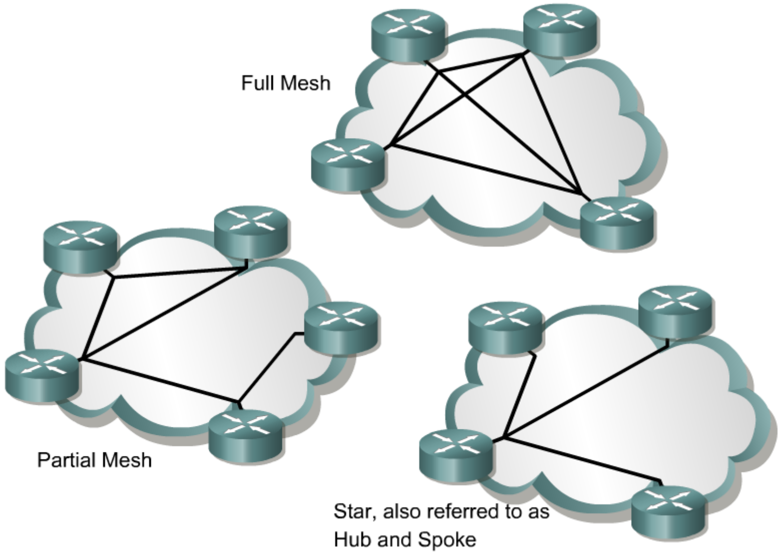
NBMA – Non Broadcast Multiple Access

Frames between two routers are only seen by those two devices (non broadcast). Similar to a LAN, multiple computers have access to the same network and potentially to each other (multiple access).



- An **NBMA network** is the opposite of a broadcast network.
- On a **broadcast network**, multiple computers and devices are attached to a shared network cable or other medium. When one computer transmits frames, all nodes on the network "listen" to the frames, but only the node to which the frames are addressed actually receives the frames. Thus, the frames are broadcast.
- A **nonbroadcast multiple access network** is a network to which multiple computers and devices are attached, but data is transmitted directly from one computer to another over a virtual circuit or across a switching fabric. The most common examples of nonbroadcast network media include ATM (Asynchronous Transfer Mode), frame relay, and X.25.
- http://www.linktionary.com/

Star Topology

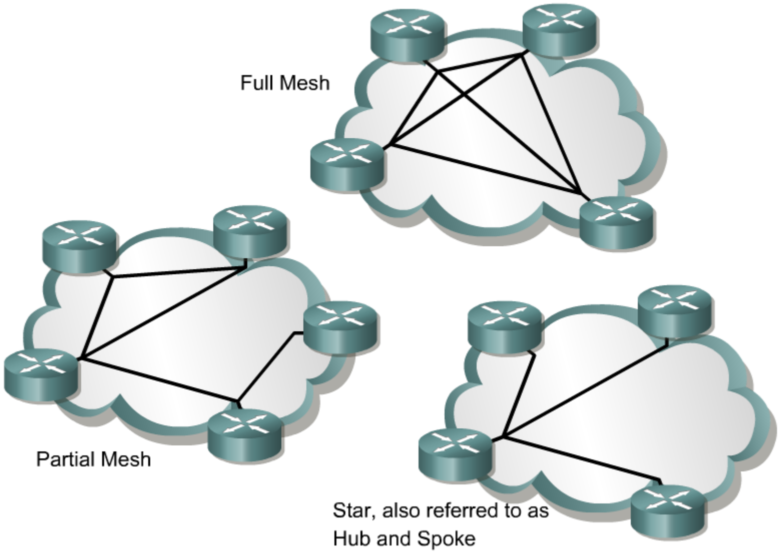


- A star topology, also known as a hub and spoke configuration, is the most popular Frame Relay network topology because it is the most cost-effective.
- In this topology, remote sites are connected to a central site that generally provides a service or application.
- This is the least expensive topology because it requires the fewest PVCs.
- In this example, the central router provides a multipoint connection, because it is typically using a single interface to interconnect multiple PVCs.

Full Mesh

Full Mesh Topology

Number of Connections	Number of PVCs
2	1
4	6
6	15
8	28
10	45

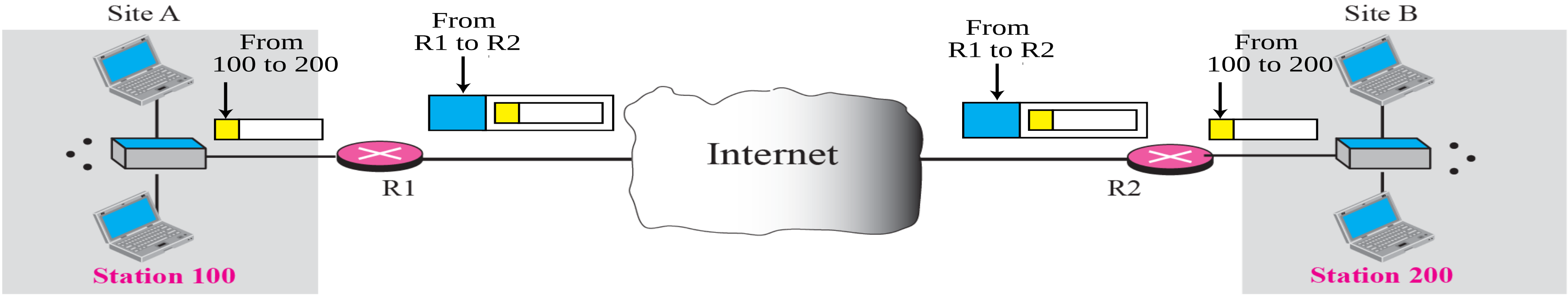


- In a full mesh topology, all routers have PVCs to all other destinations.
- This method, although more costly than hub and spoke, provides direct connections from each site to all other sites and allows for redundancy.
- For example, when one link goes down, a router at site A can reroute traffic through site C.
- As the number of nodes in the full mesh topology increases, the topology becomes increasingly more expensive.
- The formula to calculate the total number of PVCs with a fully meshed WAN is [n(n - 1)]/2, where n is the number of nodes.

VPN (Virtual Private Network)

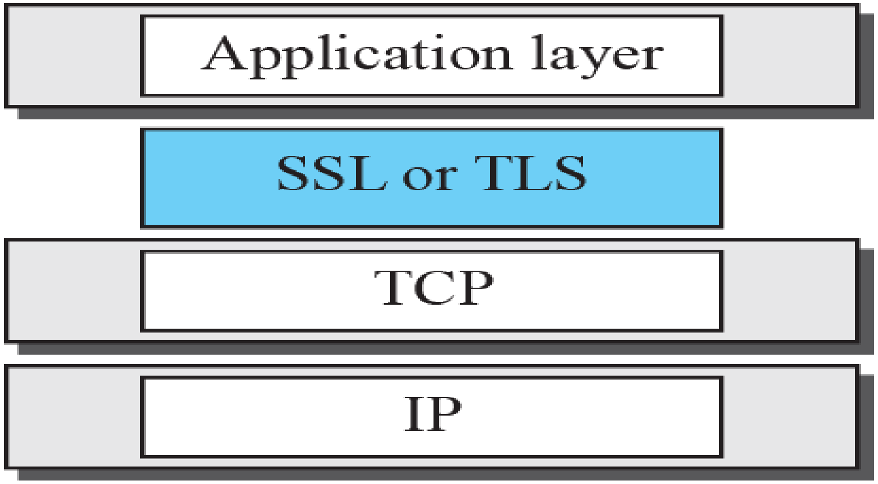
VPN (Virtual Private Network)

- VPN is a network that is private but virtual.
- It is private because it guarantees privacy inside the organization.
- It is virtual because it does not use real private WANs; the network is physically public but virtually private.
- Routers R1 and R2 use VPN
  technology to guarantee privacy for the organization.


Site A
From
100 to 200
Station 100
From
R1 to R2
R1
Internet
From
R1 to R2
R2
Site B
From
100 to 200
Station 200

TRANSPORT LAYER SECURITY

Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol. The latter is actually an IETF version of the former. We discuss SSL in this section; TLS is very similar. Figure shows the position of SSL and TLS in the Internet model.


Application layer
SSL or TLS
TCP
IP

SSL services

- SSL provides several services on data received from the application layer.
  ❑ **Fragmentation**. First, SSL divides the data into blocks of 214 bytes or less.
  ❑ **Compression.** Each fragment of data is compressed using one of the lossless compression methods negotiated between the client and server. This service is optional.
  ❑ **Message Integrity.** To preserve the integrity of data,

Key Exchange Algorithms

- To exchange an authenticated and confidential message, the client and the server each
  need a set of cryptographic secrets.
- However, to create these secrets, one pre-master secret must be established between the two parties.
- SSL defines several key-exchange
  methods to establish this pre-master secret.

Key Exchange Algorithms

- ***Encryption/Decryption Algorithms***
  The client and server also need to agree to a set of encryption and decryption algorithms.
  Hash Algorithms
  SSL uses hash algorithms to provide message integrity (message authentication). Several hash algorithms have also been defined for this purpose.
  Cipher Suite
  The combination of key exchange, hash, and

Cryptographic Parameter Generation

- To achieve message integrity and confidentiality, SSL needs six cryptographic secrets, four keys and two IVs (initialization vectors).
- The client needs one key for message authentication, one key for encryption, and one IV as original block in calculation.
- The server needs the same. SSL requires that the keys for one direction be different from
  those for the other direction.

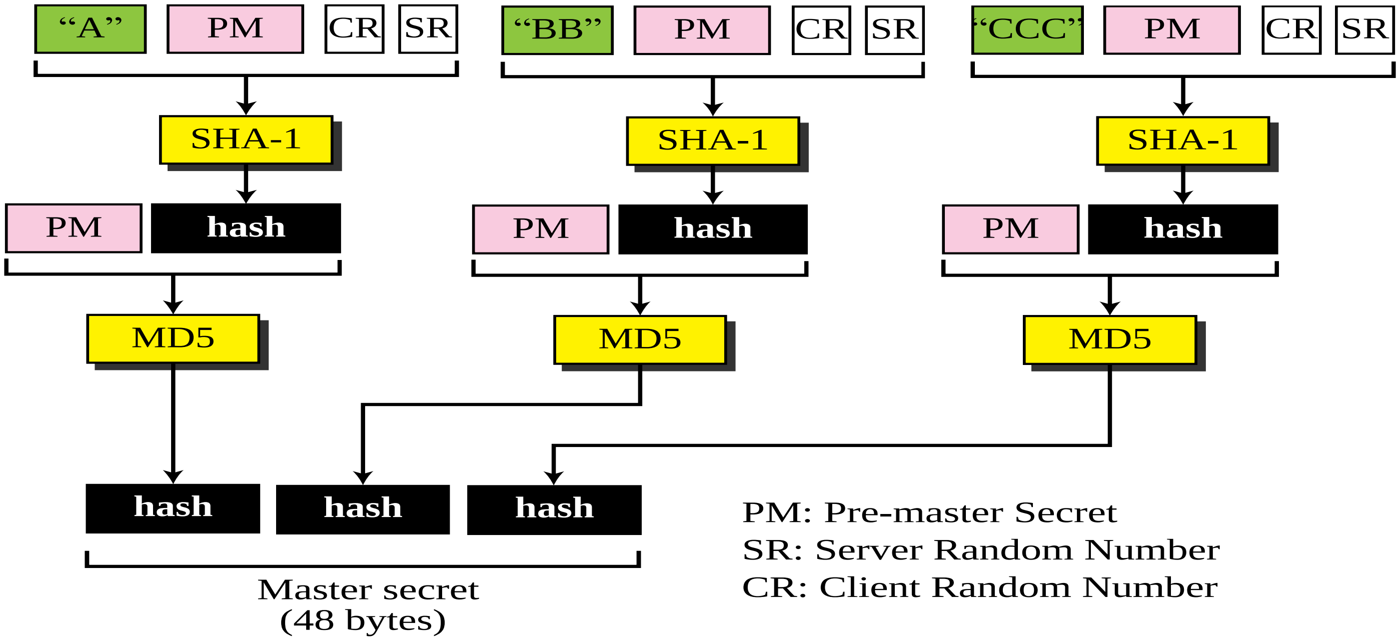
Cryptographic Parameter Generation

- 1. The client and server exchange two random numbers; one is created by the client and the other by the server
- 2. The client and server exchange one **pre-master secret** using one of the predefined key- exchange algorithms.

  3. A 48-byte **master secret** is created from the pre-master secret by applying two hash functions (SHA-1 and MD5)

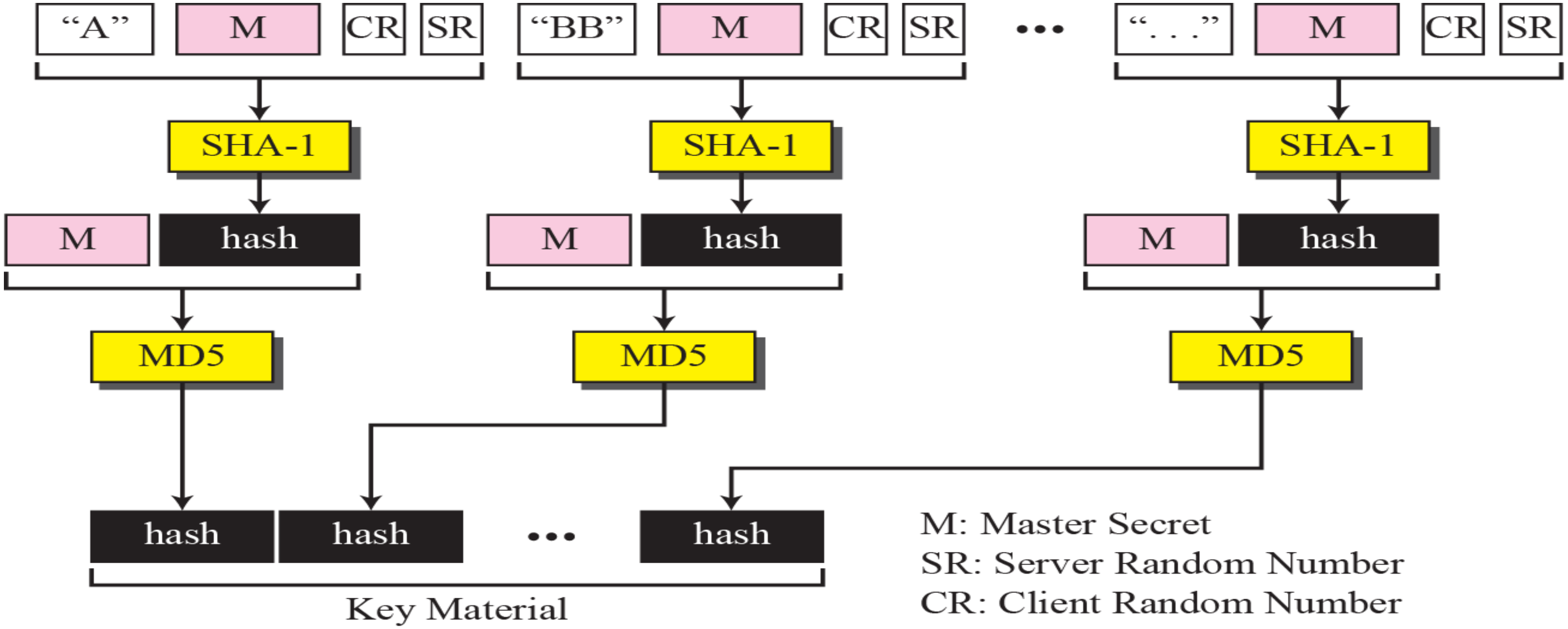
Cryptographic Parameter Generation

- **4.** The master secret is used to create variable-length **key material** by applying the
  same set of hash functions and prepending with different constants, as shown in Figure The module is repeated until key material of adequate size is created.
- 5. Six different secrets are extracted from the key material, as shown in Figure



