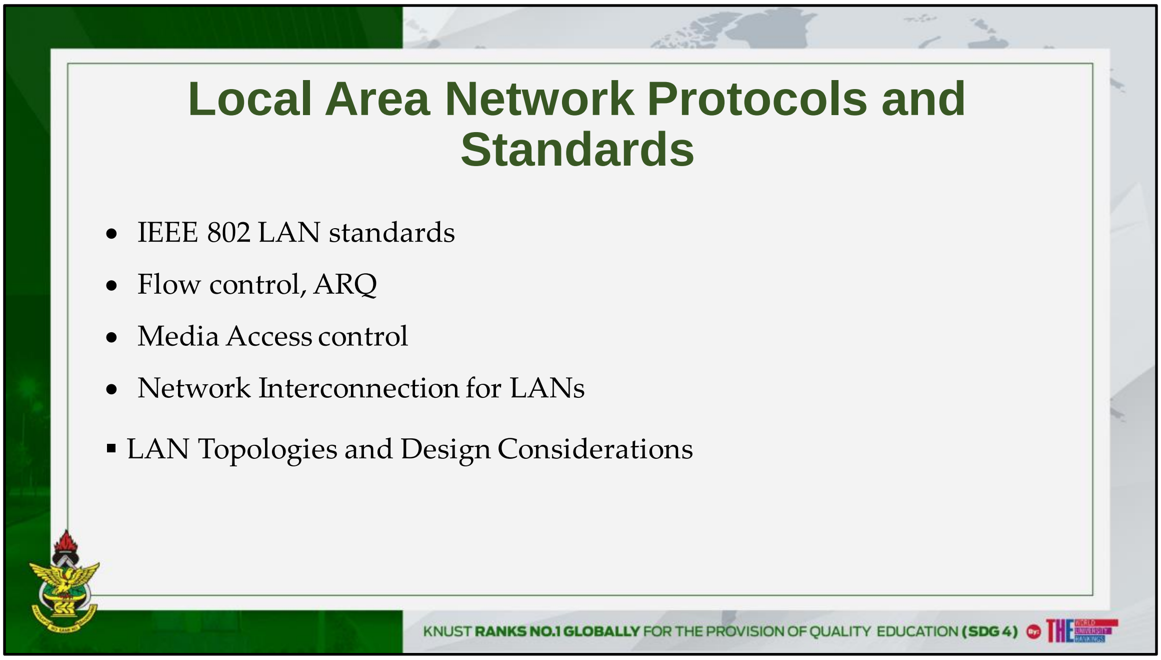
KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

COE 457
Computer Networking

Lecture 2:Local Area Network Protocols and Standards

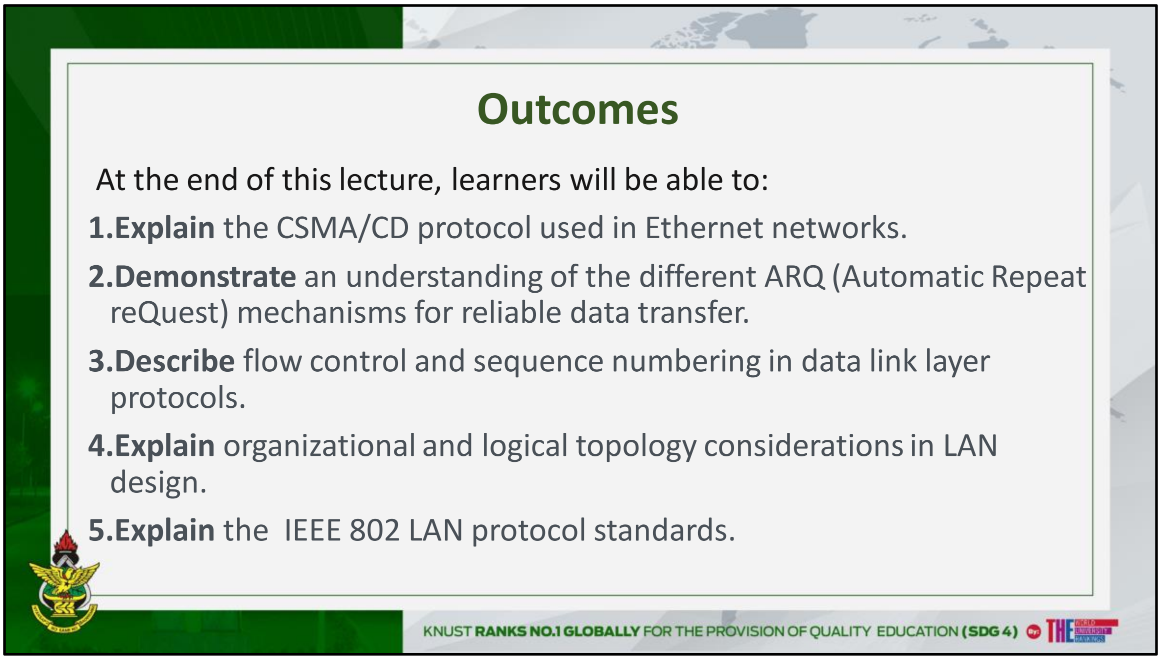
Ing. Prof. E. K. Akowuah
Email: ekakowuah.coe@knust.edu.gh
Room: 416, Caesar Building, College of Engineering
Linkedin: https://www.linkedin.com/in/ekakowuah/
Twitter: @ekakowuah

