AHRAM CANADIAN UNIVERSITY

Lecture (04)
Packet switching & Frame Relay techniques

Dr. Ahmed ElShafee

Agenda

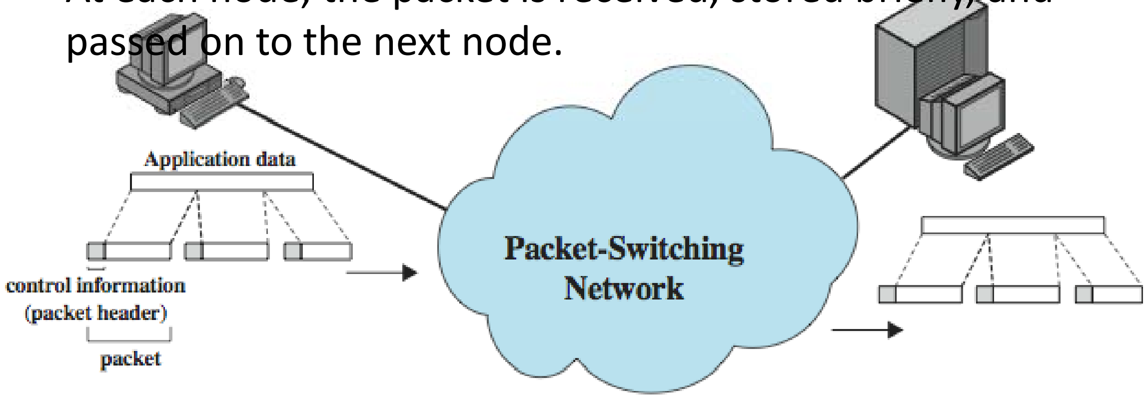
- Packet switching technique
- Packet switching protocol layers (X.25)
- Frame Relay

Packet switching technique

Introduction

- In contrast a packet-switching network is designed for data use.
- Data are transmitted in short packets.
- Fixed packet length say 1000 octets (bytes).
- If a source has a longer message to send, the message is broken up into a series of packets.
- Each packet contains a portion (or all for a short message) of the user's data plus some control information.

- The control information, at a minimum, includes the information that the network requires to be able to route the packet through the network and deliver it to the intended destination.
- At each node, the packet is received, stored briefly, and passed on to the next node.



Advantages

1. Line efficiency is greater,

- because a single node-to-node link can be dynamically shared by many packets over time.
- The packets are queued up and transmitted as rapidly as possible over the link.
- By contrast, with circuit switching, time on a node-to-node link is pre-allocated using synchronous time division multiplexing.
- Much of the time, such a link may be idle because a portion of its time is dedicated to a connection that is idle (considered to disadvantage)

2. A packet-switching network can perform data-rate conversion.

- Two stations of different data rates can exchange packets because each connects to its node at its proper data rate.

3. When traffic becomes heavy on a circuit-switching network, some calls are blocked;

- that is, the network refuses to accept additional connection requests until the load on the network decreases.
- On a packet-switching network, packets are still accepted, but delivery delay increases.

5. Priorities can be used.

- If a node has a number of packets queued for transmission, it can transmit the higher-priority packets first.
- These packets will therefore experience less delay than lower-priority packets.

Switching technique

- Two approaches are used in packet switching networks: datagram and virtual circuit.

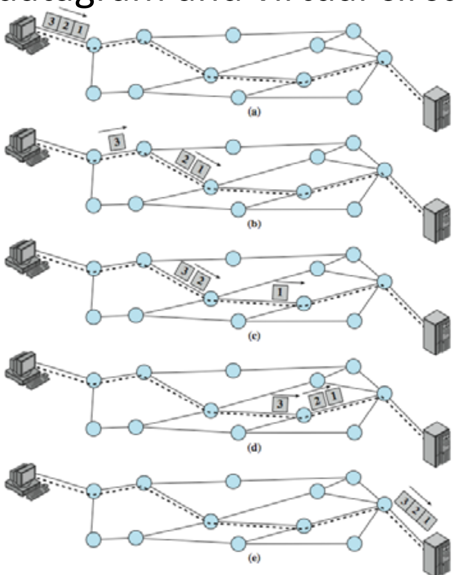


Figure 10.10 Packet Switching: Virtual-Circuit Approach

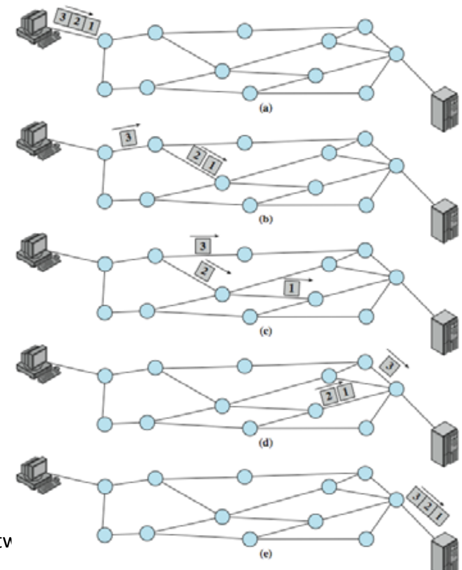


Figure 10.9 Packet Switching: Datagram Approach

datagram approach,

- each packet is treated independently, with no reference to packets that have gone before.
- Each node chooses the next node on a packet's path, taking into account information received from neighboring nodes on traffic, line failures, and so on.
- So the packets, each with the same destination address, do not all follow the same route, and they may arrive out of sequence at the exit point.
- Exit node, or destination rearrange the data grams to restore the original squence.

Virtual circuit

- a preplanned route is established before any packets are sent.
- Once the route is established, all the packets between a pair of communicating parties follow this same route through the network.
- Because the route is fixed for the duration of the logical connection, it is somewhat similar to a circuit in a circuits witching network and is referred to as a virtual circuit.
- Each packet contains a virtual circuit identifier as well as data.
- Each node on the pre-established route knows where to direct such packets; no routing decisions are required.