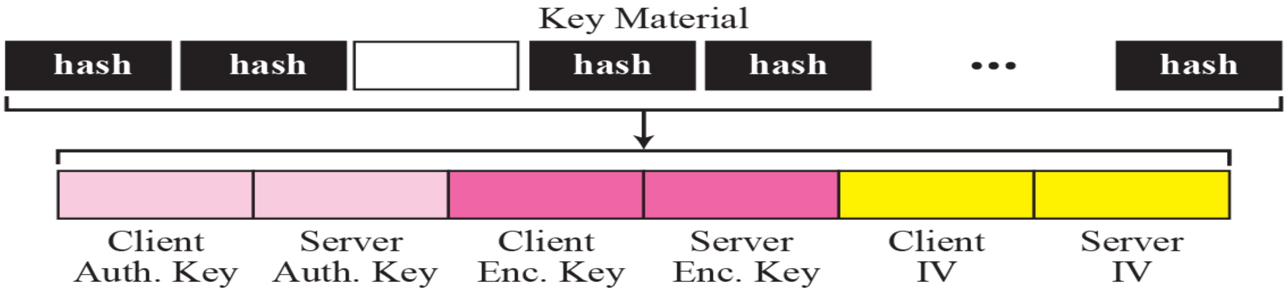
PM: Pre-master Secret
SR: Server Random Number
CR: Client Random Number

Calculation of the key materials from master secret



Extraction of cryptographic secrets from key materials

Auth. Key: Authentication Key
Enc. Key: Encryption Key
IV: Initialization Vector



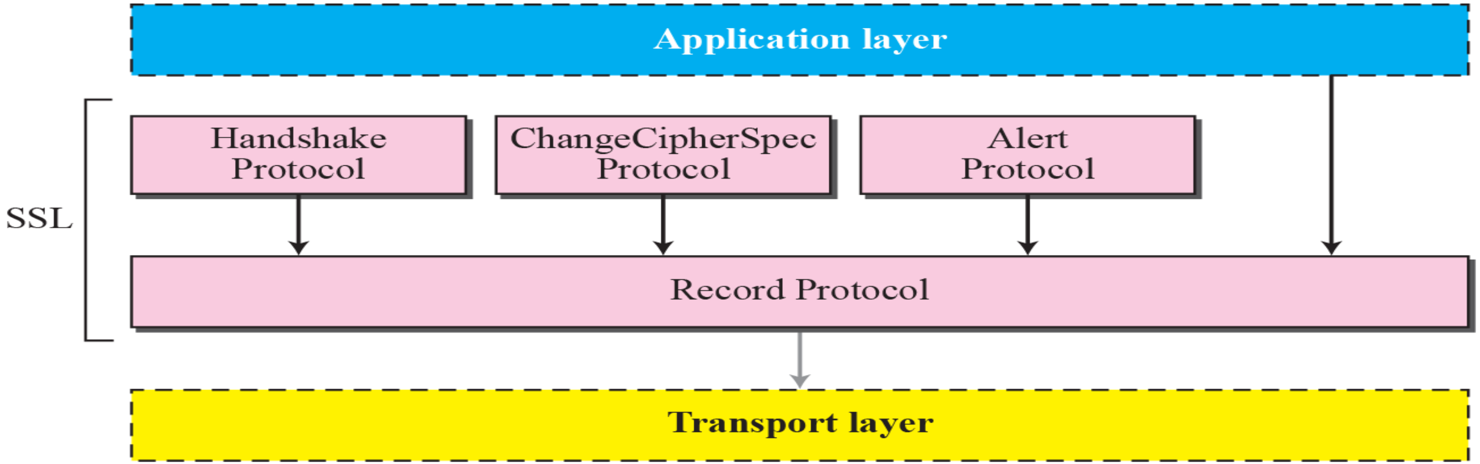
Sessions and Connections

- A session is an association between a client and a server
- A session can consist of many connections. A connection between two parties can be terminated and reestablished within the same session.
  A session can consist of many connections.
- A connection between two parties can be terminated and reestablished within the same session.

Handshake Protocol

- **Handshake Protocol** uses messages to negotiate the cipher suite, to authenticate
  the server to the client and the client to the server if needed, and to exchange information for building the cryptographic secrets.

Four SSL protocols




Client
Server
Phase I
Establishing Security Capabilities
Server authentication and key exchange
Phase II
Phase III
Client authentication and key exchange
Finalizing the Handshake Protocol
Phase IV

Phase I: Establishing Security Capability

- In Phase I, the client and the server announce their security capabilities and choose those that are convenient for both.
- In this phase, a session ID is established and the cipher suite is chosen. The parties agree upon a particular compression method.
- Finally, two random numbers are selected, one by the client and one by the server, to be used for creating a master secret as we saw before.

Note

After Phase I, the client and server know the version of SSL, the cryptographic algorithms, the compression method, and the two random numbers for key generation.

Phase II: Server Key Exchange and Authentication

- In Phase II, the server authenticates itself if needed.
- The sender may send its certificate, its public key, and may also request certificates from the client.

Note

After Phase II, the server is authenticated to the client, and
the client knows the public
key of the server if required.

Phase III is designed to authenticate the client.

- Phase III is designed to authenticate the client.

Note

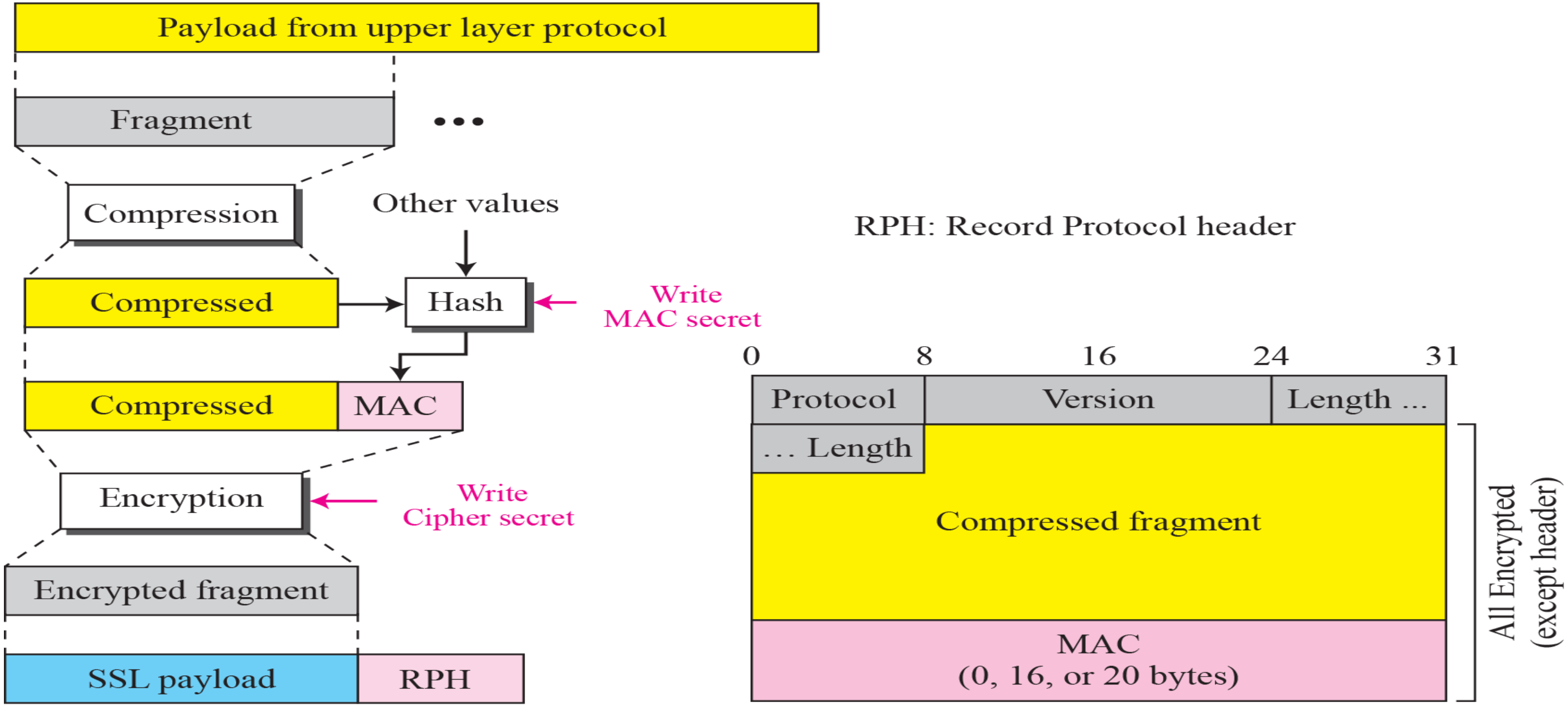
After Phase III, The client is authenticated for the serve, and both the client and the server know the pre-master secret.

Phase IV: Finalizing and Finishing

- In Phase IV, the client and server send messages to change cipher specification and to finish the handshaking protocol

Record Protocol

- The **Record Protocol** carries messages from the upper layer (Handshake Protocol,ChangeCipherSpec Protocol, Alert Protocol, or application layer).
- The message is fragmented and optionally compressed; a MAC is added to the compressed message using the negotiated hash algorithm.



a. Process

b. Encapsulation

Asynchronous Transfer Mode

ATM

ATM Features

- Cell relay protocol.
- Works along with SONET to provide high speed interconnection.
- Designed by ATM Forum and adopted by ITU-T.

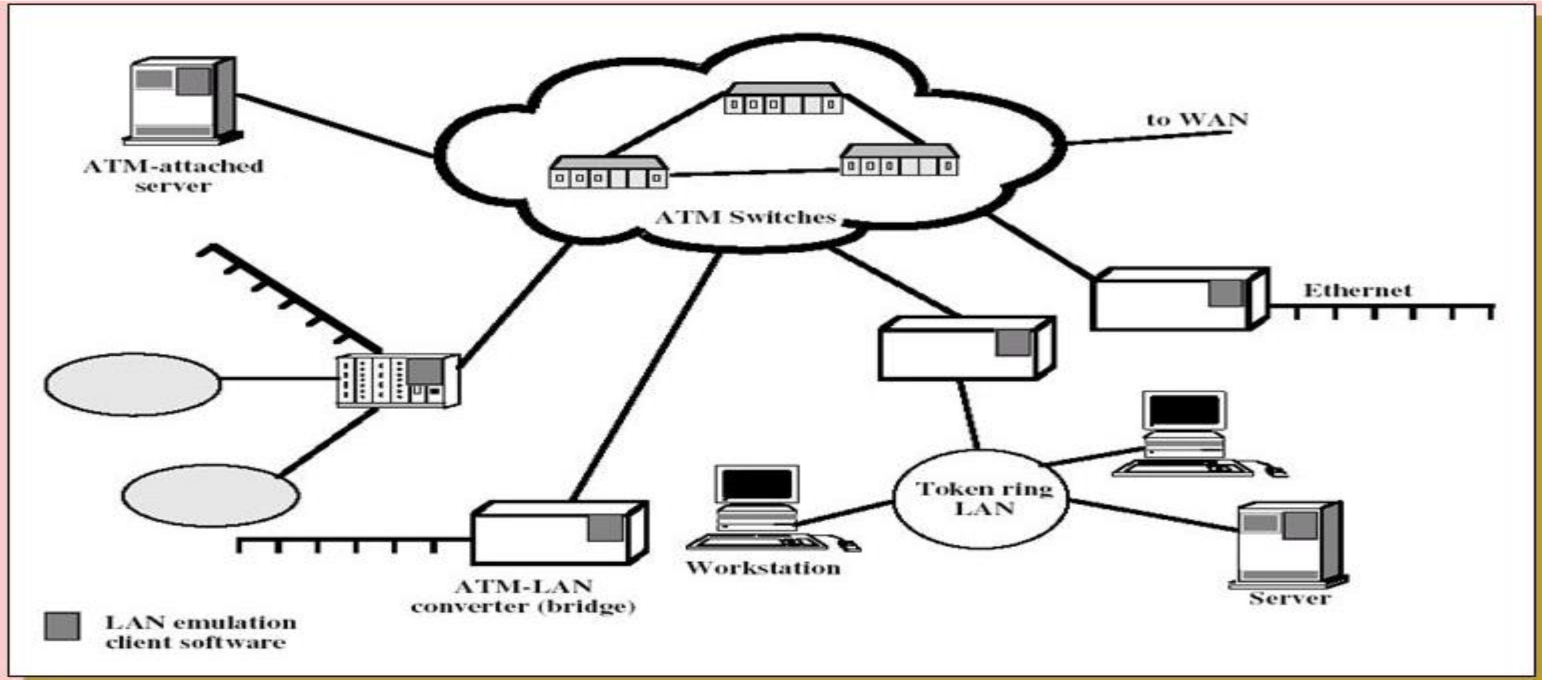
ATM

- Destined to replace most existing WAN technologies
- Improves on performance of Frame Relay
- 53-byte cells of fixed size=48 byte data+5 header
- The standard-sized cells allow switching mechanisms to achieve faster switching rates
- Rates of 155 – 622 Mbps are achieved with theoretical rates up to 1.2 Gbps
- Compatible with twisted-pair, coax, and fiber
- ATM uses Asynchronous Time Division Multiplexing
- Allows any-speed and even variable rate connection

Issues Driving LAN Changes

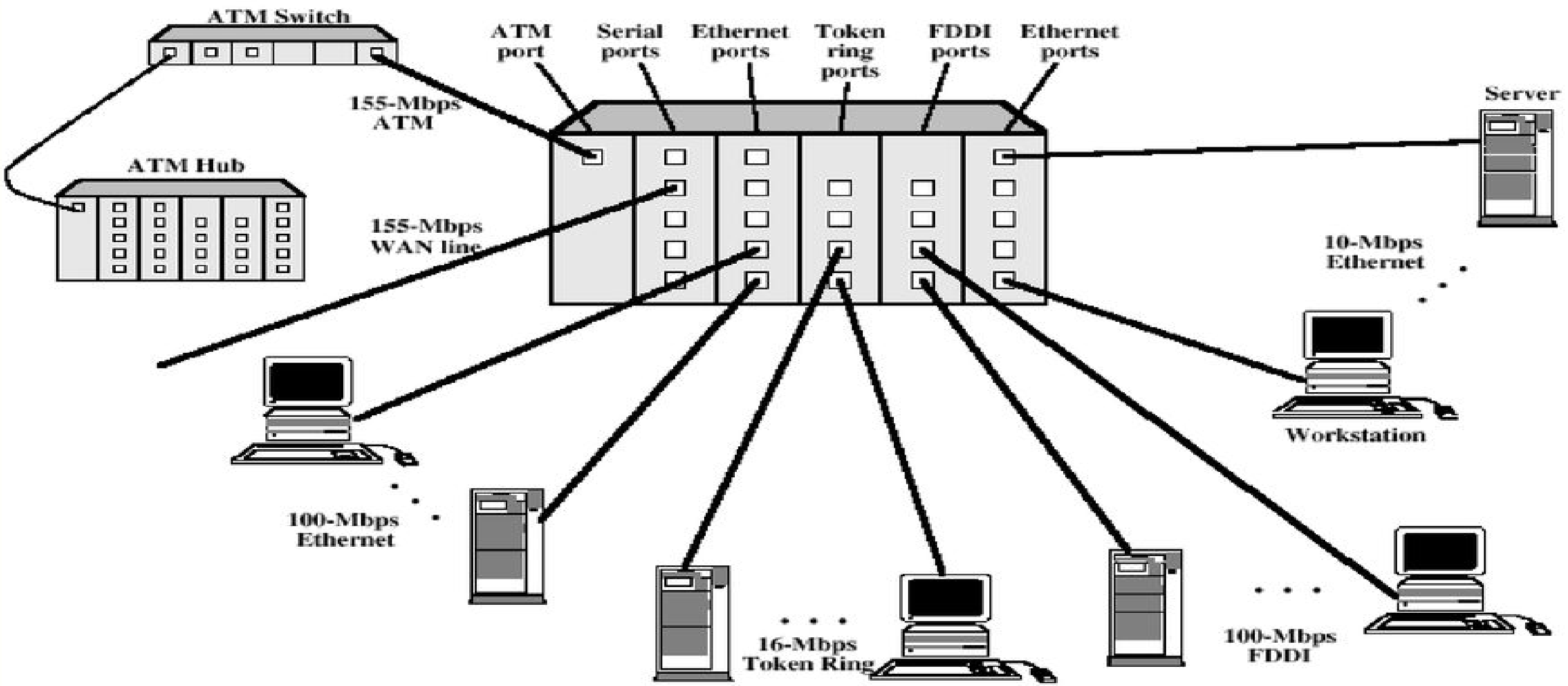
- Traffic Integration
  - Voice, video and data traffic
  - *Multimedia* became the ‘buzz word’
    - One-way batch — Web traffic
    - Two-way batch — voice messages
    - One-way interactive — Mbone broadcasts
    - Two-way interactive — video conferencing
- Quality of Service guarantees (e.g. limited jitter, non-blocking streams)