uro@knust.edu.gh | Follow KNUST on: Visit us at www.knust.edu.gh



Local Area Network Protocols and Standards

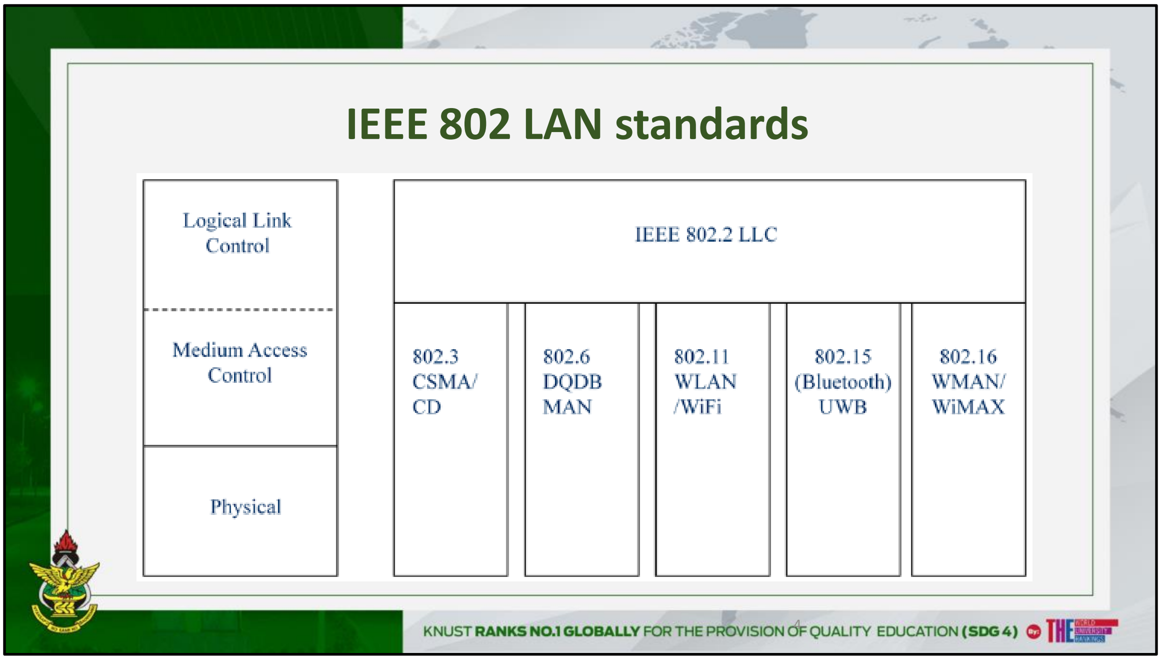
- IEEE 802 LAN standards
- Flow control, ARQ
- Media Access control
- Network Interconnection for LANs
- LAN Topologies and Design Considerations



Outcomes

At the end of this lecture, learners will be able to:

1. **Explain** the CSMA/CD protocol used in Ethernet networks.
2. **Demonstrate** an understanding of the different ARQ (Automatic Repeat reQuest) mechanisms for reliable data transfer.
3. **Describe** flow control and sequence numbering in data link layer protocols.
4. **Explain** organizational and logical topology considerations in LAN design.
5. **Explain** the IEEE 802 LAN protocol standards.



IEEE 802 LAN standards

Logical Link Control

Medium Access Control

Physical

IEEE 802.2 LLC

802.3 CSMA/ CD

802.6 DQDB MAN

802.11 WLAN /WiFi

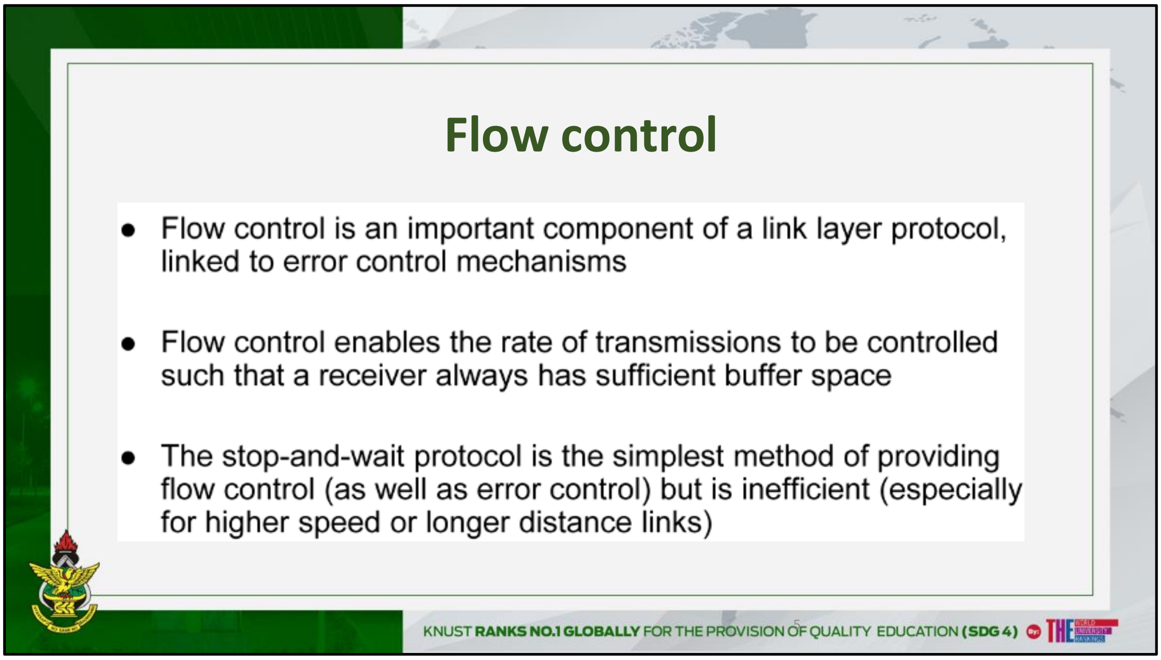
802.15 (Bluetooth) UWB

802.16 WMAN/ WiMAX

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The Data link layer is divided into two sublayers: Logical Link Control and Medium Access Control.
The MAC sublayer defines and implements the access protocol - it uses the Physical Layer to present the LLC with what looks like a link between the two communicating stations. The LLC performs the more typical layer 2 functions. With LANs there is no intermediate switching or routing nodes in the network - so the Network Layer is not necessary. Certain layer 3 type functions are present in LLC which must support the multi-access nature of the LAN.
LLC is independent of access protocol/network topology.