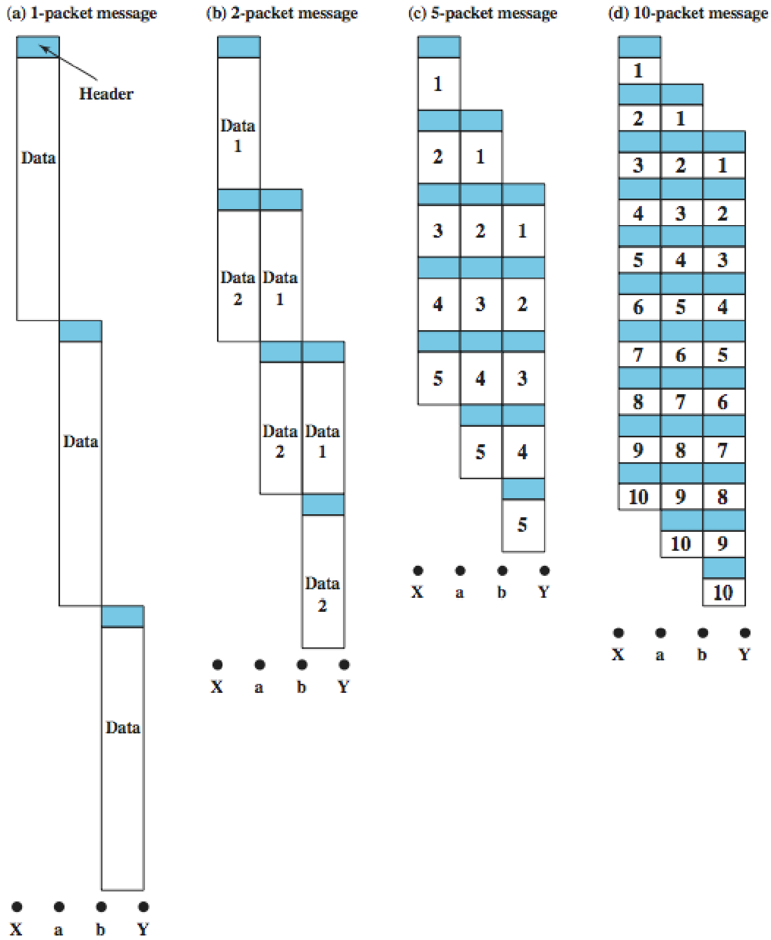
- At any time, each station can have more than one virtual circuit to any other station.
- The virtual circuit is established before data being transferred, even, it’s not a dedicated path.
- A transmitted packet is buffered at each node, and queued for output over a line, while other packets on other virtual circuits may share the use of the line.
- Nods do no routing decisions, as virtual path is already established.

Comparisons between datagrame, and Virtual circuits

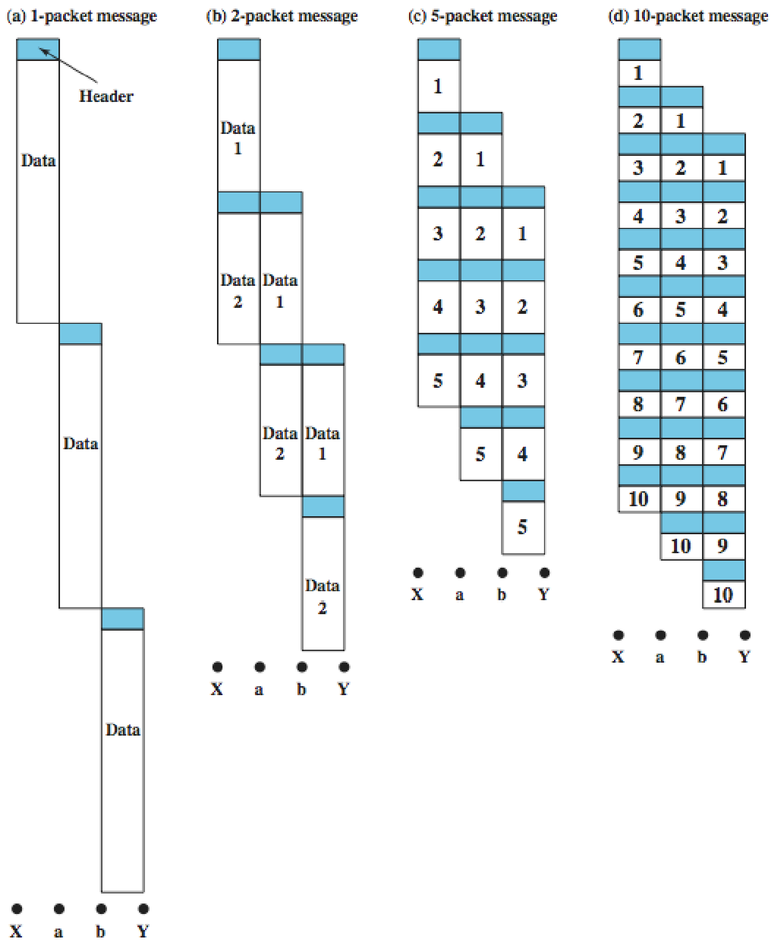
Datagram	Virtual circuit
No sequencing or error control, destination or exit node should solve these problems	network can provide sequencing and error control, as all packets follow the same route
Packets are slow, need routing decision at each node.	packets are forwarded more quickly, no routing decisions
no call setup phase, immediate transmission	Call setup, wait before start
More reliable, any available path, if node fail, forward to any nearby node	less reliable, only predefined path, if node fails, path down
more flexible	Less fixable