ATM LAN



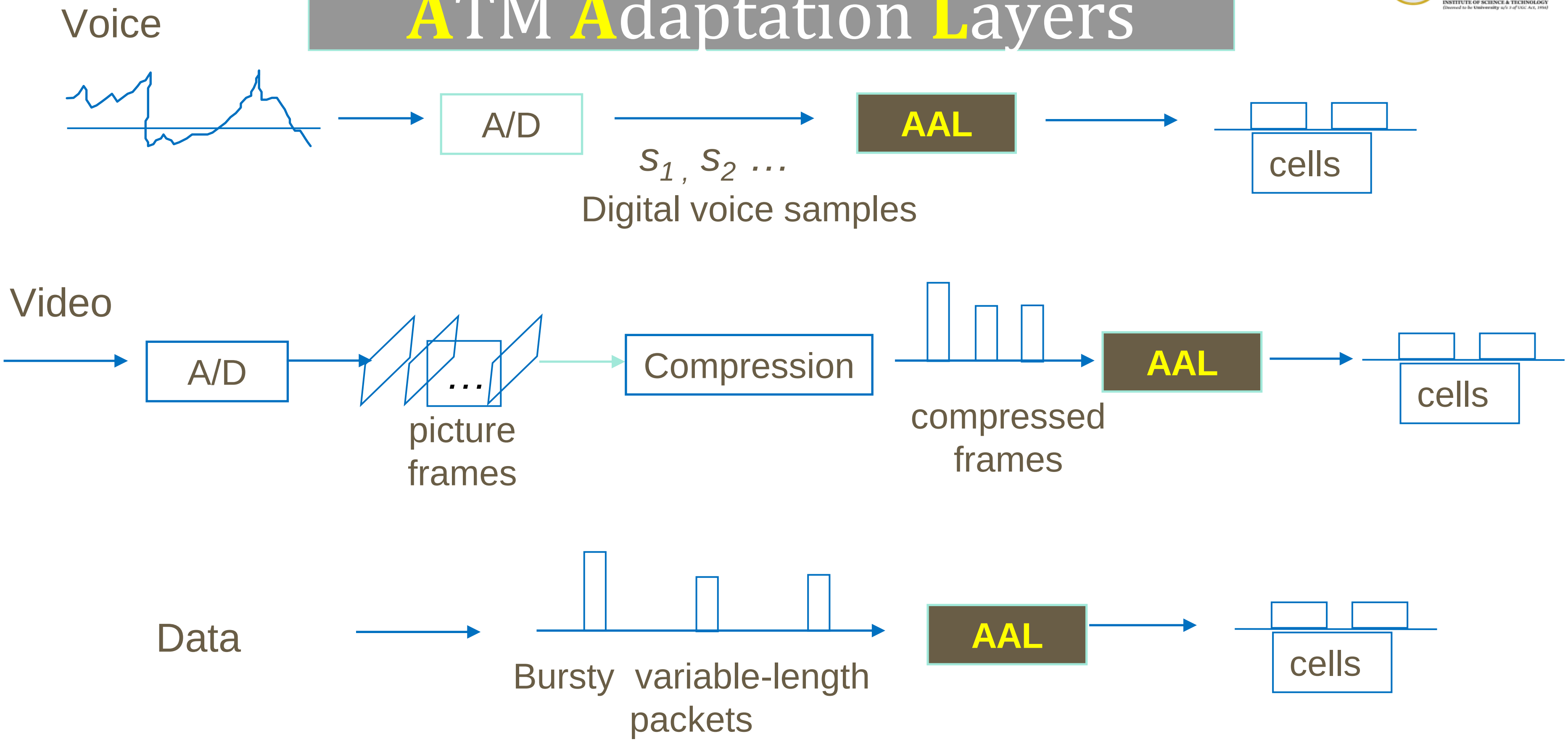
Source: William stallings, Data and computer communications, Eigth edition

ATM LAN Hub configuration



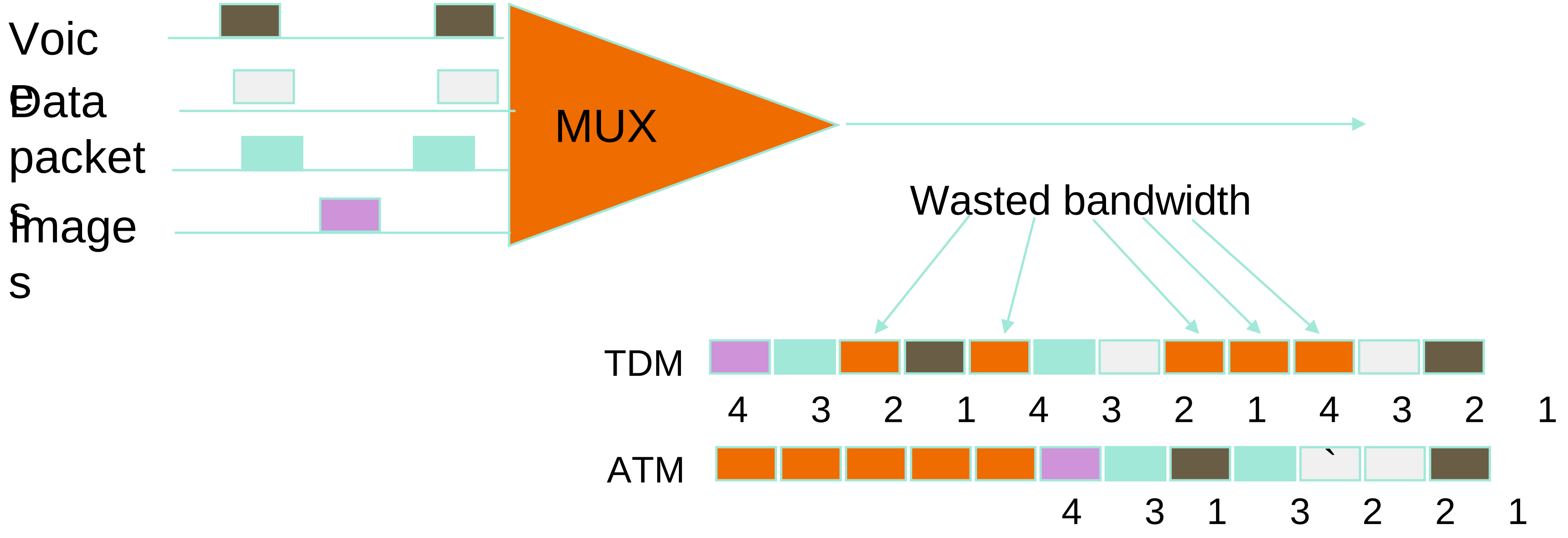
Source: William stallings, Data and computer communications, Eigth edition

ATM Adaptation Layers



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

Asynchronous Transfer Mode (ATM)

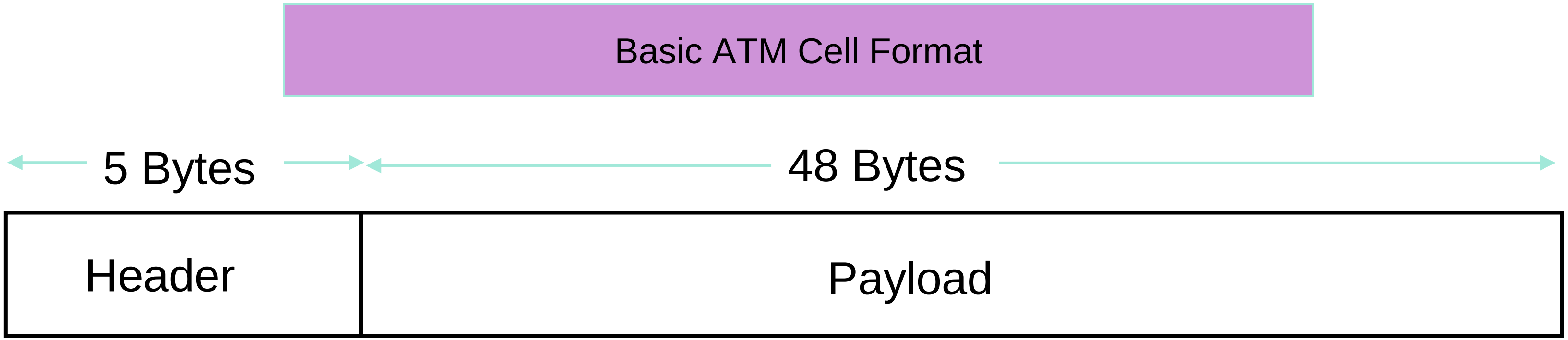


Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

ATM

- ATM standard (defined by CCITT) is widely accepted by common carriers as mode of operation for communication – particularly BISDN.

- ATM is a form of <u>cell switching</u> using small fixed-sized packets.



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

ATM Conceptual Model Assumptions

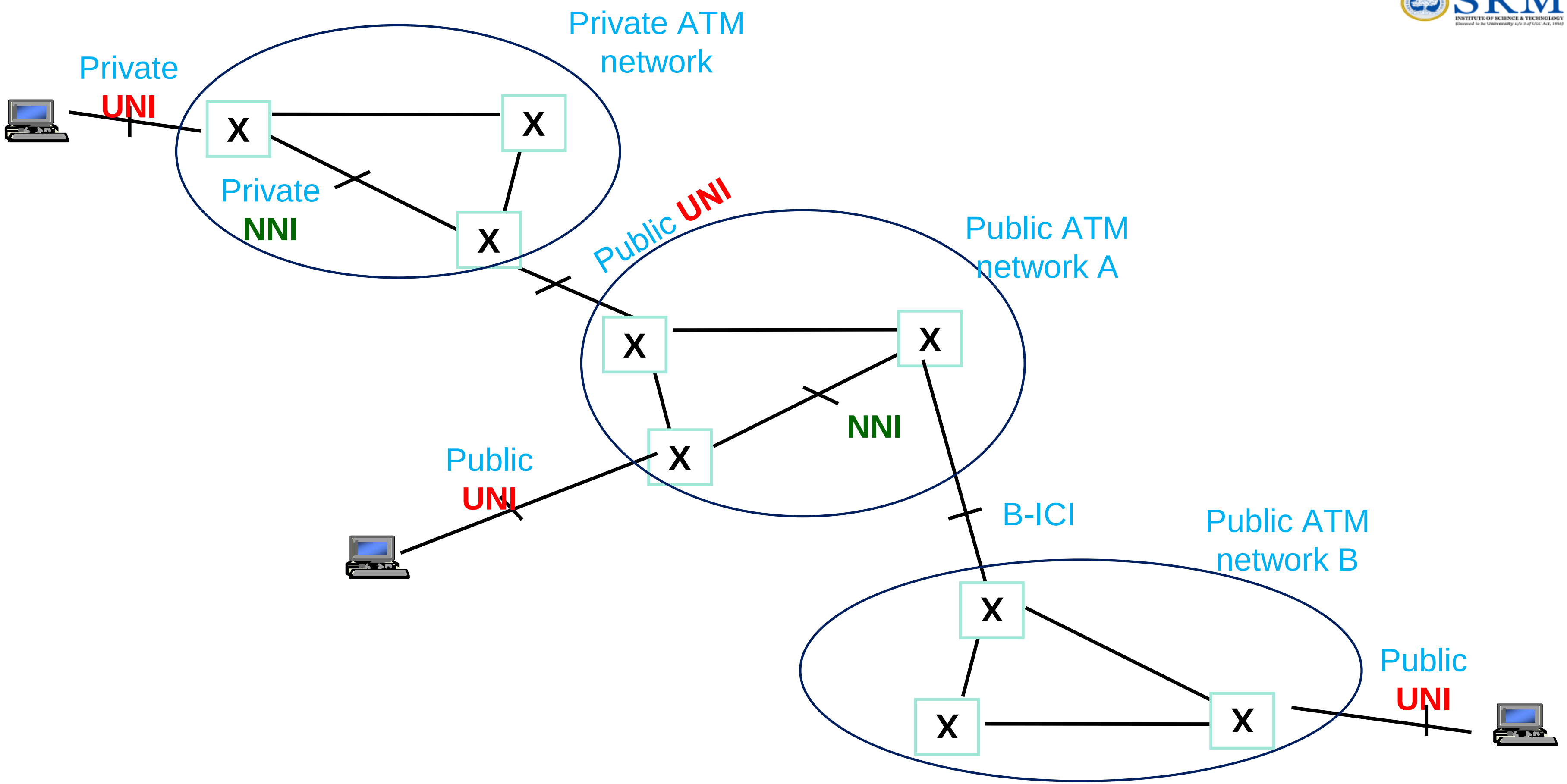
1. ATM network will be organized as a hierarchy.

   User's equipment connects to networks via a **UNI** (User-Network Interface).

   Connections between provided networks are made through **NNI** (Network-Network Interface).

2. ATM will be connection-oriented.

   A connection (an ATM channel) must be established before any cells are sent.



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

ATM Connections

- two levels of ATM connections:

  virtual path connections

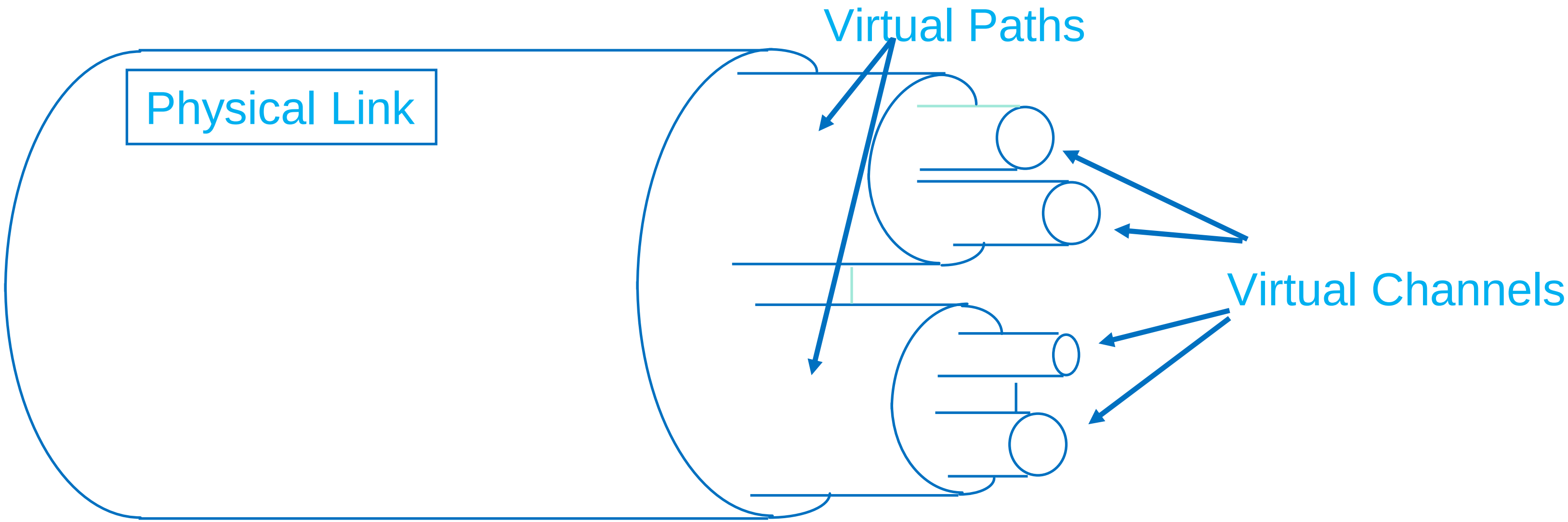
  virtual channel connections

- indicated by two fields in the cell header:

  virtual path identifier (**VPI**)

  virtual channel identifier(**VCI**)

ATM Virtual Connections



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

ATM Conceptual Model Assumptions (cont.)