IEEE 802 includes a number of MAC/physical layer standards. For wired LANs, there are other standards such as 802.4 token bus and 802.5 token ring, but these are less used now. In this course we will concentrate mainly on the ubiquitous Ethernet CSMA/CD standard.
First, however, we will look at Data Link layer protocols and LLC.



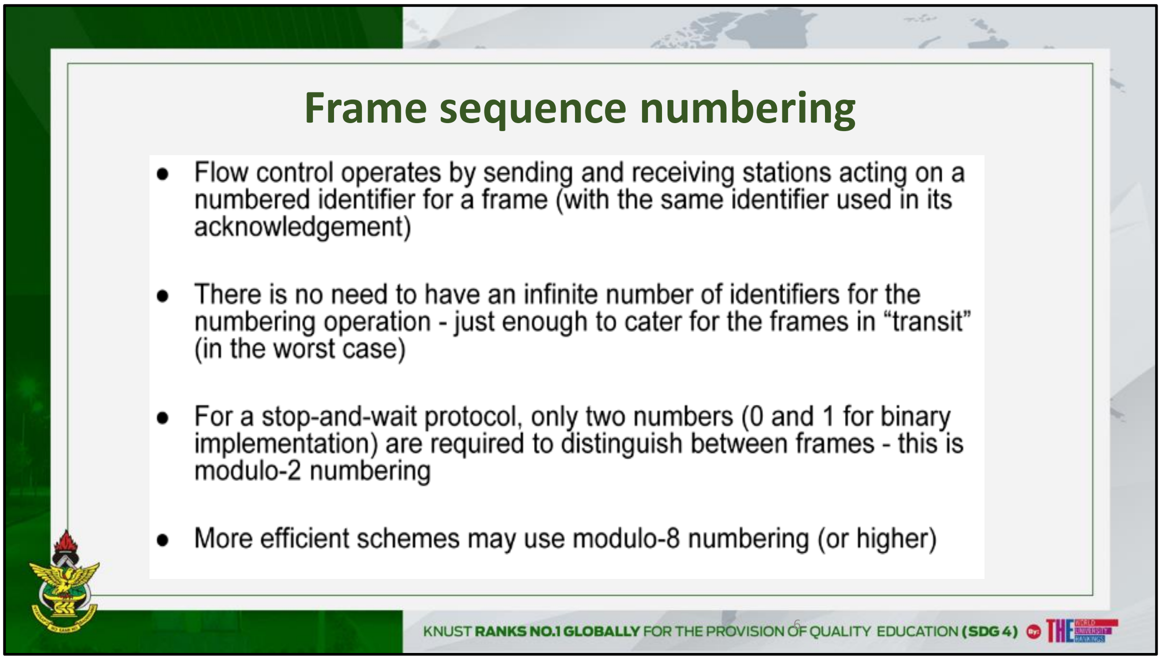
Flow control

- Flow control is an important component of a link layer protocol, linked to error control mechanisms
- Flow control enables the rate of transmissions to be controlled such that a receiver always has sufficient buffer space
- The stop-and-wait protocol is the simplest method of providing flow control (as well as error control) but is inefficient (especially for higher speed or longer distance links)

Flow control is an aspect of link layer control related to error control. Together they form the key
part of data link layer protocols.
The function of flow control is to enable the receiver to control the rate of transmissions from the
source so that it doesn’t receive more information than it can store in its buffers.
A stop-and-wait protocol can obviously be used, as this restricts transmission until the previous
transmission has been acknowledged. The receiver can delay acknowledgement until it is ready
to receive more data. However, stop-and-wait is inefficient for longer and higher-speed links. Flow control is an aspect of link layer control related to error control. Together they form the key part of data link layer protocols.

The function of flow control is to enable the receiver to control the rate of transmissions from the
source so that it doesn’t receive more information than it can store in its buffers.
A stop-and-wait protocol can obviously be used, as this restricts transmission until the previous

transmission has been acknowledged. The receiver can delay acknowledgement until it is ready to receive more data. However, stop-and-wait is inefficient for longer and higher-speed links.



Frame sequence numbering

- Flow control operates by sending and receiving stations acting on a numbered identifier for a frame (with the same identifier used in its acknowledgement)
- There is no need to have an infinite number of identifiers for the numbering operation - just enough to cater for the frames in "transit" (in the worst case)
- For a stop-and-wait protocol, only two numbers (0 and 1 for binary implementation) are required to distinguish between frames - this is modulo-2 numbering
- More efficient schemes may use modulo-8 numbering (or higher)