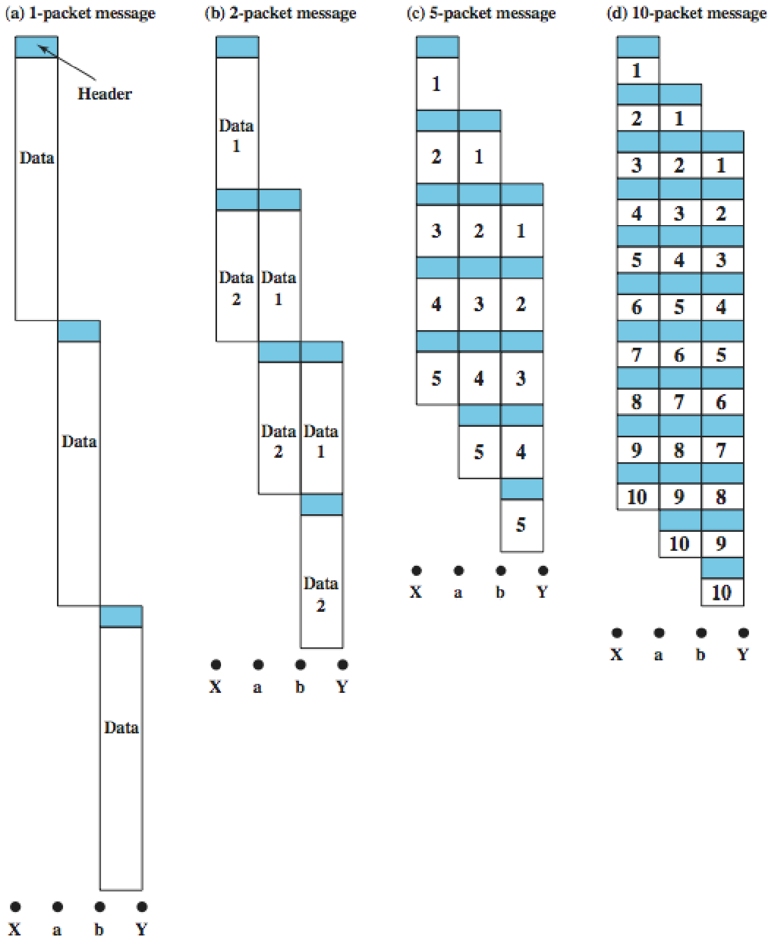
Packet size and transmission time

- Assume that a virtual circuit exists from station "X" through nodes "a" and "b" to station "Y".
- The message to be sent comprises 40 octets, with 3 octets of control information at the beginning of each packet in the header.

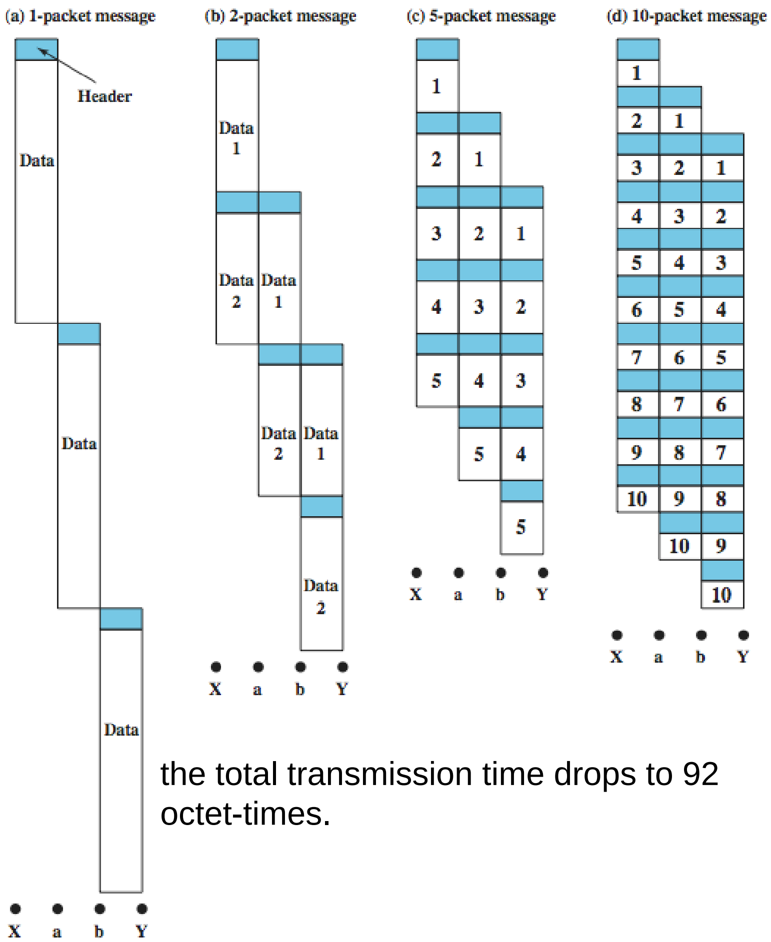


- If the entire message is sent as a single packet of 43 octets
- (3 octets of header plus 40 octets of data), then the packet is first transmitted from station "X" to node "a"
- When the entire packet is received, it can then be transmitted from "a" to "b".