3. Vast majority of ATM networks will run on optical fiber networks with extremely low error rates.
4. ATM must support low cost attachments.

- This decision lead to a significant decision – to prohibit cell reordering in ATM networks.

➔ ATM switch design is more difficult.

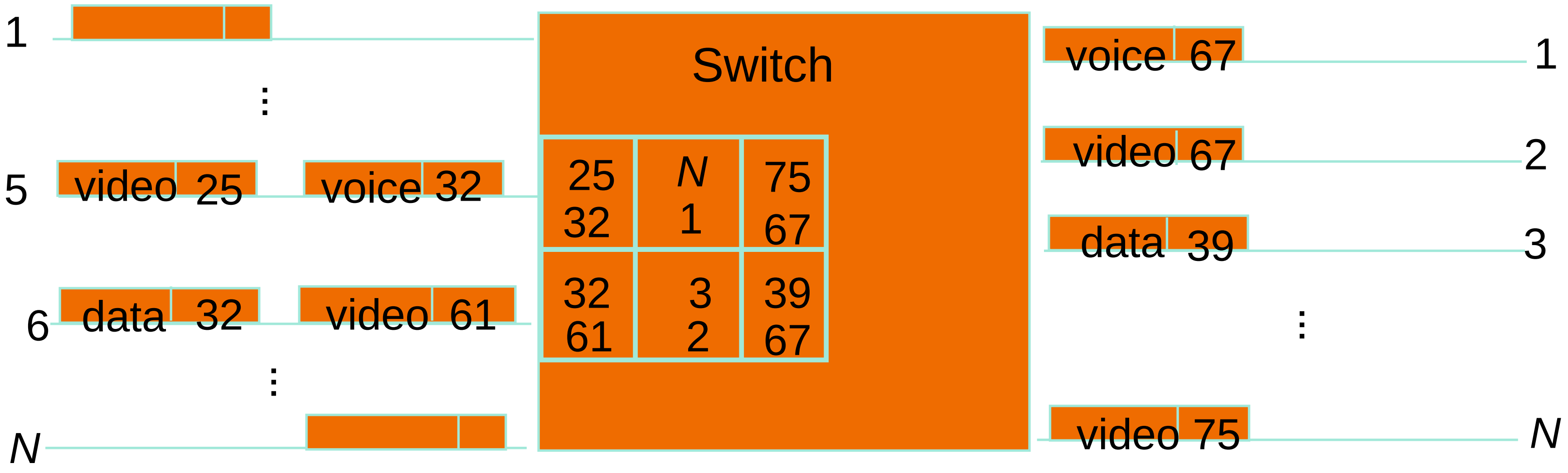
UNI Cell Format

ATM cell header

GFC (4 bits)	VPI (4 bits)	
VPI (4 bits)	VCI (4 bits)	
VCI (8 bits)		
VCI (4 bits)	PT (3 bits)	CLP (1 bit)
HEC (8 bits)		
Payload (48 bytes)		

- **GFC(Generic Flow Label):**
    - primary function of this header is the physical access control, it is often used to reduce cell jitters in CBR services, assign fair capacity for VBR services, and to control traffic for VBR flows.
    - VPI/VCI-identification numbers, so that the cells belonging to the same connection can be distinguished
    - PT-Payload TYpe
    - CLP(Cell Loss Priority)-whether the corresponding byte is to be discarded during network congestion
    - HEC(Header Error Control) is a CRC byte for the cell header field and is used for sensing and correcting cell errors and in delineating the cell header.

ATM Cell Switching



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

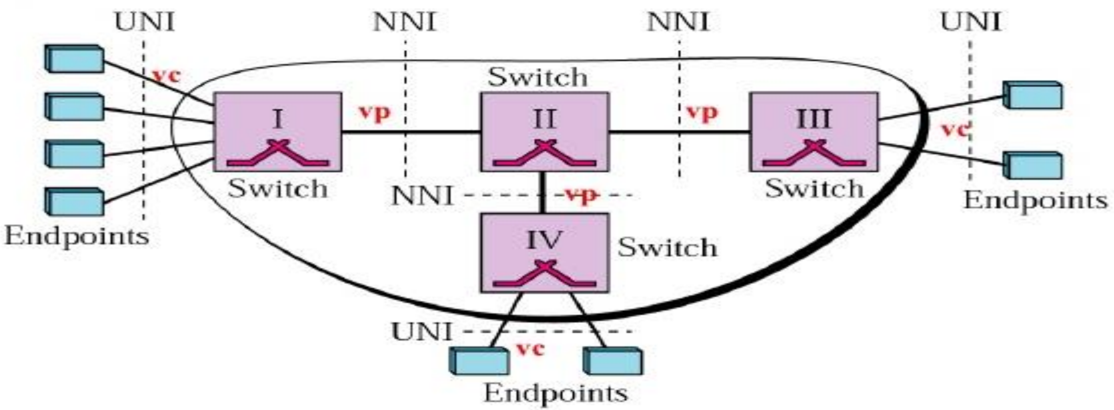
ATM Protocol Architecture

- ATM Adaptation Layer (AAL) – the protocol for packaging data into cells is collectively referred to as AAL.

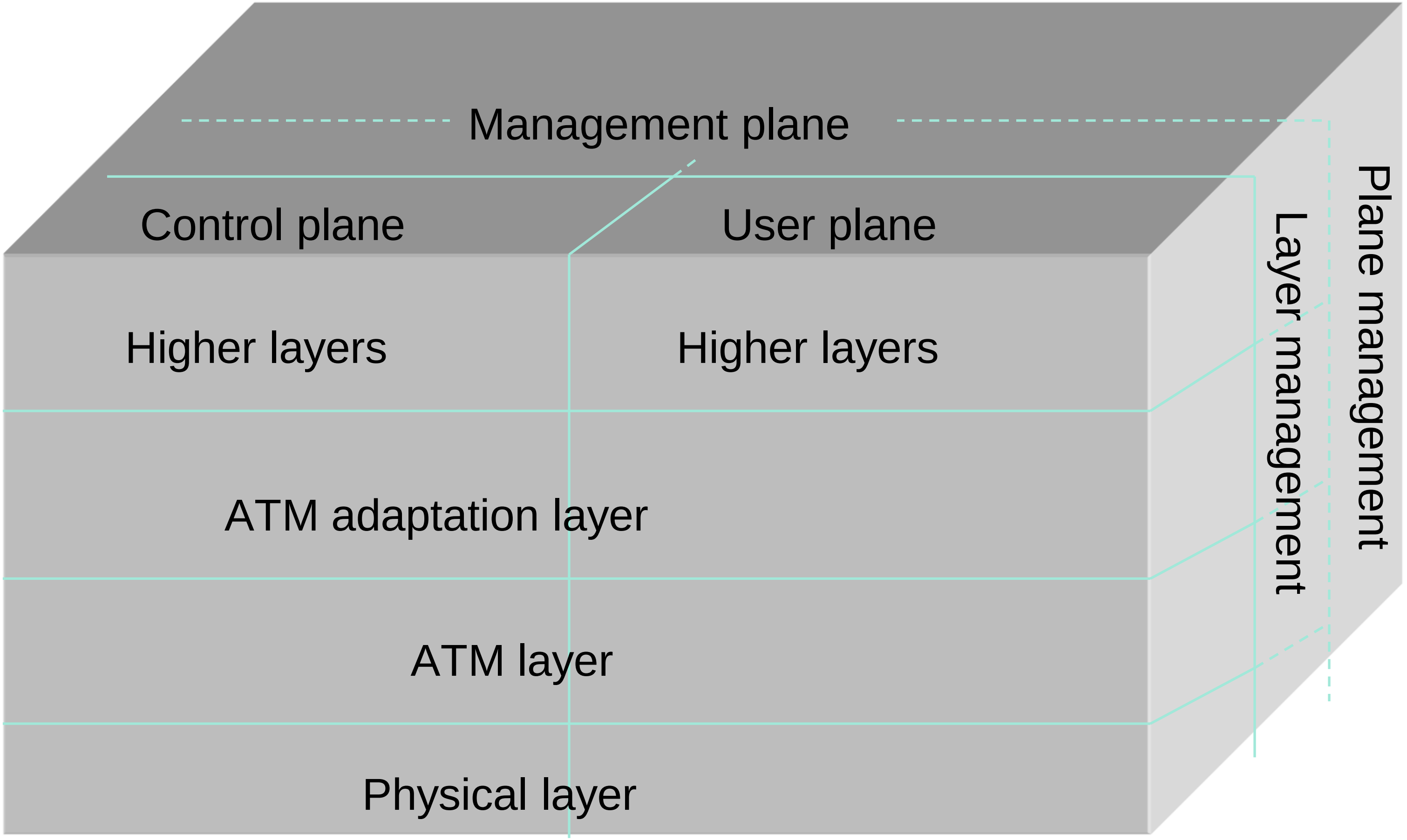
- Must efficiently package higher level data such as voice samples, video frames and datagram packets into a series of cells.

Design Issue: How many adaptation layers should there be?

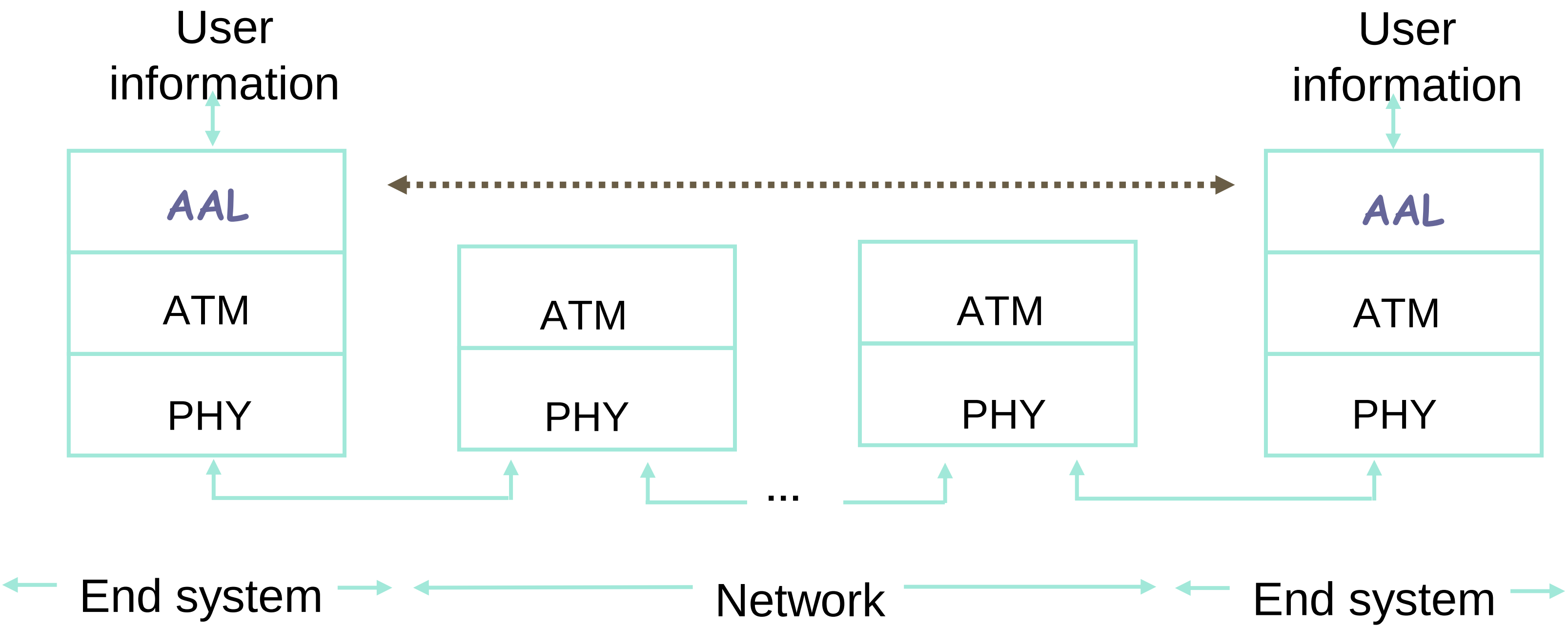
ATM Network Architecture



Source: Behrouz Forouzan, Data communication and networking, 5th Edition,2006



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

- AAL-How to break application messages to cells.
- The ATM Layer –
  - Transmission/Swiching/Reception
  - Congestion Control/Buffer management
  - Cell header generation/removal at source/destination
  - Reset connection identifiers for the next hop (at switch)
  - Cell address translation
  - Sequential delivery

Original ATM Architecture

- CCITT envisioned four classes of applications (A-D) requiring four distinct adaptation layers (1-4) which would be *optimized* for an application class:

A. Constant bit-rate applications CBR

B. Variable bit-rate applications VBR

C. Connection-oriented data applications

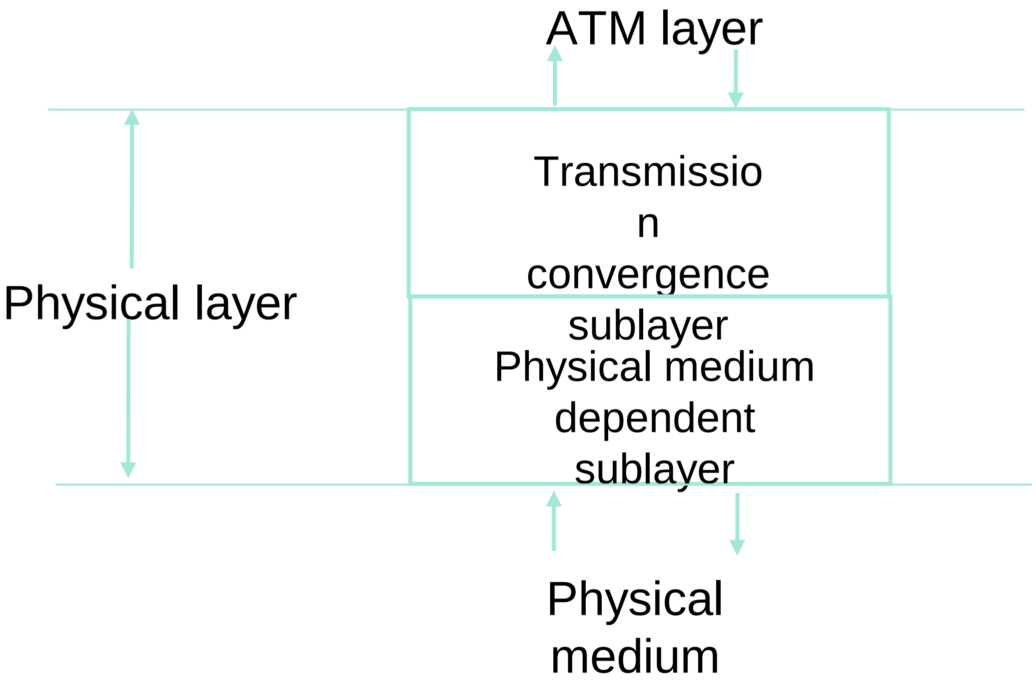
D. Connectionless data application

ATM Architecture

An AAL is further divided into:

The **Convergence Sublayer (CS)** manages the flow of data to and from SAR sublayer.