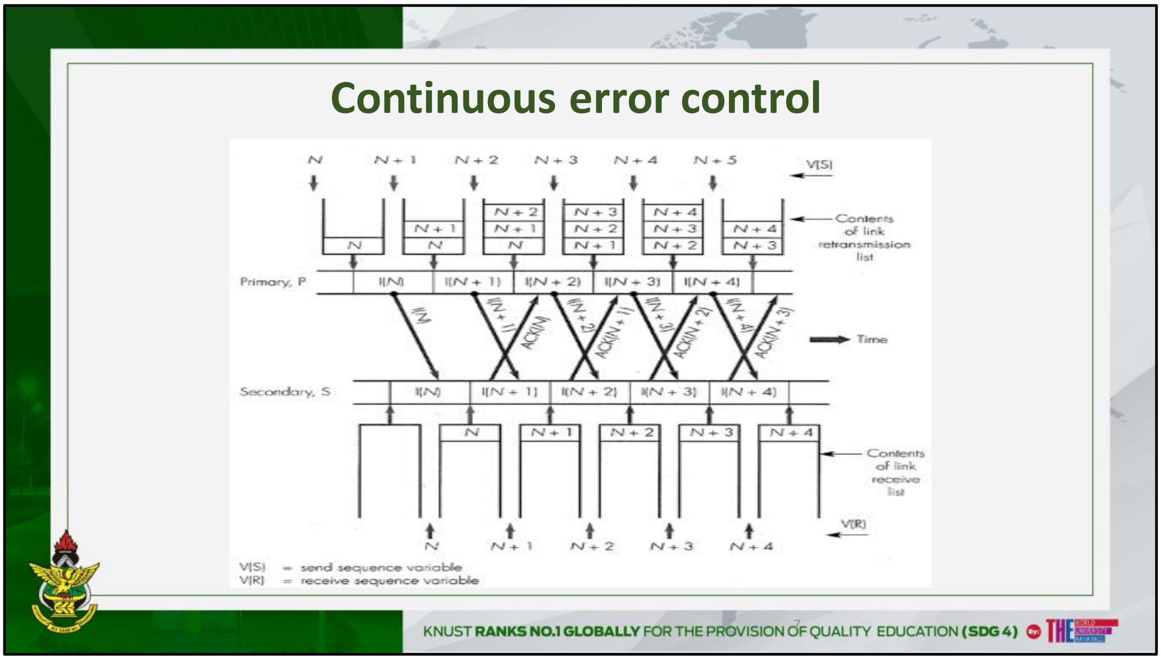
By using numbered frames, flow control can operate on sequences of frames, not just one frame at a time. Acknowledgements are for particular numbered frames (or, alternatively, for all frames up to that number).

We will see that we do not have to have an infinite number of identifiers (numbers) for frames.

Frames can be numbered modulo-2n - we just need enough numbers for the frames in "transit" in the worst case.

For stop-and-wait, as we only need to make sure that we can distinguish between one frame and the next, modulo-2 numbering is sufficient.

Other schemes may use 3-bit modulo-8 numbering (or 7-bit, modulo-128 numbering).