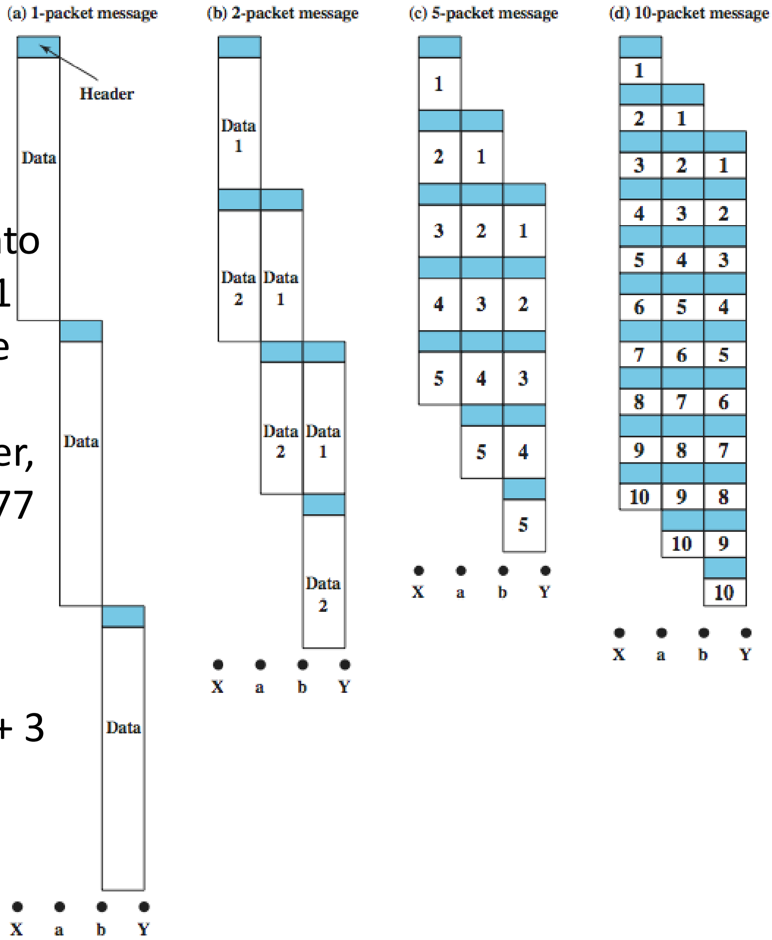


- When the entire packet is received at node “b”, it is then transferred to station “Y”.
- Ignoring switching time, total transmission time is 129 octet-times (43 octets × 3 packet transmissions).

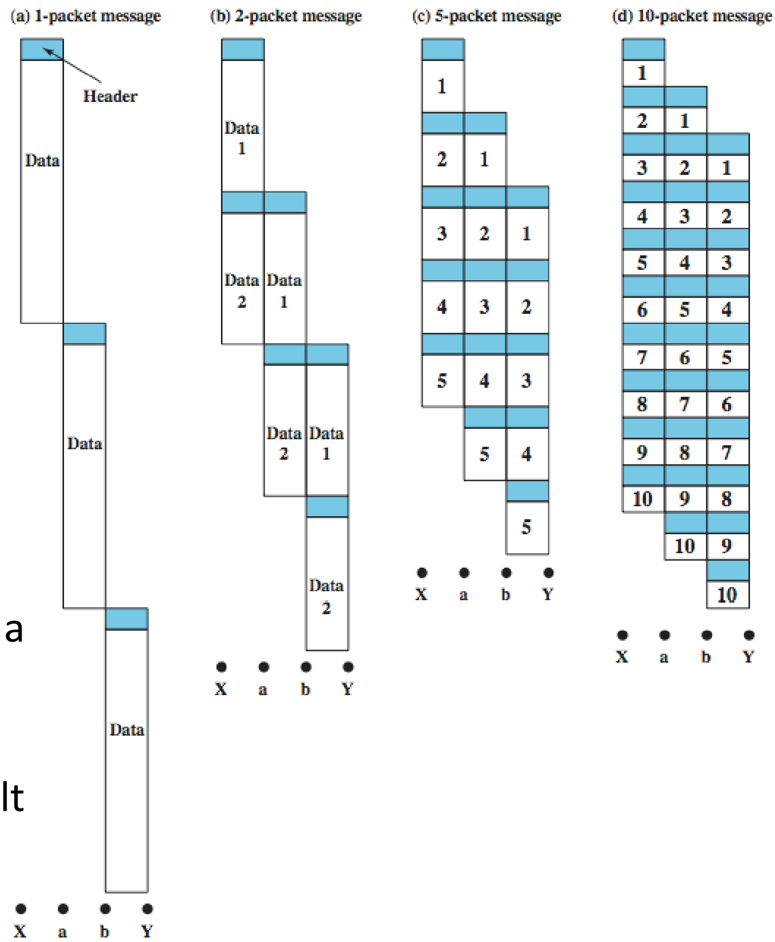


- If we break the message into two packets with 20 octets of message and 3 octets of header each.
- node “a” can begin transmitting the first packet as soon as it has arrived from “X”. Because of this overlap in transmission,
- Tx time=92 octet time

the total transmission time drops to 92 octet-times.



- breaking the message into five packets (40/5)+3=11 octet, each intermediate node can begin transmission even sooner, with a total of = 11x7 = 77 octet-times for transmission.
- Dividing message to 10 packets each of 4 octet + 3 control=7 octet/ packet
- Total Tx time = 12x7=84 octet time



Conclusions:

- each packet contains a fixed amount of header, and more packets Also, processing and queuing delays at each node are greater when more packets are handled for a single message.
- extremely small packet size (53 octets) can result in an efficient network design.