The **Segmentation and Reassembly Sublayer (SAR)** breaks data into cells at the sender and reassembles cells into larger data units at the receiver.



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

Original ATM Architecture

- The AAL interface was initially defined as classes **A-D** with SAP (service access points) for **AAL1-4.**
- **AAL3** and **AAL4** were so similar that they were merged into **AAL3/4.**
- The data communications community concluded that **AAL3/4** *was not suitable* for data communications applications. They pushed for standardization of **AAL5 (also referred to as SEAL – the Simple and Efficient Adaptation Layer).**
- **AAL2 was not *initially* deployed.**

Revised ATM Service Categories

Class	Description	Example
CBR	Constant Bit Rate	T1 circuit
RT-VBR	Real Time Variable Bit Rate	Real-time videoconferencing
NRT-VBR	Non-real-time Variable Bit Rate	Multimedia email
ABR	Available Bit Rate	Browsing the Web
UBR	Unspecified Bit Rate	Background file transfer

QoS, PVC, and SVC

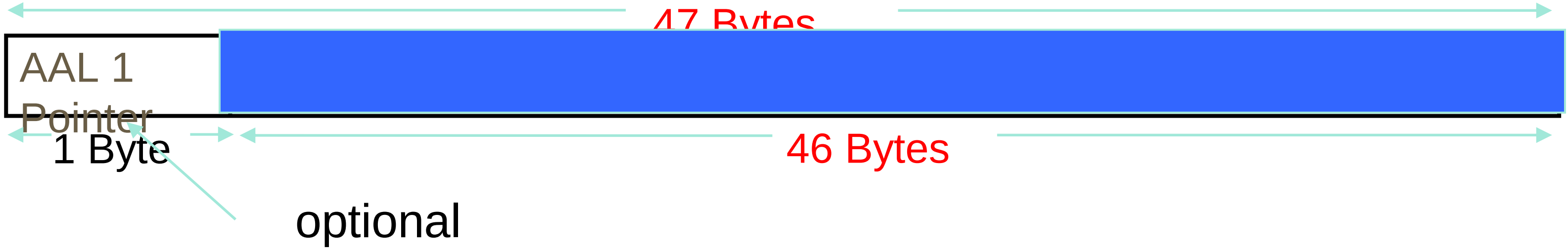
- Quality of Service (QoS) requirements are handled at connection time and viewed as part of *signaling.*
- ATM provides permanent virtual connections and switched virtual connections.
    - Permanent Virtual Connections (**PVC**)

      permanent connections set up *manually* by network manager.
    - Switched Virtual Connections (SVC)

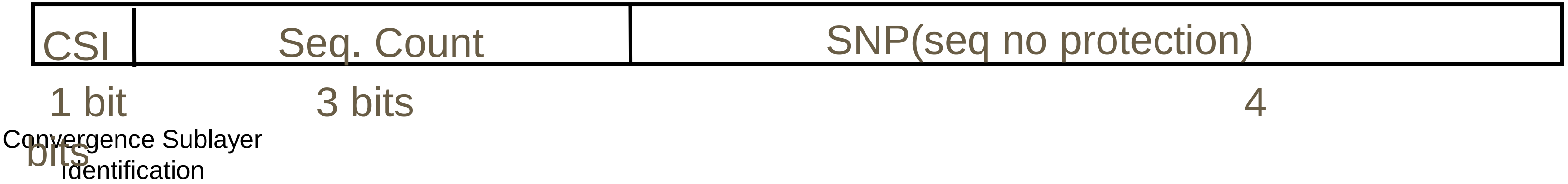
      set up and released *on demand* by the end user via signaling procedures.

AAL 1 Payload

(b) CS PDU with pointer in structured data transfer

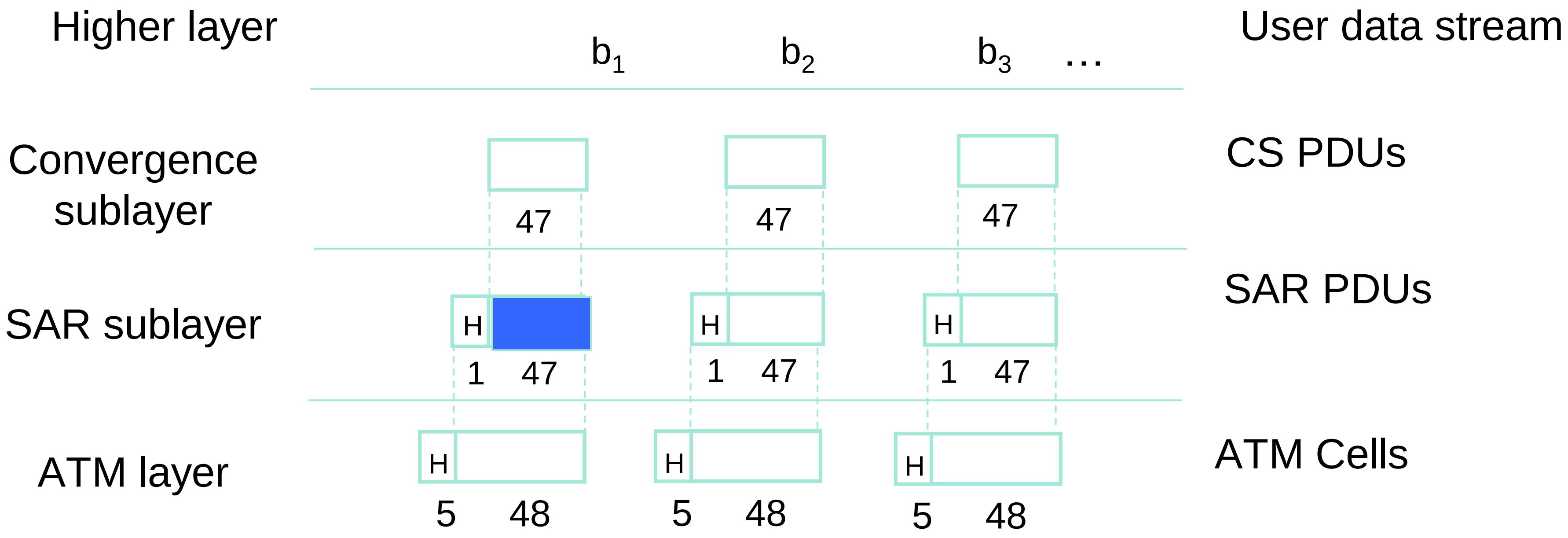


(a) SAR PDU header



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

AAL 1



Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

AAL 3/4

Common Part Indicator	Begin Tag	Buffer Allocation Size	Payload	PAD	Align ment	End Tag	Len-gth
1B	1B	2B	0-9188B	0-3B	1B	1B	2B

- Cell Format

Segment Type	Seq No	Multiplexing ID	Payload	Length Indicator	CRC
2b	4b	10b	44B	6b	10b

AAL 3/4
CS and SAR PDUs

(a) CPCS-PDU format

Header / Trailer

CPI	Btag	BASize	CPCS - PDU Payload	Pad	AL	Etag	Length
1	1	2	1 - 65,535	0-3	1	1	2

(bytes) (bytes) (bytes)

(b) SAR PDU format

Header (2 bytes) / Trailer (2 bytes)

ST	SN	MID	SAR - PDU Payload	LI	CRC
2	4	10	44	6	10

(bits) (bytes) (bits)

Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

AAL 5

Convergent Sublayer Format

Information	Pad	UU	CPI	Length	CRC
0 - 65,535 (bytes)	0-47	1	1	2	4

(bytes)

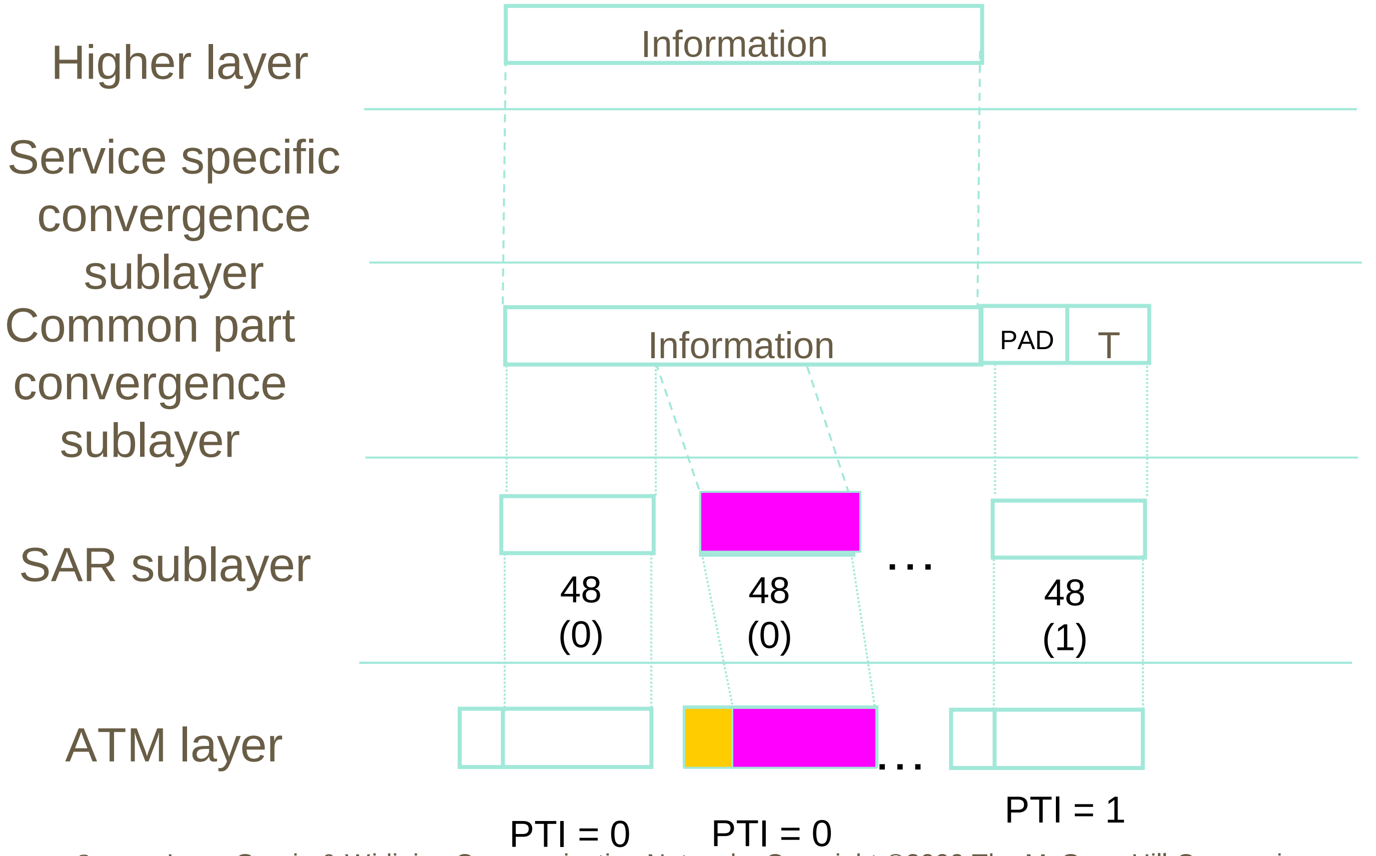
SAR Format

ATM Header	48 bytes of Data

1-bit end-of-datagram field (PTI)

Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

AAL 5



Assume null

Source: Leon-Garcia & Widjaja: Communication Networks Copyright ©2000 The McGraw Hill Companies

Thank you

Point to Point Protocol

Unit-5

PPP- Point to Point Protocol

PPP

The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The **Point-to-Point Protocol (PPP**) was designed to respond to this need.

PPP is comprised of three main components:

A method for encapsulating multi-**protocol** datagrams.

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

A family of **Network** Control **Protocols** (NCPs) for establishing and configuring different **network**-layer **protocols**)

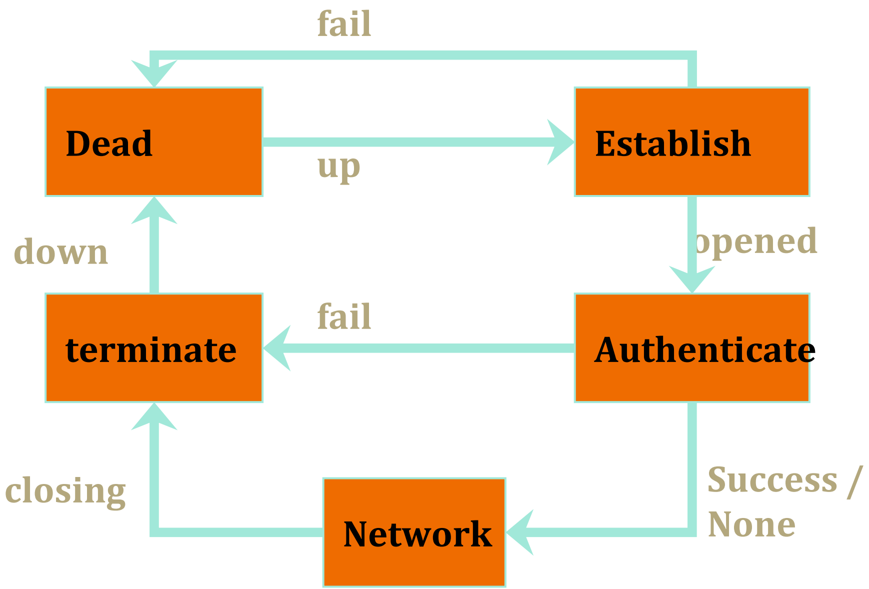
PPP – design principles

- Support multiple network protocols
- Link configuration
- Error detection
- Establishing network addresses
- Authentication
- Extensibility

PPP – a protocol

- PPP relies on another DLP –
  - **HDLC** – to perform some basic operations
- After the initial handshake, PPP executes its own handshake
- PPP itself consists of two protocols:
  - **LCP** – Link Control Protocol
  - **NCP** – Network Control Protocol

PPP state machine



PPP STATES

- Dead
- Establish
- Authenticate
- Network
- terminate

PPP state machine

1.DEAD:It means that the link is not being used .

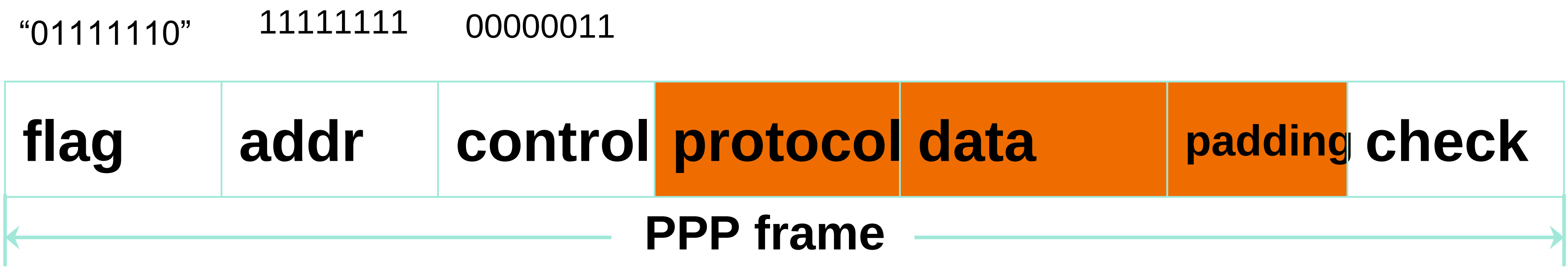
2.ESTBLISHING:-When one of the end machine starts the communication, the connection goes into the establishing state.