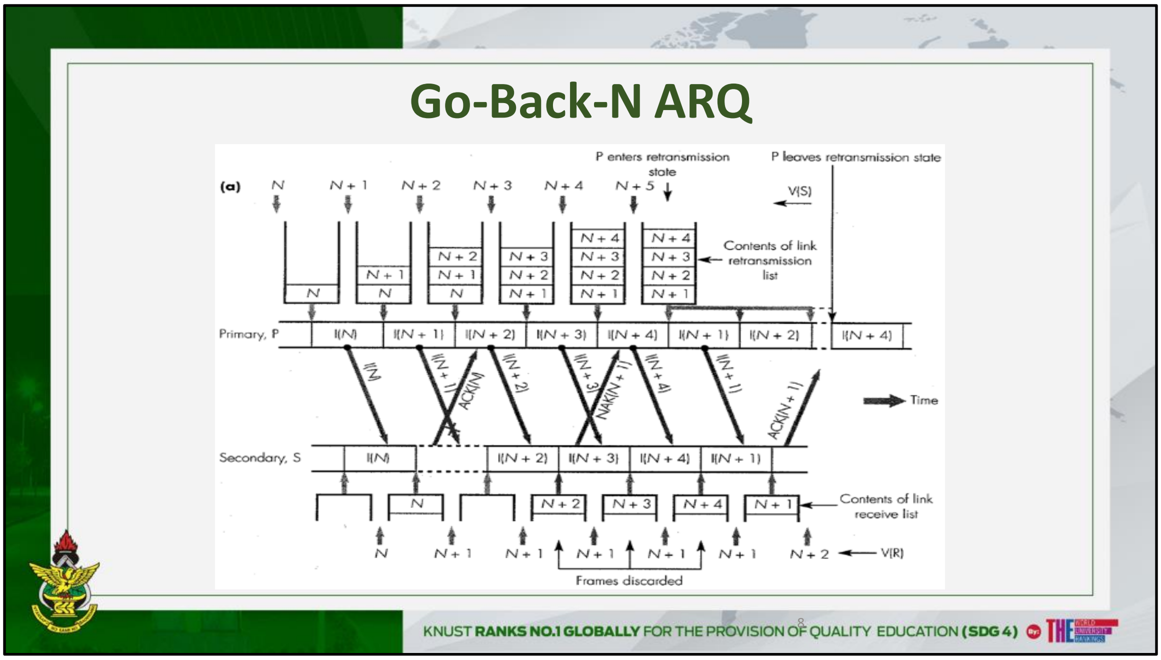
Continuous error control

7

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE

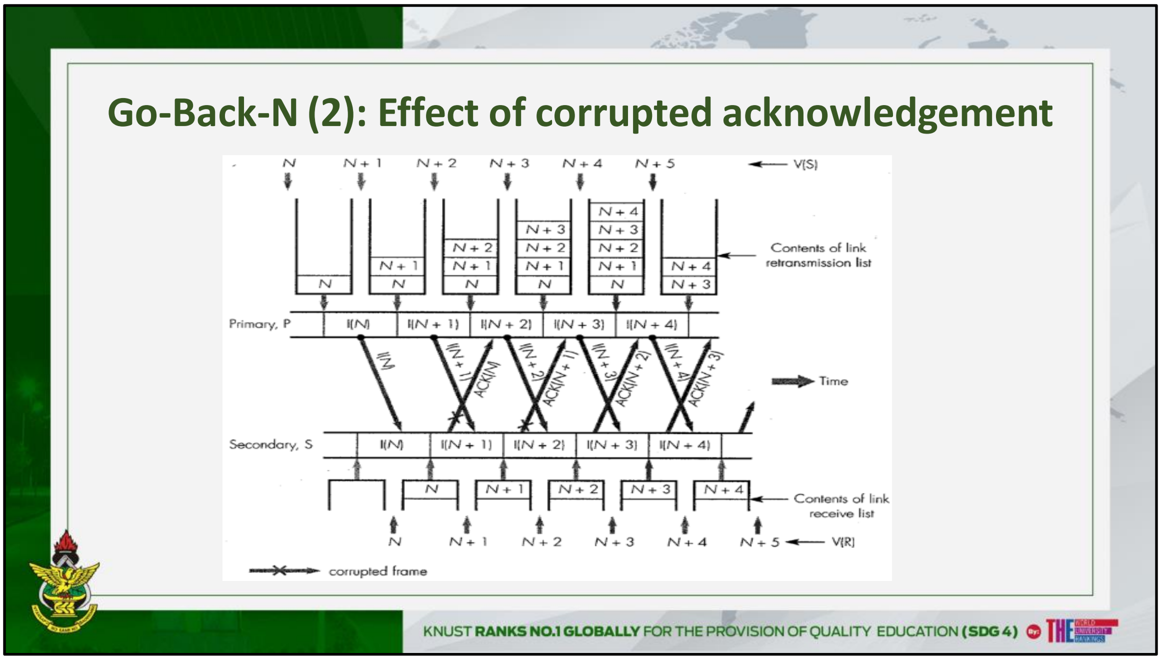
With a continuous ARQ control scheme, link utilisation is improved at the expense of increased
buffer storage requirements.
The Primary (P), sending station sends frames continuously without waiting for acknowledgement
for each one. A copy of each information (I) frame is kept in a retransmission list, until it is acknowledged.

The secondary (S), receiving station uses acknowledgement (ACK) frames containing the unique
identifier of the I frame being acknowledged.
Error free frames are placed in a receive list for further processing. Immediately when processed,
the information content in the frame is passed to the next protocol layer.
The response to erroneous frames depends on the continuous ARQ protocol being used.



Go-Back-N ARQ

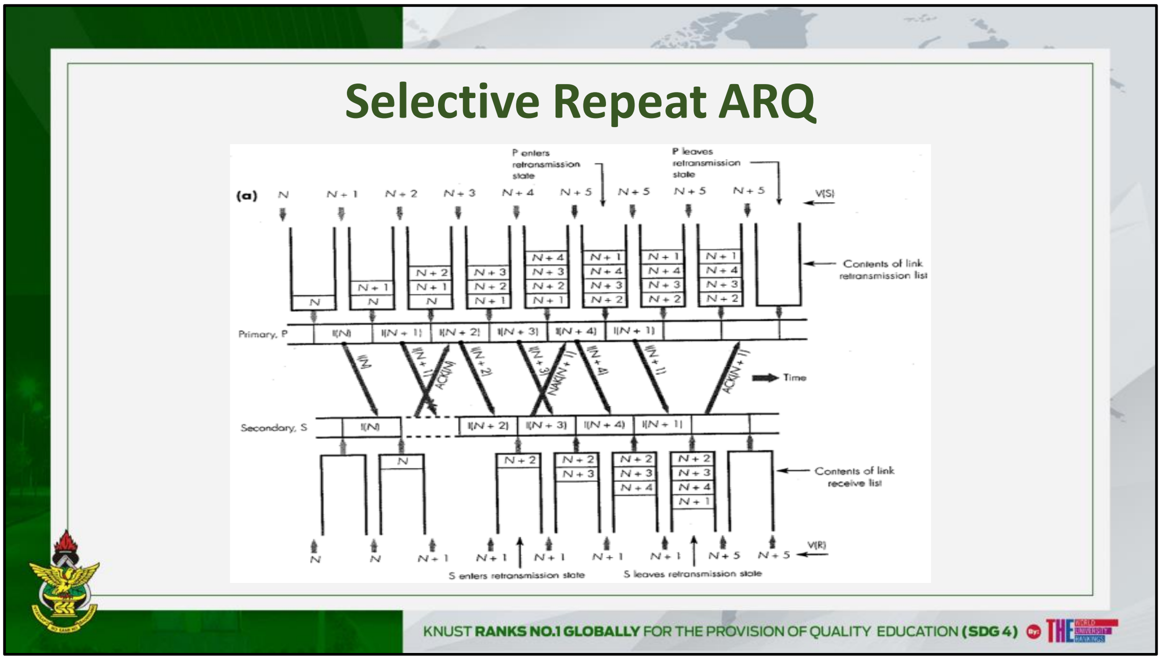
In the go-back-N retransmission control scheme if a frame is corrupted {I(N+1)} the next one
{I(N+2)} is received out-of-sequence.
The secondary then returns a {NAK(N+1)} negative acknowledgement frame corresponding to the missing frame.
On receiving the negative acknowledgement, the primary enters the retransmission state, and
commences to retransmit all frames awaiting acknowledgement in the retransmission list.
The secondary discards all frames until it receives the missing I-frame {I(N+1)} at which point it
resumes accepting frames and returning acknowledgements.
If the secondary did not receive an in-sequence frame after its first NAK, a timeout is applied and
a second NAK would be sent.



Go-Back-N (2): Effect of corrupted acknowledgement

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The above shows the effect of corrupted acknowledgement frames: ACK(N) and ACK(N+1) are
corrupted.
On receipt of ACK(N+2) the primary detects that there are two outstanding information frames in
the retransmission list. Since this is a positive acknowledgement, based on the protocol, the
primary can assume that these two frames have been received correctly. Hence, ACK(N+2) acts
as an acknowledgement for all frames up to I(N+2) in the list.
In most implementations the sequence number variable used in the acknowledgement is actually
that of the next frame expected rather than that of the one just received.
The acknowledgement frame is called a receive ready (RR) frame; the negative acknowledgement frame a reject (REJ) frame.