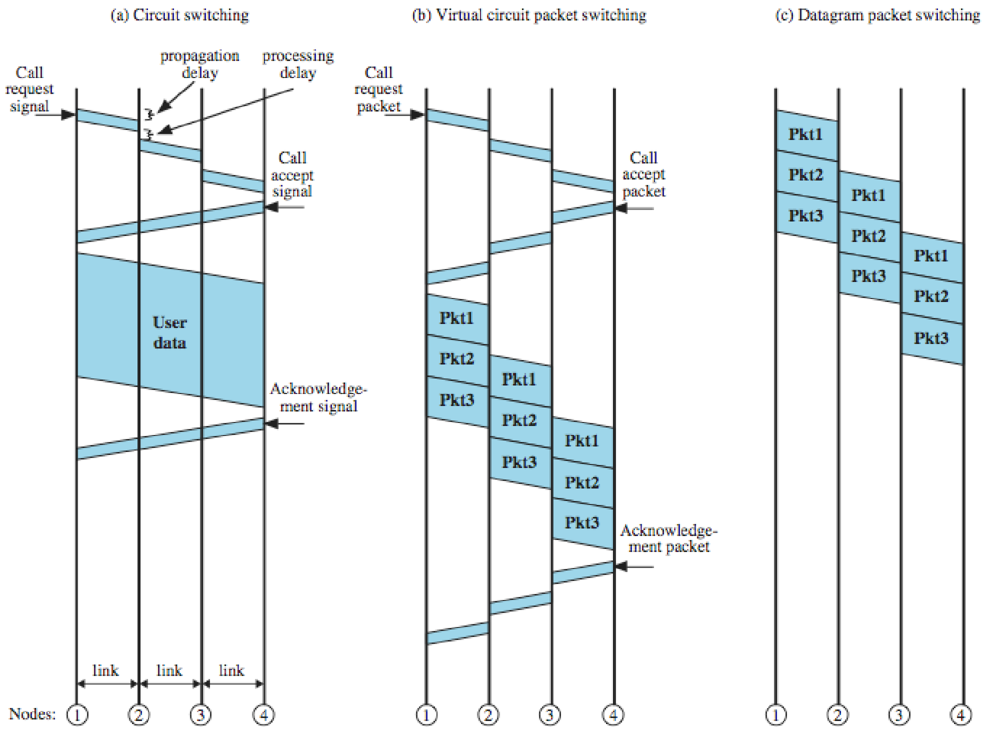
Packet switching delays

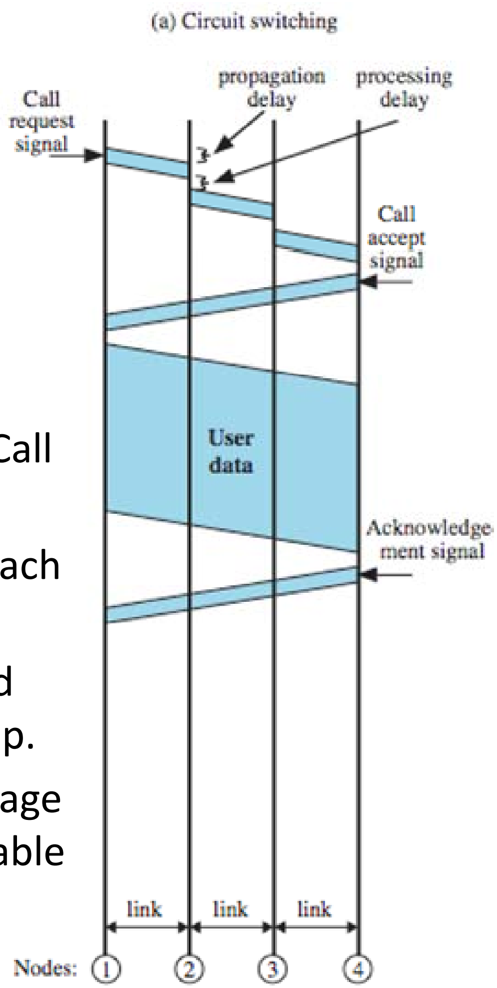
- **Propagation delay:** The time it takes a signal to propagate from one node to the next. The speed of electromagnetic signals through a wire medium, for example, is typically 3×10^8 m/s, delay is neglectable.
- **Transmission time:** The time it takes for a transmitter to send out a block of data. For example, it takes 1 s to transmit a 10,000-bit block of data onto a 10-kbps line.
- **Node delay:** The time it takes for a node to perform the necessary processing as it switches data.

Circuit switching and packet switching comparison

Circuit switching	Packet switching
Transparent service, once connection is established fixed data rate in provided	Variable delay is introduced to packets, which need some sequencing and error recovery
No overhead required for routing packets	Add header to each packet contains routing information
Not achieving 100% line utilization	Almost achieves 100% line utilization
Blocking till free up resources	Blocking till solving congestion
no traffic priority	Traffic Priority
expansive	Cheap
Fixed data rate	Equalizing data rates
Analog and digital	Digital only
Wait till establishment	Immediate start(datagram) or wait for establishment (Virtual circuit)

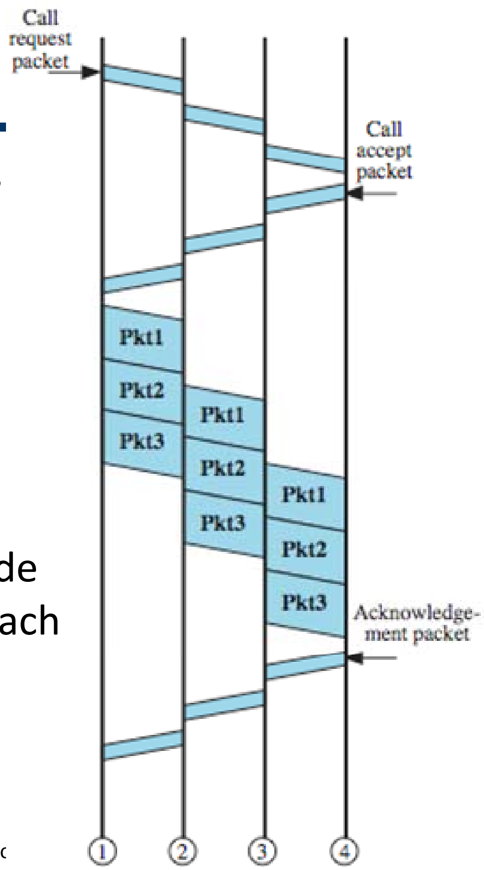
Event timing





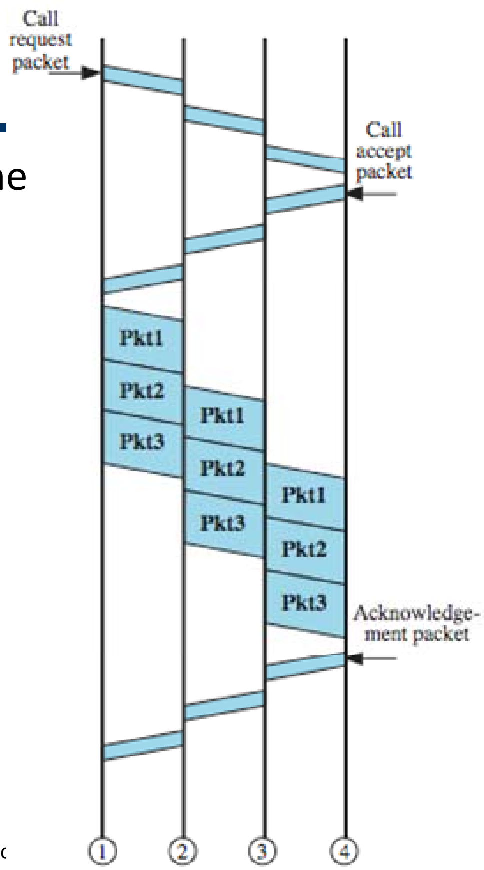
- For **circuit switching**, there is a delay before the message is sent.
- First, a Call Request signal is sent.
- If the destination station is not busy, a Call Accepted signal returns.
- Note a processing delay is incurred at each node during the call request.
- On return, this processing is not needed because the connection is already set up.
- After the connection s set up, the message is sent as a single block, with no noticeable delay at the switching nodes.