3.AUTHENATICATING:-The user sends the authenticate request packet & includes the user name & password.

4.NETWORKING:-The exchange of user control and data packets can started.

5.TERMINATING:-The users sends the terminate the link. With the reception of the terminate.

PPP – Frame Format



PPP – Frame Format

1. **Flag field.** The flag field identifies the boundaries of a PPP frame. Its value is 01111110.

2. **Address field.** Because PPP is used for a point-to-point connection, it uses the broadcast address used in most LANs, 11111111, to avoid a data link address in the protocol.

3. **Control field.** The control field is assigned the value 11000000 to show that, as inmost LANs, the frame has no sequence number; each frame is independent.

4. **Protocol field.** The protocol field defines the type of data being carried in the datafield: user data or other information.

5. **Data field.** This field carries either user data or other information.

6. **FCS.** The frame check sequence field is simply a 2-byte or 4-byte CRC used for error detection.

Link Control Protocol (LCP)

- **Purposes**
  - Link establishment
  - Link maintenance
  - Link termination
- **Optional operations**
  - Link quality determination
  - Authentication

Link Control Protocol (LCP)- Packets

- There are 3 classes of LCP packets:
  - **Link configuration**
    configure-request, configure-ack,
    configure-nak & configure-reject
  - **Link termination**
    terminate-request & terminate-ack
  - **Link monitoring**
    code-reject, protocol-reject, echo-request,
    echo-reply & discard-request

Link Control Protocol (LCP)- Packets Format

PPP frame	code	ID	length	Data	PPP frame

- **Code** – type of LCP packet (configure-ack etc`)
- **ID** – request-response matching ID
- **Length** – of the LCP packet
- **Data** – the LCP packet

Link Control Protocol (LCP)- Options

- MRU determination
- Magic number selection
- Authentication Protocol
- Escaped characters map

Network Control Protocol(NCP)

- **Purpose**

  Configuring the network layer protocol.

  There exists a separate NCP for each

  network layer protocol
- **Negotiation process**

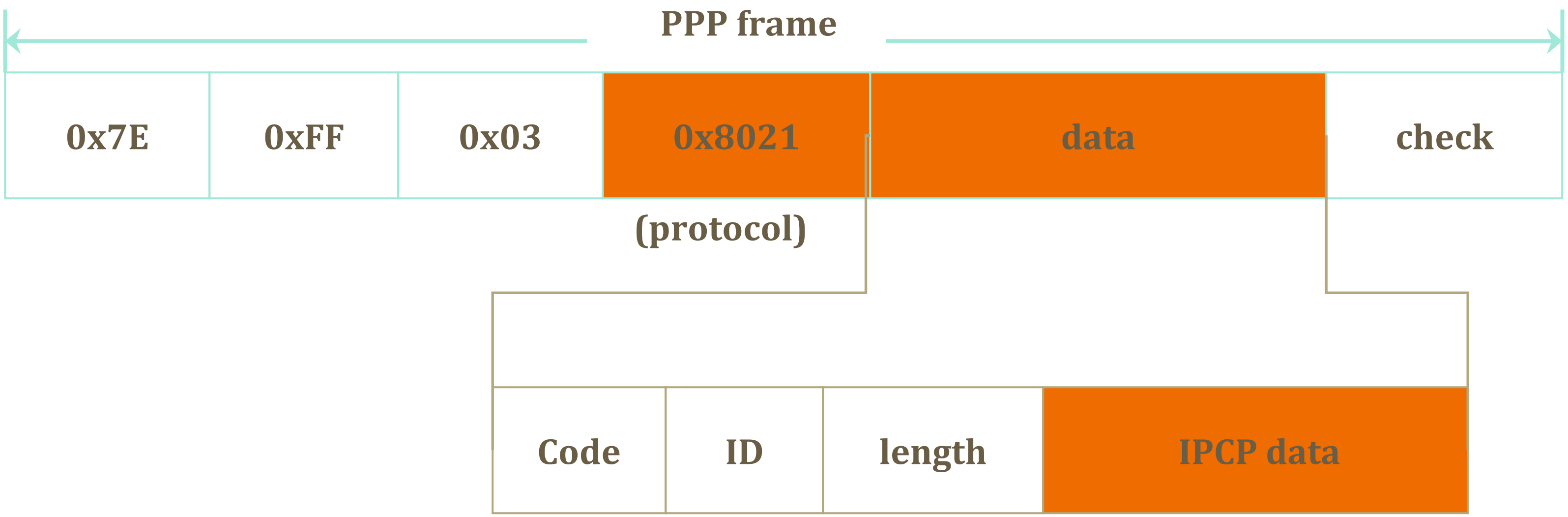
  Same message formats, code numbers

  and state machines as LCP

IPCP – IP Control Protocol

- **Purpose**
  - TCP/IP matching NCP
  - Establishes, configures and terminates the TCP/IP network layer protocol
- **Options**
  - IP-Compression protocol – I.e Van-Jacobson (VJ) compressed TCP/IP
  - IP address – allows dynamic IP configuration
  - DNS & NBNS address(NetBIOS Name Server)

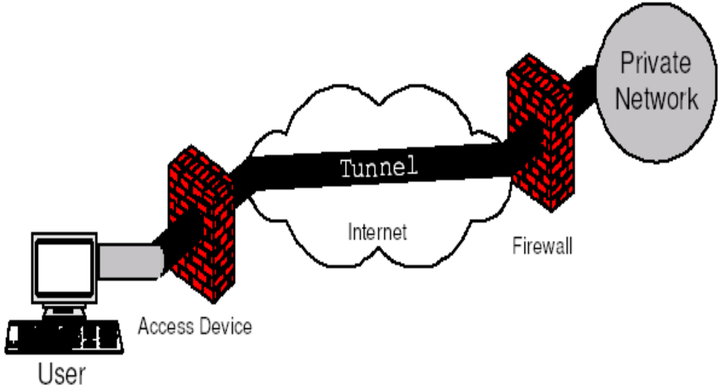
IPCP – IP Control Protocol



PPP – unsupported options

- **Flow control**
  Any PPP frame sent that overflows the receiver's buffer are lost
- **Error correction**
  PPP includes only Frame Check Sequence (CRC)
- **Re-sequencing**
  PPP assumes all frames, sent and received, retain their original intended order

Tunneling & PPP



- Tunneling - definition
  The process of running one network protocol
  on top of another.
  Common use: VPN (Virtual Private Network)
- Tunneling method
  Extending the link between the HDLC driver
  and the rest of PPP over a separate network
- PPP tunneling protocols
  L2TP, L2F(**Layer 2 Forwarding)**, PPTP(Point-to-Point_Tunneling_Protocol) & ethernet (PPPoE)

HDLC

Data link protocol

Defintion

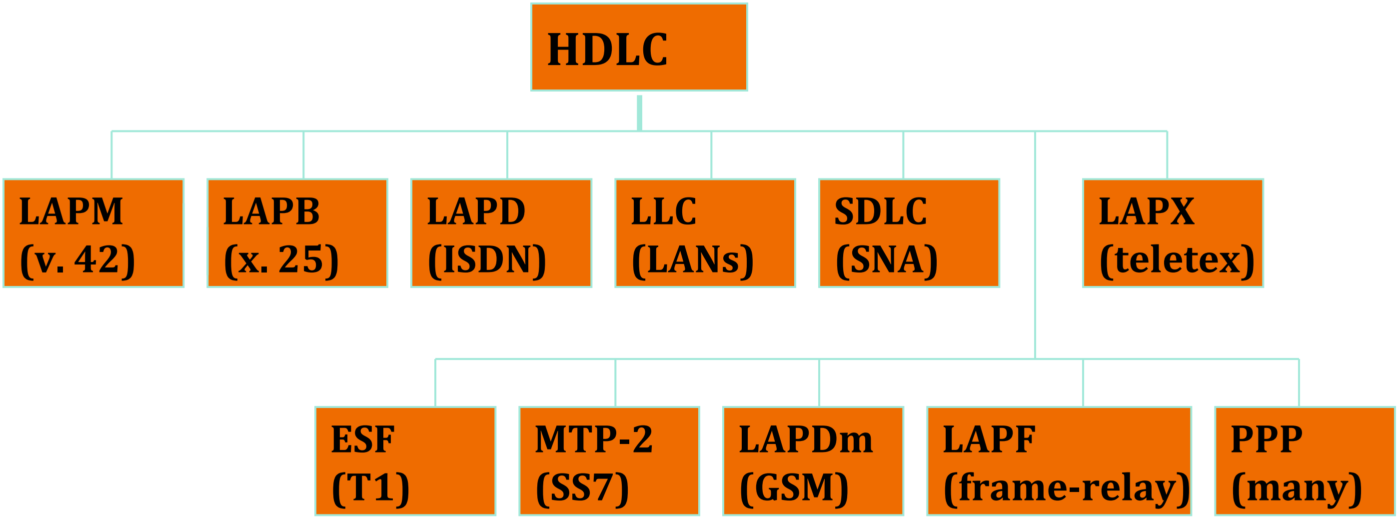
manages node-to-node transfer of data between

two directly connected machines.

Operations

- Error detection and correction (depends on the protocol)
- Addressing (in LANs)
- Frame-level synchronization between sender and receiver

HDLC `s (High level Data link Control) family



High-level Data link control

- Exchange of Digital data between two devices some form of data link control

- This Protocol is important for two reasons:

    - it is a widely used standardized data link control protocol.

    - HDLC serves as a baseline from which virtually all other important data link control protocols are derived

High Level Data Link Control

- HDLC
- ISO 33009, ISO 4335
- Most widely used DLC protocol

High-level Data link control

- **Basic Characteristics**
    - HDLC defines three types of stations
    - Two link configurations
    - Three data-transfer modes of operation

HDLC Station Types

- Primary station
  - Controls operation of link
  - Issues commands (frames)
  - Maintains separate logical link to each secondary station
- Secondary station
  - Under control of primary station
  - Issues responses (frames)
- Combined station
  - May issue commands and responses
  - Combines the features of primary and secondary stations

HDLC Link Configurations

- Unbalanced
  - One primary and one or more secondary stations
  - Supports full duplex and half duplex
- Balanced
  - Two combined stations
  - Supports full duplex and half duplex

HDLC Transfer Modes (1)

- Normal Response Mode (NRM)
  - Unbalanced configuration
  - Primary can only initiate transmission
  - Secondary may only transmit data in response to command (poll) from primary
  - Used on multi-drop lines
  - Host computer as primary
  - Terminals as secondary

HDLC Transfer Modes (2)

- Asynchronous Balanced Mode (ABM)
  - Balanced configuration
  - Either station may initiate transmission without receiving permission
  - Most widely used
  - No polling overhead

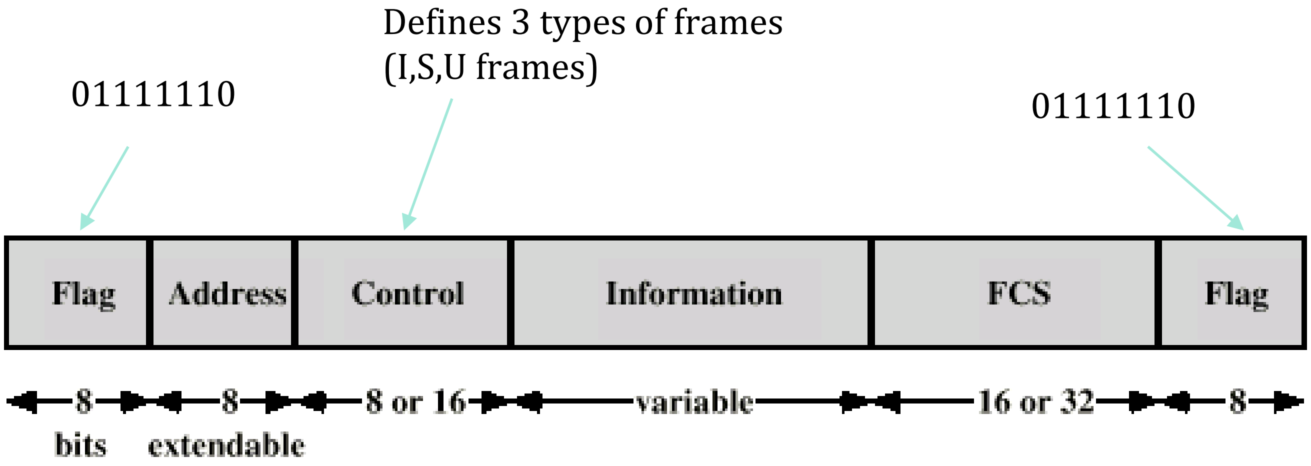
HDLC Transfer Modes (3)

- Asynchronous Response Mode (ARM)
  - Unbalanced configuration
  - Secondary may initiate transmission without permission form primary
  - Primary is responsible for connect, disconnect, error recovery, and initialization
  - rarely used

Frame Structure

- Synchronous transmission
- All transmissions in frames
- Single frame format for all data and control exchanges

Frame Structure



(a) Frame format

Flag Fields

- Delimit frame at both ends
- 01111110
- Receiver hunts for flag sequence to synchronize
- Bit stuffing used to avoid confusion with data containing 01111110
    - The transmitter inserts 0 bit after every sequence of five 1s with the exception of flag fields
    - If receiver detects five 1s it checks next bit
        - If 0, it is deleted
        - If 1 and seventh bit is 0 (i.e., 10), accept as flag

Bit Stuffing

- Example with possible errors

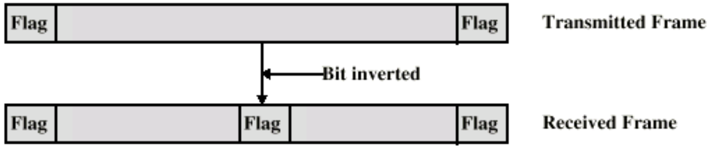
Original Pattern:

111111111111011111101111110

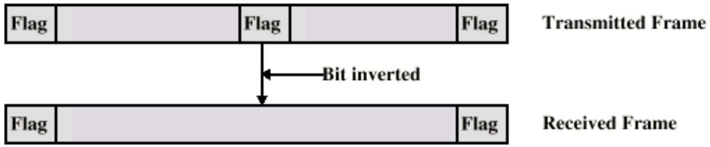
After bit-stuffing

1111101111101101111101011111010

(a) Example



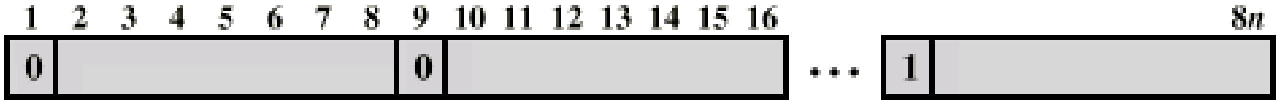
(b) An inverted bit splits a frame in two



(c) An inverted bit merges two frames

Address Field

- Identifies secondary station that sent or will receive frame
- Usually 8 bits long
- May be extended to multiples of 7 bits
    - LSB of each octet indicates that it is the last octet (1) or not (0)
- All ones (11111111) is broadcast