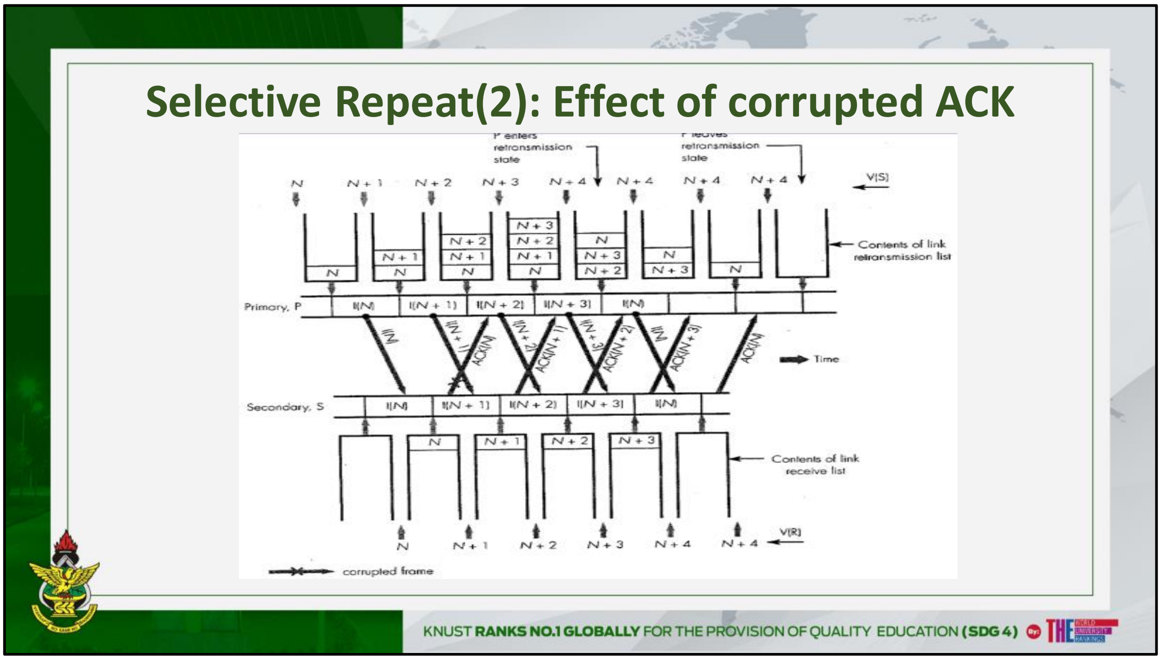


Selective Repeat ARQ

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)**

In the selective repeat scheme, a receive list containing more than one frame buffer is required.
When the secondary detects an out-of-sequence I frame, it returns a NAK frame for the missing I
frame. The NAK frame is a selective reject (SREJ) frame in most implementations.
Having sent the NAK frame, the secondary enters the retransmission state, and does not send any acknowledgements until it receives the missing frame.

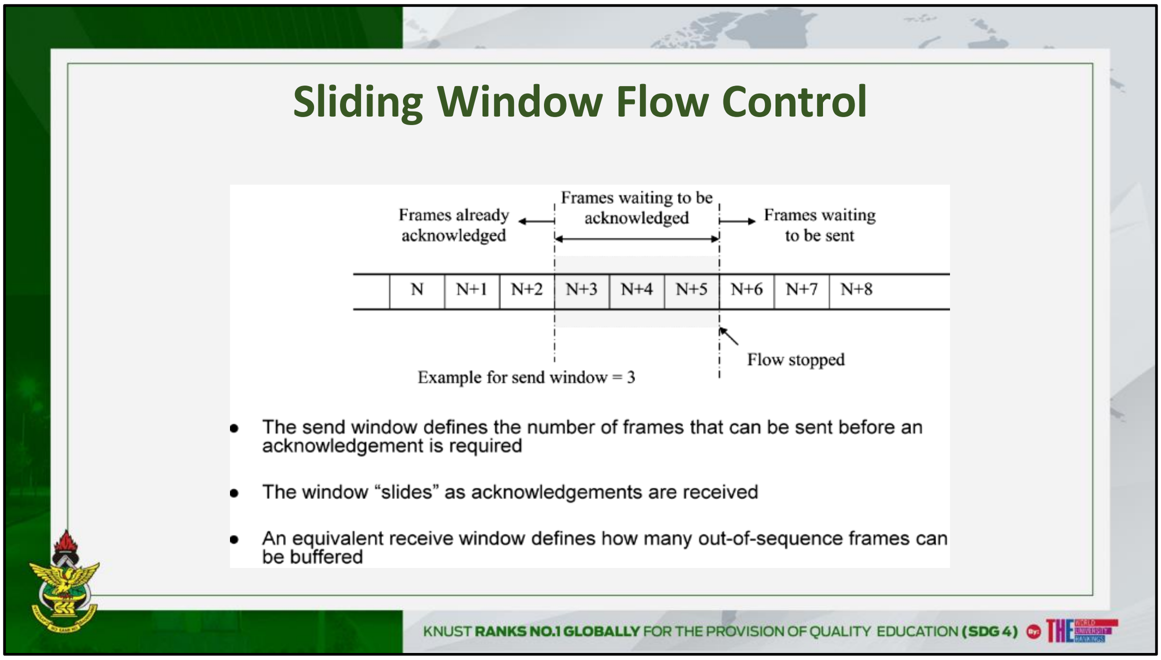
On receipt of the NAK frame, the primary enters the retransmission state too. It resends the
missing I frame, and suspends sending any new frames until it receives an acknowledgement.
On receiving the missing I-frame, the secondary leaves the retransmission state and resumes
sending acknowledgements. *ACK(N+4) acknowledges all frames up to N+4 including the missing
frame.*