(b) Virtual circuit packet switching

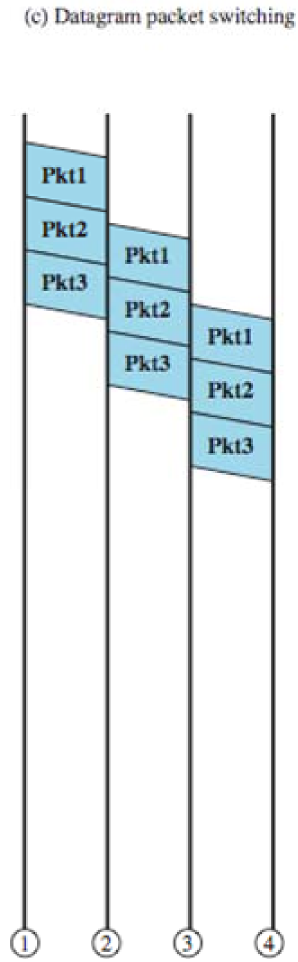


- **Virtual circuit packet switching** appears similar to circuit switching.
- A virtual circuit is requested using a Call Request packet, which incurs a delay at each node, and is accepted with a Call Accept packet.
- In contrast to the circuit-switching case, the call acceptance also experiences node delays, since each packet is queued at each node and must wait its turn for transmission.

(b) Virtual circuit packet switching



- Once the virtual circuit is established, the message is transmitted in packets.
- Packet switching involves some delay at each node in the path.
- Worse, this delay is variable and will increase with increased load.



- Datagram packet switching does not require a call setup.
- Thus, for short messages, it will be faster than virtual circuit and perhaps circuit switching.
- However, because each individual datagram is routed independently, the processing at each node may be longer than for virtual circuit packets.
- For long messages virtual circuits may be superior.

Packet switching protocol layers (X.25)

- Circuit switching network provides a transparent communications path for attached devices that makes it appear that the two communicating stations have a direct link.
- packet-switching networks, the attached stations must organize their data into packets for transmission.
- This requires a certain level of cooperation between the network and the attached stations
- The standard used for traditional packet-switching networks is X.25, which is an ITU-T standard

- The functionality of X.25 is specified on three levels:
  - Physical level,
  - Link level, and
  - Packet level.

1. The Physical layer

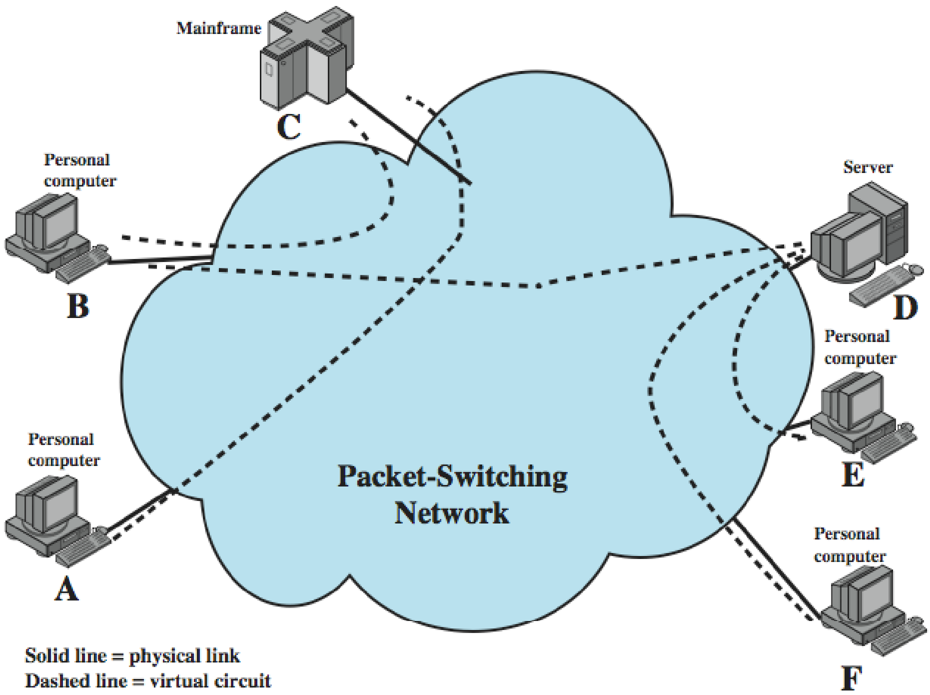
- interface between station node link
- two ends are distinct
  - Data Terminal Equipment DTE (user equipment)
  - Data Circuit-terminating Equipment DCE (node)
- physical layer specification is X.21
- can substitute alternative such as EIA-232

2. The link layer (link control layer)

- referred to as LAPB (Link Access Protocol - Balanced).
- sending data as a sequence of frames.
- provides reliable (sequencing and error control) transfer of data over link.