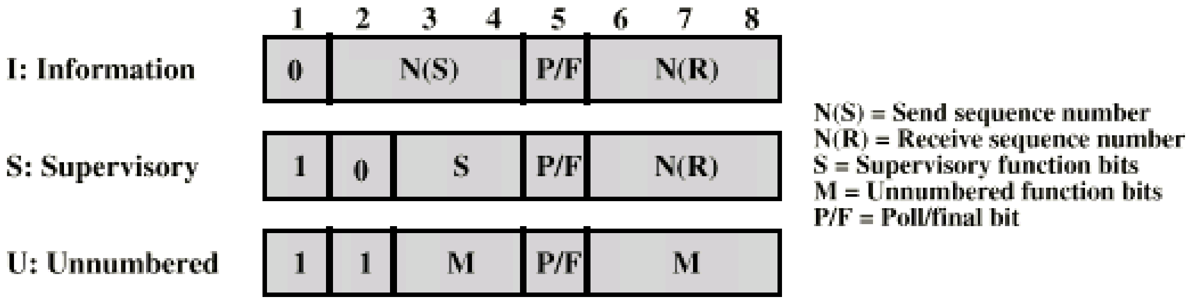


(b) Extended Address Field

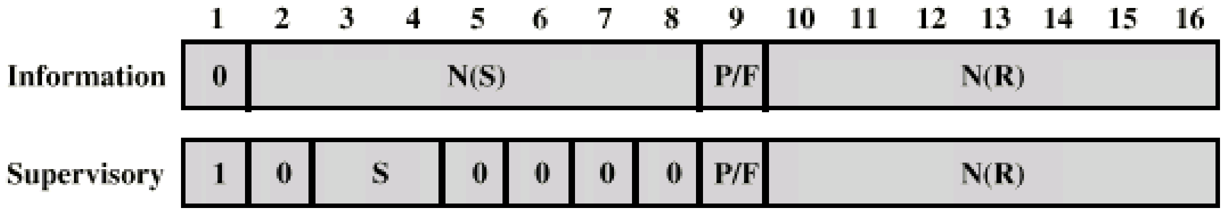
Control Field

- Different for different frame type
  - I-frame (information frame)
    - data to be transmitted to user (next layer up)
    - Flow and error control piggybacked on information frames
  - S-frame (Supervisory frame)
    - Used for flow and error control
  - U-frame (Unnumbered frame)
    - supplementary link control
- First one or two bits of control filed identify frame type

Control Field Diagram



(c) 8-bit control field format



(d) 16-bit control field format

Poll/Final Bit

- Use depends on context
- Command frame
    - P bit : used for poll from primary
    - 1 to solicit (poll) response from peer
- Response frame
    - F bit : used for response from secondary
    - 1 indicates response to soliciting command

I-frame

- Contains the sequence number of transmitted frames and a piggybacked ACK

1	2 3 4	5	6 7 8
0	N(S)	P/F	N(R)

- I,0,0
- I,1,0
- I,2,0,P

S-frame

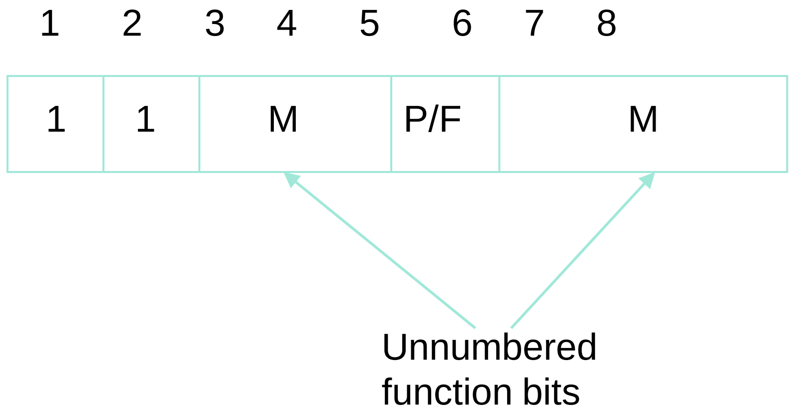
- Used for flow and error control

1	2	3	4	5	6	7	8
1	0	S		P/F	N(R)		

- RR --- receive ready
- RNR --- receive not ready
- REJ --- reject on frame N(R)
- SREJ --- selective reject on N(R)

U-frame

- Mode setting, recovery, connect/disconnect



Unnumberred frames

- Set normal response mode (SNRM)
- Set asynchronous response mode (SARM)
- Set asynchronous balanced mode (SABM)
- Disconnect (DISC)
- Unnumberred acknowledgement (UA)
- Disconnect mode (DM)
- Request disconnect (RD)
- Unnumberred poll (UP)
- Reset (RSET)
- Exchange identification (XID)
- Test (TEST)
- Frame reject (FRMR)

Information Field

- Only in information and some unnumbered frames
- Must contain integral number of octets
- Variable length

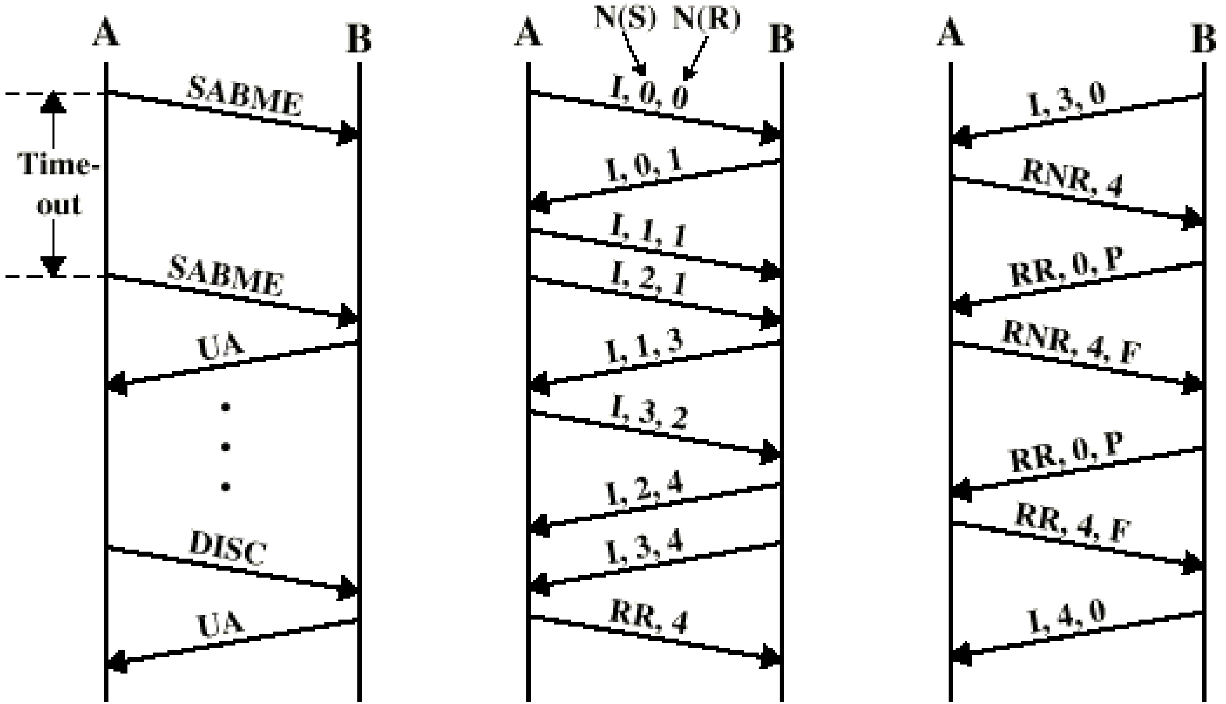
Frame Check Sequence Field

- FCS
- Error detection
- 16 bit CRC
- Optional 32 bit CRC

HDLC Operation

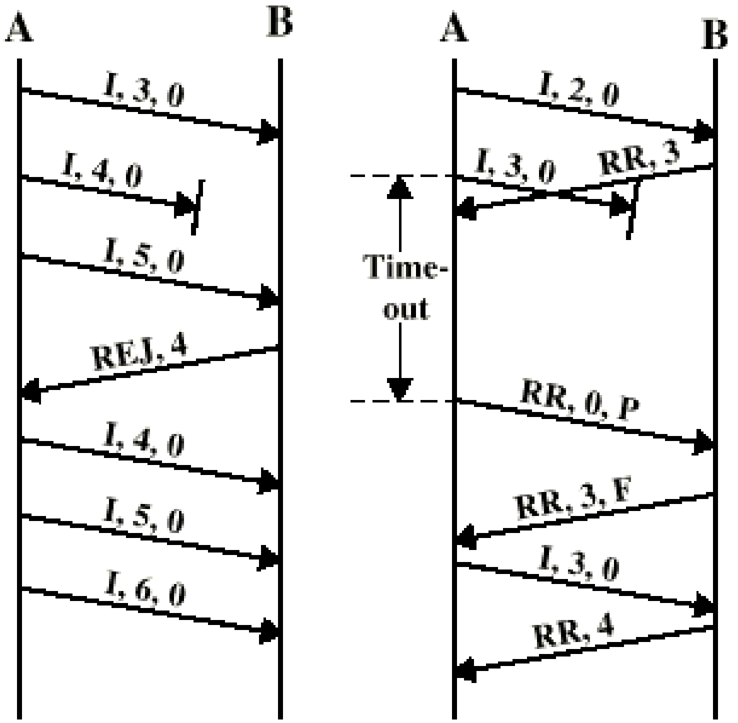
- Exchange of information, supervisory and unnumbered frames
- Three phases
    - Initialization
    - Data transfer
    - Disconnect

Examples of Operation (1)



(a) Link setup and disconnect (b) Two-way data exchange (c) Busy condition

Examples of Operation (2)



(d) Reject recovery (e) Timeout recovery

MPLS

What is MPLS?

- MPLS - Multi Protocol Label Switching
- A protocol to establish an end-to-end path from source to the destination.
- To setup this path basically using labels

  - Require a protocol to set up the labels along the path.

  It builds the connection oriented service on the IP network
- MPLS is an efficient encapsulation mechanism
- A hop-by-hop forwarding mechanism
- MPLS packets can run on other layer 2 technologies such as ATM, PPP, POS, FR, Ethernet
- Labels can be used as designators

- example: IP prefixes, ATM VC, or a bandwidth guaranteed path.

- This technique designed to speed up and shape traffic flows across

  enterprise wide area and service provider networks.

MPLS – MOTIVATION

Disadvantages of IP Routing

- It is a connectionless protocol, it does not directly any support for quality of service
- Each router has to make independent forwarding decisions based on the IP-address
- Large IP headers (at least 20bytes)
- Routing in Network Layer(Slower that Switching)

Motivation

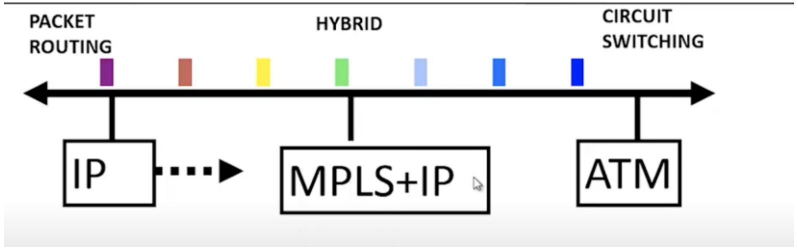
- Growth and evolution of the internet

  -The need to evolve routing algorithms

  -Allow speed of L2 switching at L3

  Router makes L3 forwarding decision based on a single field: similar to L2 forwarding => speed

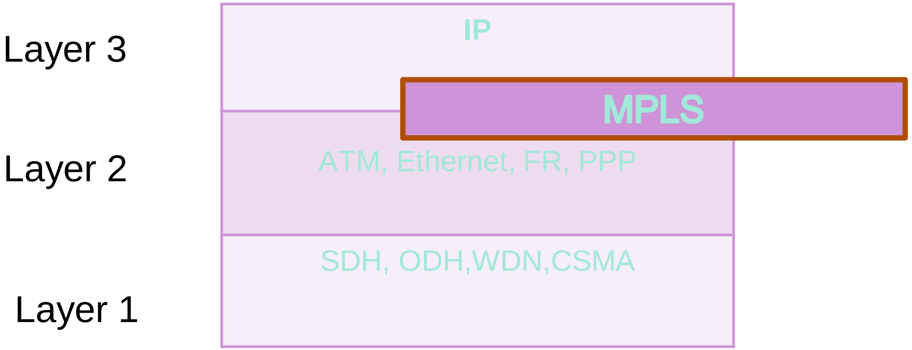
  -The need for advanced forwarding algorithm



MPLS + IP form a middle ground that combines the best of IP and the best of circuit

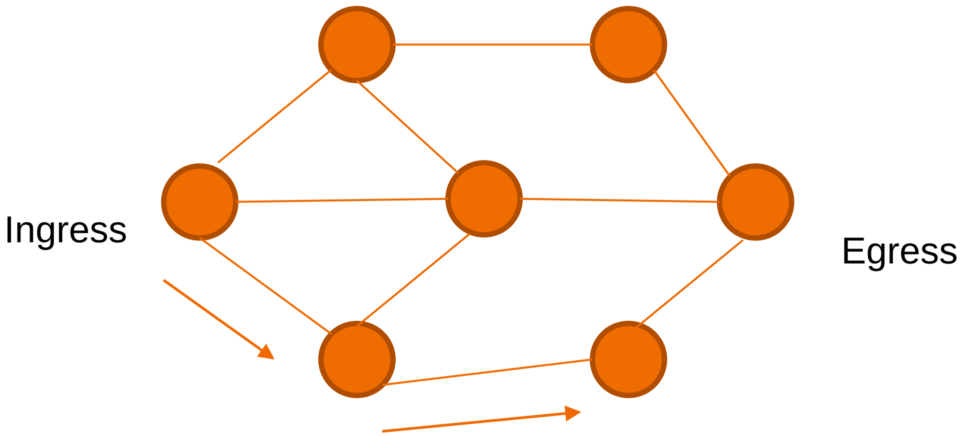
MPLS Basics

Multi-Protocol Label Switching is arranged between
Layer 2 and Layer3. Infect MPLS refer to as a Layer 2.5



- MPLS uses Label Switching
- A label is assigned for each IP flow
- A LSP is created between *ingress* and *egress*
- Packet forwarding at each router by table lookup (based on label)

When an *ingress* receives a packet it encapsulates it inside a MPLS packet at layer 2 and passed on to *egress* which then puts of the MPLS headers.



MPLS Characteristics

- It can support the traffic flows of various granularities
- It is independent of Layer 2 and Layer 3 Protocols
- It maps IP address to fixed length labels
- Interfaced to existing routing protocols
- It can support ATM, Frame-Relay and Ethernet

Technology Basics

Label

- A label is an integer identifying a FEC (a flow)
- Labels are not globally or network - unique label
- Labels are unique only between nodes
- Labels change at each node as a packet traverses a path
- Labels can set manually or we can use label distribution

Label Format

Label (20bits)	EXP (3bits)	Stack bit(s)	TTL (8bits)

Label: Label value used as the pointer for forwarding.