Selective Repeat(2): Effect of corrupted ACK

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

If the ACK frame is corrupted, then on receipt of the next ACK frame, say for N+1, the primary will
retransmit I frame N.
On receipt of the retransmitted I-frame, the secondary realises from its receive sequence variable
that this is a duplicate and can be discarded. It returns another ACK for the frame, so that the
primary can remove it from its retransmission list.
Selective repeat ARQ generally requires fewer retransmissions than go-back-N.
However, go back-N is more popular, because:
a. the receiver does not require a buffer
b. the receiver does not require logic circuitry to re-order out-of-sequence frames
c. the transmitter is less complex as it does not have to deal with sending out-of-sequence frames
(it goes back and repeats in-sequence).



Sliding Window Flow Control

Frames already acknowledged

Frames waiting to be acknowledged

Frames waiting to be sent

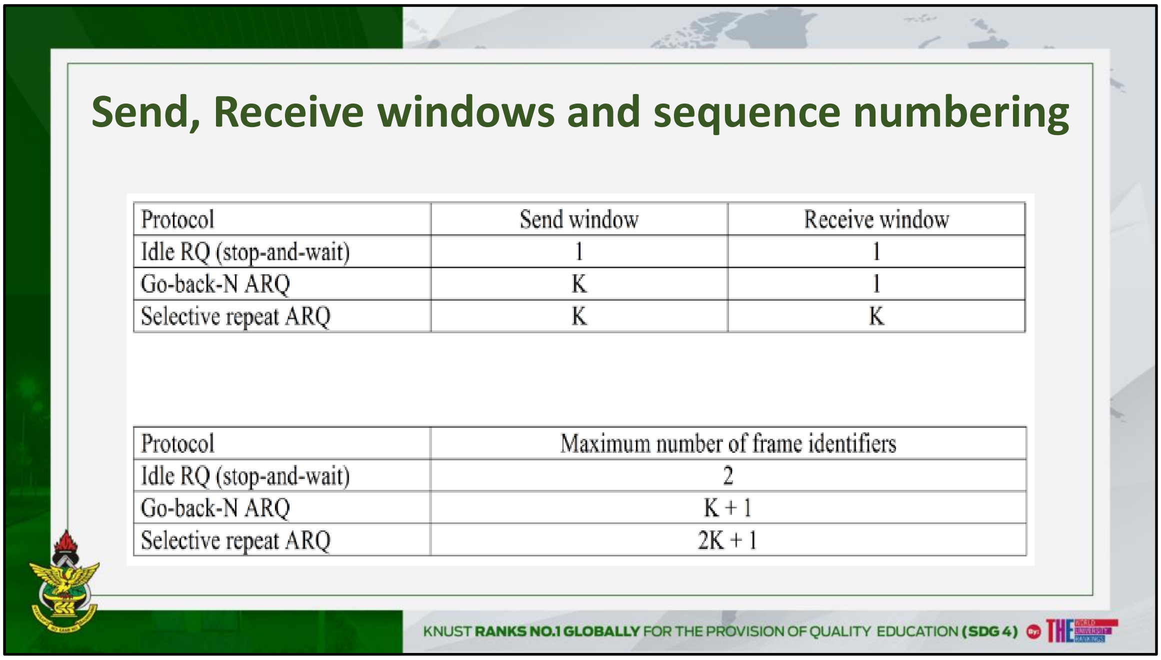
N	N+1	N+2	N+3	N+4	N+5	N+6	N+7	N+8

Flow stopped

Example for send window = 3

- The send window defines the number of frames that can be sent before an acknowledgement is required
- The window “slides” as acknowledgements are received
- An equivalent receive window defines how many out-of-sequence frames can be buffered

Continuous ARQ protocols use sliding-window flow control.
The send window defines how may frames can be sent without an acknowledgement. When this
number is reached, transmissions must be stopped until an acknowledgement is received. The
window slides as acknowledgements are received.
An equivalent receive window defines how many out-of-sequence frames can be accepted. For
go-back-N, the receive window is 1 - only in-sequence information frames are accepted.



Send, Receive windows and sequence numbering

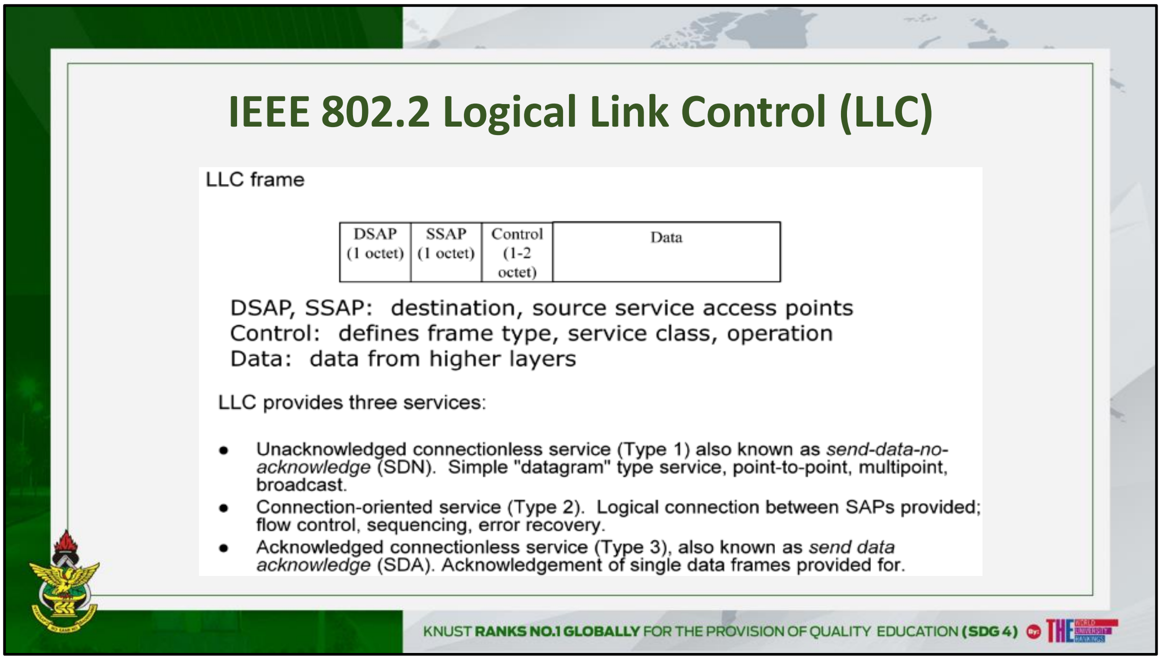
Protocol	Send window	Receive window
Idle RQ (stop-and-wait)	1	1
Go-back-N ARQ	K	1
Selective repeat ARQ	K	K