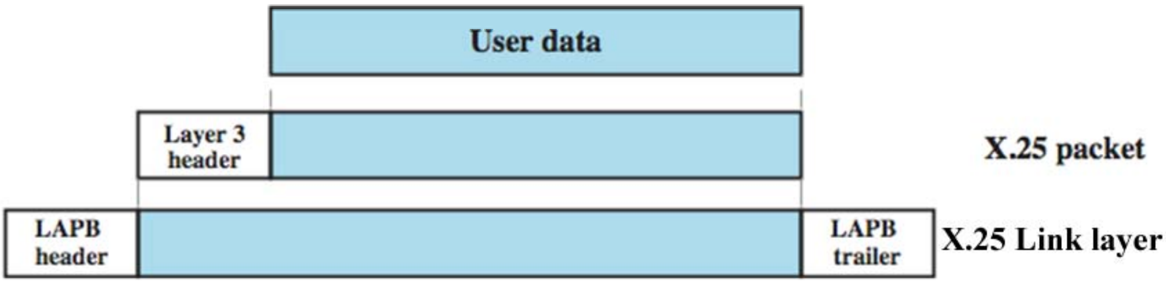
3. The packet layer

- provides a External virtual circuit service, enabling any subscriber to the network to set up logical connections, called virtual circuits, to other subscribers.
- "virtual circuit" refers to the logical connection between two stations through the network;
- X.25 can transferee datagrams, through the virtual circuit (data associated with that logical channel), after its establishment



- Last figure shows an example of X.25 virtual circuits
- station A has a virtual circuit connection to C; station B has two virtual circuits established, one to C and one to D; and stations E and F each have a virtual circuit connection to D.
- As an example of how these external virtual circuits are used, station D keeps track of data packets arriving from three different workstations (B, E, F) on the basis of the virtual circuit number associated with each incoming packet.

X.25 packet



Steps

- User data are passed down to X.25 level 3, which appends control information as a header, creating a packet.
- This control information do
  - identifying by number a particular virtual circuit with its associated data,
  - providing sequence numbers that can be used for flow and error control on a virtual circuit basis.
- X.25 packet is then passed down to the LAPB entity, which appends control information at the front and back of the packet the control information in the frame is needed for the operation of the LAPB protocol.

- Each X.25 data packet includes send and receive sequence numbers.
- The send sequence number, P(S), for all outgoing data packets on a particular virtual circuit.
- The receive sequence number, P(R), is an acknowledgment of packets received on that virtual circuit.

- Packets then delivered to physical layer to be transferred through terminals.

key features of the X.25

The following are key features of the X.25 approach:

1. Call control packets, used for setting up and clearing virtual circuits, are carried on the same channel and same virtual circuit as data packets.
2. Multiplexing of virtual circuits takes place at layer 3.
3. Both layer 2 and layer 3 include flow control and error control mechanisms.

Conclusions

- The X.25 approach results in considerable overhead.
- At each hop through the network, the data link control protocol (layer 2) involves the exchange of a data frame and an acknowledgment frame.
- At each intermediate node, state tables must be maintained for each virtual circuit to deal with the call management and flow control/error control aspects of the X.25 protocol.
- All of this overhead may be justified when there is a significant probability of error on any of the links in the network.
- This approach is not suitable for modern digital communication facilities.

Frame relay

- The modern transmission technology are able (ex: fiber optics) are
  - Reliable
  - high quality
  - High data rate
- the overhead of X.25 is not only unnecessary but degrades the effective utilization of the available high data rates
- Frame relay is designed to eliminate much of the overhead that X.25 imposes on end user systems and on the packet-switching network.

Differences between frame relay and a conventional X.25 packet-switching service are:

- Call control signaling, (needed to set up and manage a connection), is carried on a separate logical connection from user data.
- Thus, intermediate nodes need not maintain state tables or process messages relating to call control on an individual per-connection basis.
- Multiplexing and switching of logical connections takes place at layer 2 instead of layer 3, eliminating one entire layer of processing.

- There is no hop-by-hop flow control and error control.
- End-to-end flow control and error control are the responsibility of a higher layer, if they are employed at all (layer 3 in not implemented in switched nodes only layer 2 which speed up switching node).

- with frame relay, a single user data frame is sent from source to destination, and an acknowledgment, generated at a higher layer, may be carried back in a frame.
- There are no hop-by-hop exchanges of data frames and acknowledgments.

Disadvantage

Doesn’t provide link-by-link flow and error control

Solved by

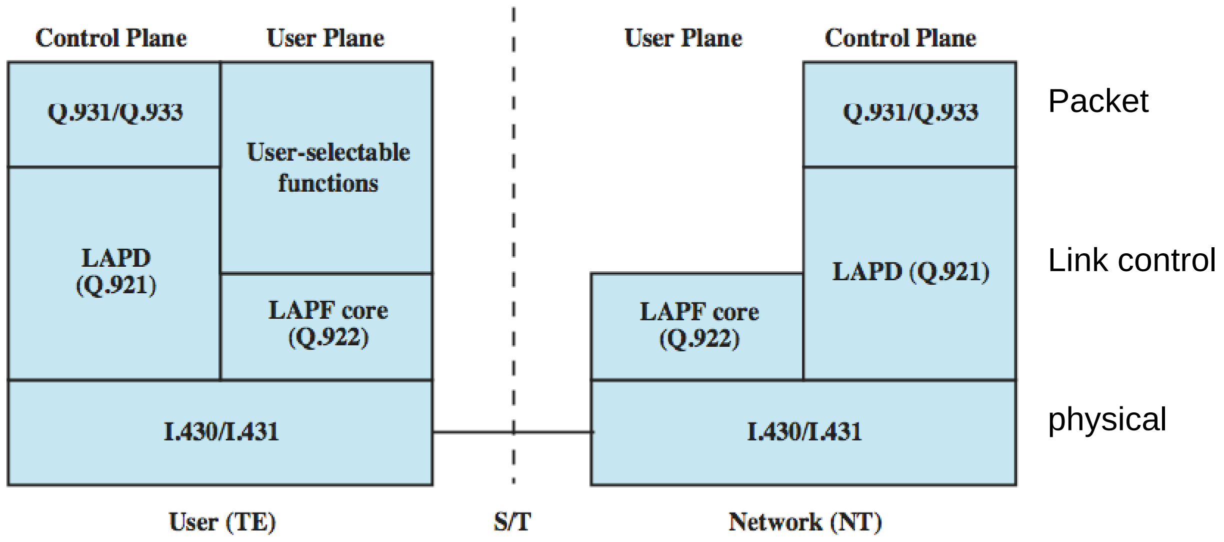
- increasing reliability of transmission and switching facilities,
- Flow and error control provided by higher layer

Advantage

- Reduced control functionality of in user network interface, and in internal network.
- Lower delay
- higher throughput

- frame relay achieved an access speeds up to 2 Mbps.
- frame relay service at even higher data rates is now available.