Exp: Experimental bits often used for quality of service

S: Bottom of stack flag – for indicating whether the label is at the

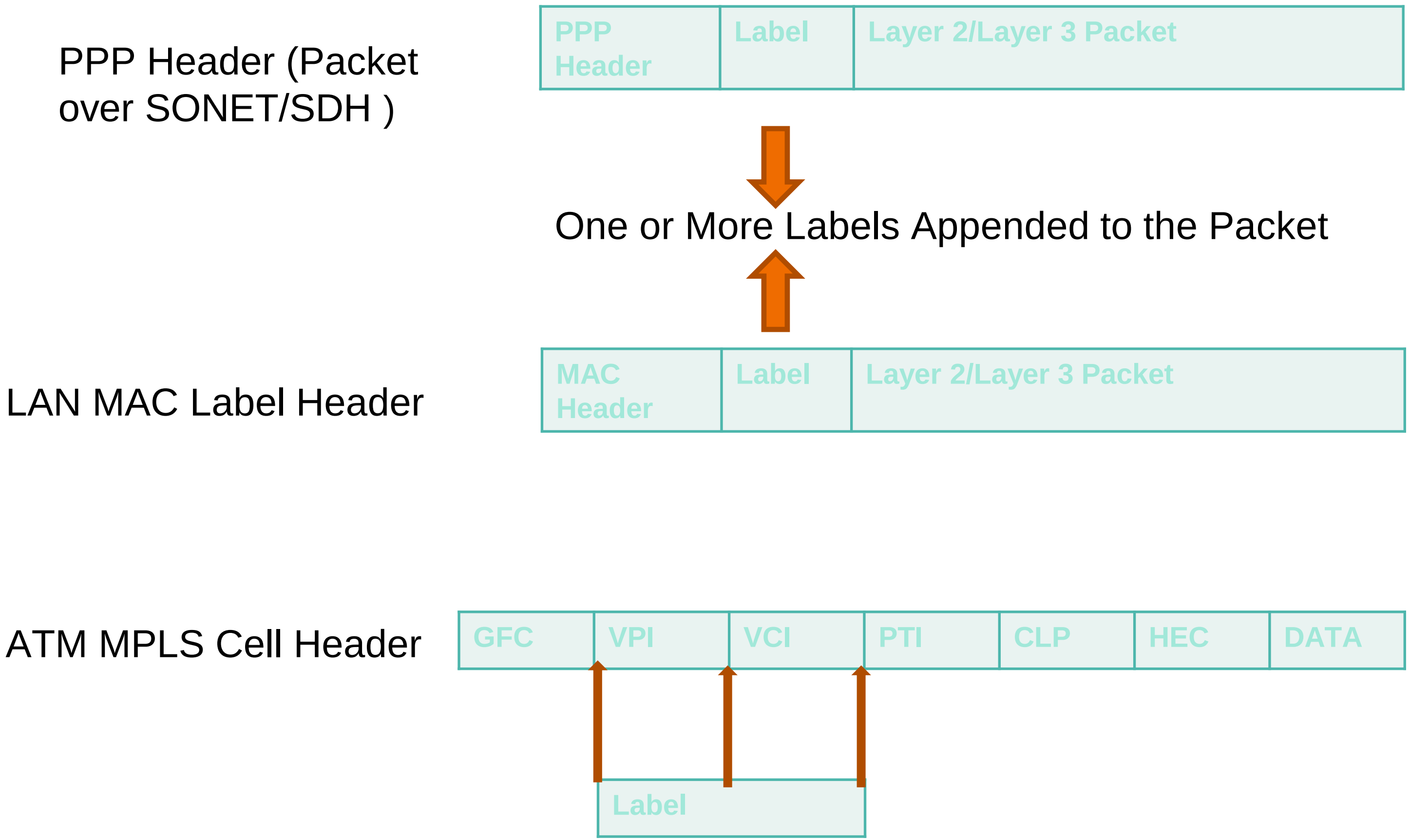
bottom of the label stack.

1 indicates that no label follows .

This field is very useful when there are multiple levels of MPLS labels.

TTL: Time to live - This field has the same meaning as that for an IP packe

Encapsulation



Label Distribution:

- MPLS does not specify a single method for label distribution

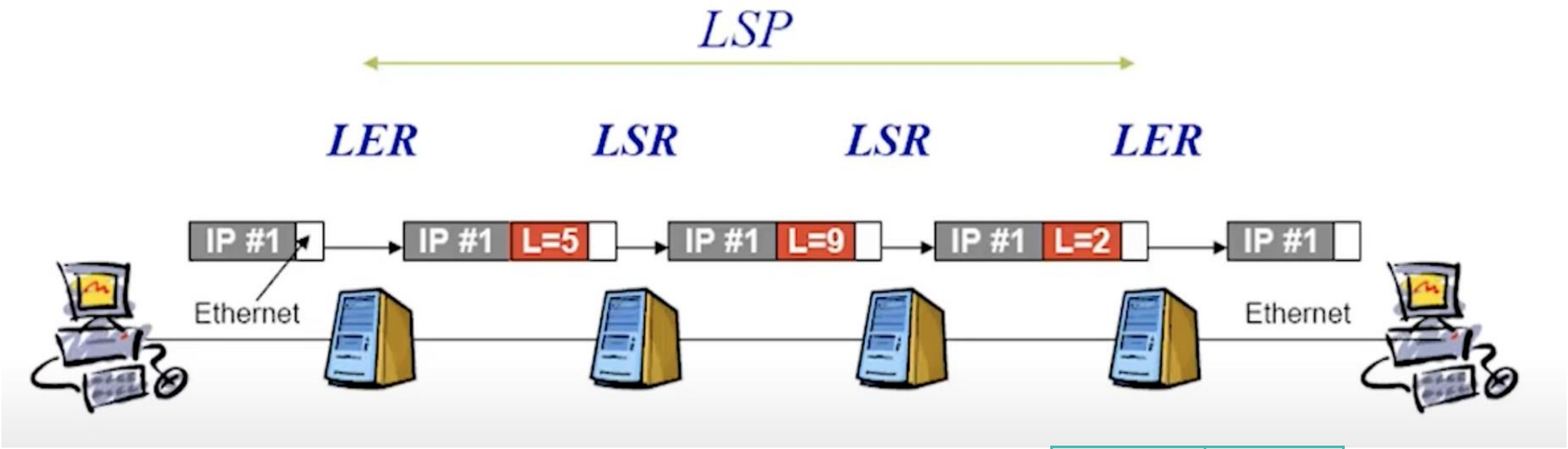
BGP has been enhanced to piggyback the label information within the contents of the protocol

- RSVP has also been extended to support piggybacked exchange of labels.
- IETF has also defined a new protocol known as the label Distribution protocol (LDP) for explicit signalling and management.
- Extensions to the base LDP protocol have also been defined to support explicit routing based on QoS requirements

Label Edge Router – LER

- Resides at the edge of an MPLS Network and assigns and removes the labels from the packets.
- Supports multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet)

Position of LERs and LSRs



IP Addr	Out Label
192.4/16	5
Layer 2 Transport	Assign init label

IP Addr	Out Label
5	9
Label Swapping	

IP Addr	Out Label
9	2
Label Swapping	

IP Addr	Out Label
2	192.4/16
Remove Label	Layer 2 Transport

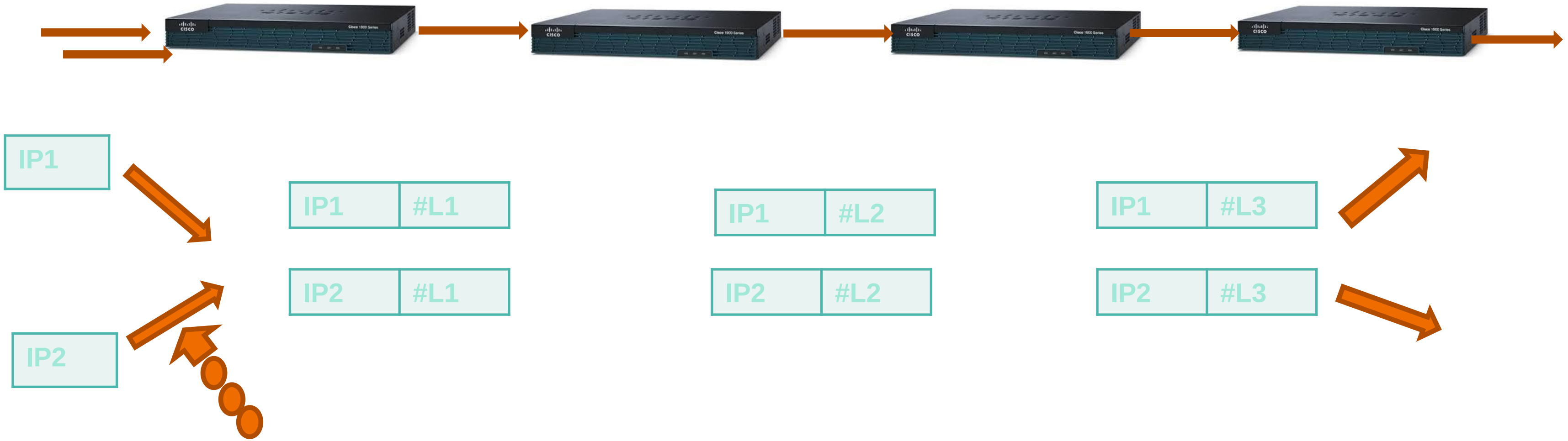
“ROUTE AT EDGE, SWITCH IN CORE”

Forward Equivalence Class – FEC

- Is a representation of a group of packets that share the same requirements for their transport.

- The assignment of a particular packet to a particular FEC is done just once(when the packet enters the network).

Forwarding Equivalence Classes



Packets are destined for different address prefixes, but can be mapped to common path

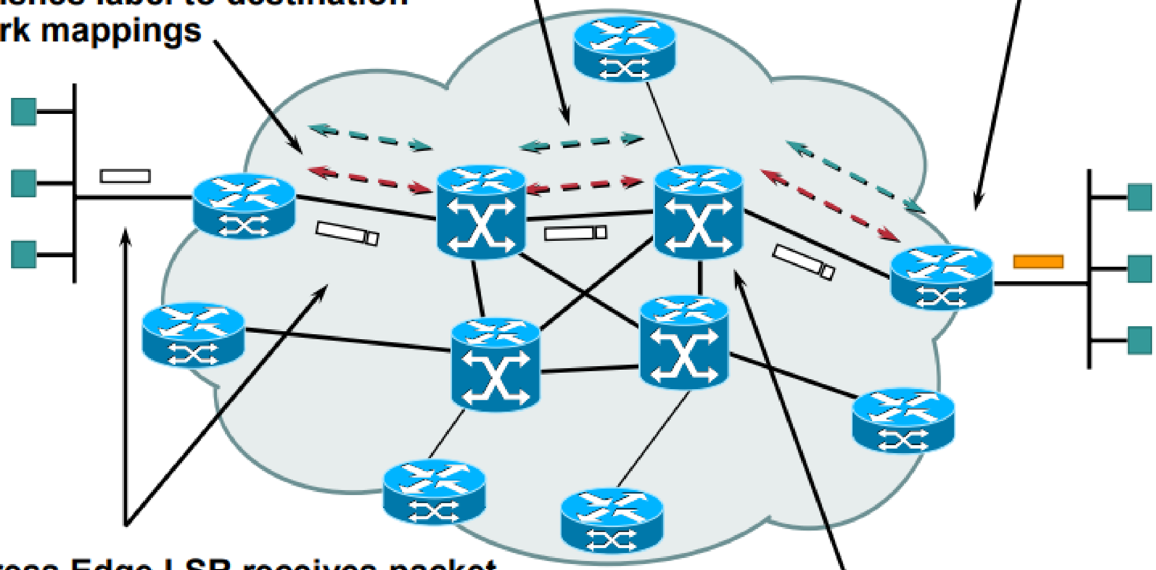
- FEC = “A set of packets with similar and /or identical characteristics which may be forwarded the same way; that is, they may be bound to the same MPLS label."

MPLS Operation

1a. Existing routing protocols (e.g. OSPF, IS-IS) establish reachability to destination networks

1b. Label Distribution Protocol (LDP) establishes label to destination network mappings

4. Edge LSR at egress removes label and delivers packet



2. Ingress Edge LSR receives packet, performs Layer 3 value-added services, and “labels” packets

3. LSR switches packets using label swapping

ST-1061

MPLS Packet Format

Label (20bits)	EXP (3bits)	Stack bit(s)	TTL (8bits)

Label (20bits)	EXP (3bits)	Stack bit(s)	TTL (8bits)

Label (20bits)	EXP (3bits)	Stack bit(s)	TTL (8bits)

MPLS has two major components:

- Control plane—exchanges L3 routing information and labels.

Control plane takes care of the routing information exchange and the label exchange between adjacent devices

- Data plane—forwards packets based on labels

Data plane takes care of forwarding either based on destination addresses or labels

Control plane contains complex mechanisms to exchange routing information (OSPF, EIGRP, IS-IS, BGP, etc.) and labels (Tag Distribution protocol [TDP], Label Distribution protocol [LDP], BGP, RSVP, etc.)

Data plane has a simple forwarding engine Control plane maintains the contents of the label switching table (label forwarding information base or LFIB)

There is a large number of different routing protocols such as OSPF, IGRP, EIGRP, IS-IS, RIP, BGP, etc. that can be used in the control plane.

The control plane also requires protocols to exchange labels, such as:

- Tag Distribution Protocol [TDP] (MPLS)
- Label Distribution Protocol [LDP] (MPLS)
- BGP (MPLS virtual private networks [VPNs])
- Resource-Reservation Protocol [RSVP] (MPLS Traffic Engineering [MPLSTE])
- CR-LDP (MPLS-TE)

The data plane however, is a simple label-based forwarding engine that is independent of the type of routing protocol or label exchange protocol. A Label Forwarding Information Base (LFIB) is used to forward packets based on labels. The LFIB table is populated by the label exchange protocols used in the control plane.

Label Switch Paths – LSPs

- A path is established before the data transmission starts.
- A path is a representation of an FEC

LSP Details

- MPLS provides two options to set up an LSP

  1. Hop by hop routing

     Each LSR independently selects the next hop for a given FEC. LSRs supports any available routing protocols (OSPF,ATM…).

  2. Explicit routing

     Is similar to source routing. The ingress LSR specifies the list of nodes through which the packet traverses.

- The LSP setup for an FEC is unidirectional. The return traffic must

Label Distribution Protocol – LDP

An application layer protocol for the distribution of label binding information to LSRs.

- It is used to map FECs to label, which, in turn, create LSPs
- LDP sessions are established between LDP peers in the MPLS network (not necessary adjacent)
- Sometimes employs OSPF or BGP.

LDP message types:

- Discovery messages - announce and maintain the presence of an LSR in a network
- Session message – establish, maintain, and terminate sessions between LDP peers
- Advertisement messages – create, change, and delete label mappings for FECs
- Notification messages – provide advisory information and signal error information

Label Advertisement Mode

Two label advertisement modes are available:

1. Downstream on demand(DoD)
2. Downstream unsolicited (DU)

Label Distribution control Mode

There are two label distribution control modes:

Independent: and LSR can notify label binding messages upstream anytime.

Ordered: an LSR can send label binding messages about a FEC upstream only when it receives a specific label binding message from the next hop a FEC or the LSR itself is the egress node of the FEC.

Label Retention Mode

Two label retention modes:

1. Liberal: an LSR keeps any received label to FEC binding regardless of whether the binding is from its next hop for the FEC or not.

2. Conservative: an LSR keeps only label to FEC bindings that are from its next hops for the FECs.

In liberal mode, an LSR can adapt to route changes quickly; while in conservative mode, there are less label to FEC bindings for an LSR to advertise and keep.

The conservative label retention mode is usually used with the DoD mode on LSRs with limited label space.

MPLS Applications

Some of the MPLS applications are follows

- Unicasting IP routing
- Multicast IP routing
- Traffic Engineering
- Virtual Private Network
- Quality of Service(QoS)

Traffic Engineering

- Traffic engineering allows a network administrator to make the path deterministic and bypass the normal routed hop-by-hop paths.
- An administrator may elect to explicitly define the path between stations to ensure QoS or have the traffic follow a specified path to reduce traffic loading across certain hops.
- The network administrator can reduce congestion by forcing the frame to travel around the overloaded segments.
- Hops are configured in the LSRs ahead of time along with the appropriate label values.

MPLS – Traffic Engineering

- End –to-End forwarding decision determined by ingress nod

- Enables Traffic Engineering

MPLS based VPN

- One of most popular MPLS applications is the implementation of VPN.
- The basic concept is the same as ATM transparent LAN.
- Using label (instead of IP address) to interconnect multiple sites over a carrier’s network. Each site has its own private IP address space.
- Different VPNs may use the same IP address space.

MPLS and QoS

- Pre configuration based on physical interface
- Classification of incoming packets into different classes
- Classification based on network characteristics (such as congestion, throughput, delay, and loss)
- A label corresponding to the resultant class is applied to the packet

Thank you