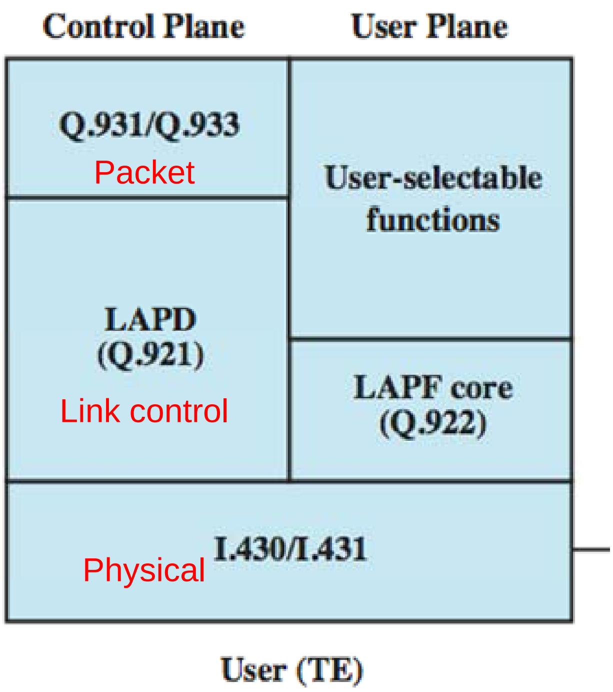
Frame relay Protocol Architecture



- Protocol contains two separate planes of operation:
  - control (C) plane,
    - between a subscriber and the network
    - Responsible of establishment and termination of logical connections,
  - user (U) plane,
    - end-to end functionality
    - which is responsible for the transfer of user data between subscribers.
- That means, a separate logical channel is used for control information.

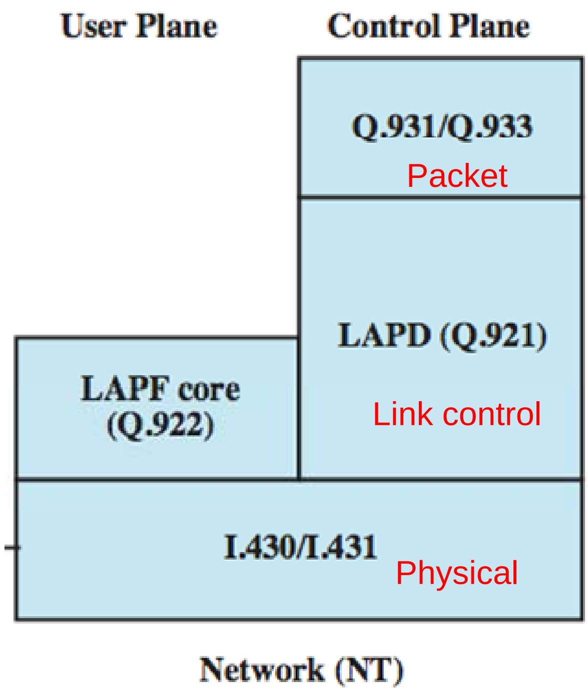
User& network/Control plane:

- Packet layer: Uses Q.933 control signaling messages for actual transfer of information between end users (end2end sequencing and error recovery)
- In link control layer LAPD (Q.921) is used to provide a reliable data link control service, with error control and flow control, between user (TE) and network (NT).
- Physical layer uses I.430/I431 signaling



Network/ User Plane:

- Physical layer uses: I.430/I431 signaling
- Link control layer: uses LAPF (Link Access Procedure for Frame) known as Q.22 protocol to
  - ensure frame is neither too long nor short
  - detection of transmission errors

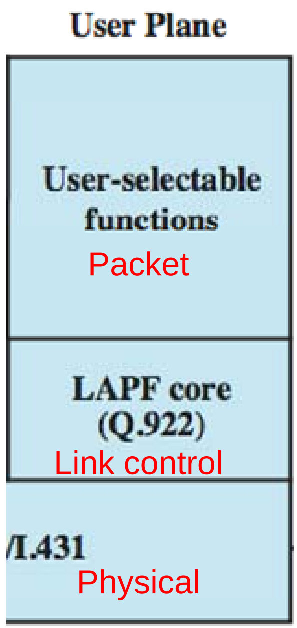


– congestion control functions
– frame mux and demux using addressing field
– ensure frame is integral number of octets

- The core functions of LAPF in the user/network plane constitute a sub-layer of the link layer.
- This provides the bare service of transferring data link
- frames from one subscriber to another, with no flow control or error control.

User/ user plan:

- the user may choose to select additional data link or network-layer end-to-end functions.
- These are not part of the frame relay service. Based on the core functions, a network offers frame relay as a connection-oriented link layer service with the following properties:
  – Preservation of the order of frame transfer from one edge of the network to the other
  – A small probability of frame loss



data link connections

- Frame relay uses data link connections rather than virtual circuits which used by X.25
- data transferred over them
- not protected by flow or error control
- uses separate connection for call control (unlike x.25)

frame format

- LAPF header, doesn't contain Control field, which means there is only one frame type, used for carrying user data.
- no sequence numbers.
- Contains
  - Flag and Frame Check Sequence (FCS) fields

– The information field carries higher-layer data.
– The address field has a default length of 2 octets and may be extended to 3 or 4 octets.
– It carries a data link connection identifier (DLCI) of 10, 16, or 23 bits.
– The DLCI serves the same function as the virtual circuit number in X.25.
– As in X.25, the connection identifier has only local significance: Each end of the logical connection assigns its own DLCI from the pool of locally unused numbers, and the network must map from one to the other.

Thanks,…