Protocol	Maximum number of frame identifiers
Idle RQ (stop-and-wait)	2
Go-back-N ARQ	K + 1
Selective repeat ARQ	2K + 1

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

As was said earlier, we don’t need an infinite number of identifiers - only enough to identify the frames in transit.

The above tables show the send and receive window sizes for the different ARQ protocols. It can be seen that for a given number of available frame identifiers, for selective-repeat, the largest send window must be smaller than for a go-back-N protocol as the secondary must be
able to distinguish between all K frames it may have in its receive window and any K newly transmitted frames in the primary’s send window.



IEEE 802.2 Logical Link Control (LLC)

LLC frame

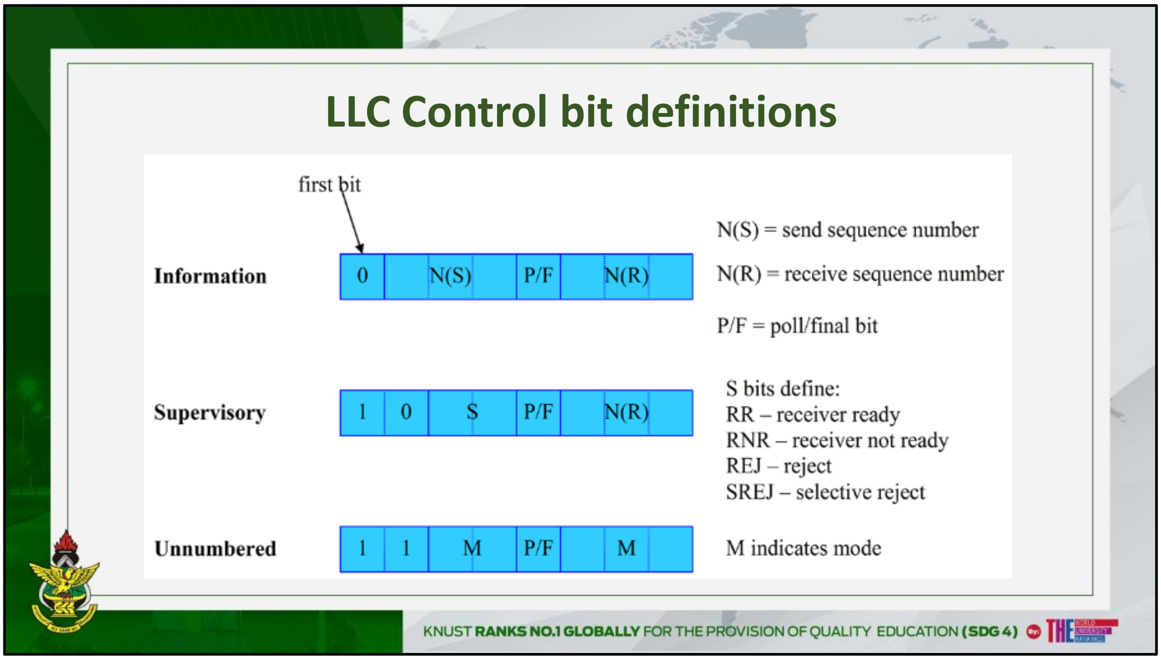
DSAP (1 octet)	SSAP (1 octet)	Control (1-2 octet)	Data

DSAP, SSAP: destination, source service access points
Control: defines frame type, service class, operation
Data: data from higher layers

LLC provides three services:

- Unacknowledged connectionless service (Type 1) also known as *send-data-no-acknowledge* (SDN). Simple "datagram" type service, point-to-point, multipoint, broadcast.
- Connection-oriented service (Type 2). Logical connection between SAPs provided; flow control, sequencing, error recovery.
- Acknowledged connectionless service (Type 3), also known as *send data acknowledge* (SDA). Acknowledgement of single data frames provided for.

LLC provides for typical layer 2 functions such as end-to-end error control and acknowledgement, and simple flow control; as in ISO’s HDLC on which it is based.
It also needs to support certain layer 3 type functions:
- provision of connectionless and connection-oriented services (can do this because no routing is required).
- multiplexing, use of service access points allows multiple processes to communicate.
- provision of multicast, broadcast transmission.
The control field enables the provision of different types of services and transmission.



LLC Control bit definitions

first bit

Information	0	N(S)	P/F	N(R)
Supervisory	1 0	S	P/F	N(R)
Unnumbered	1 1	M	P/F	M

N(S) = send sequence number

N(R) = receive sequence number

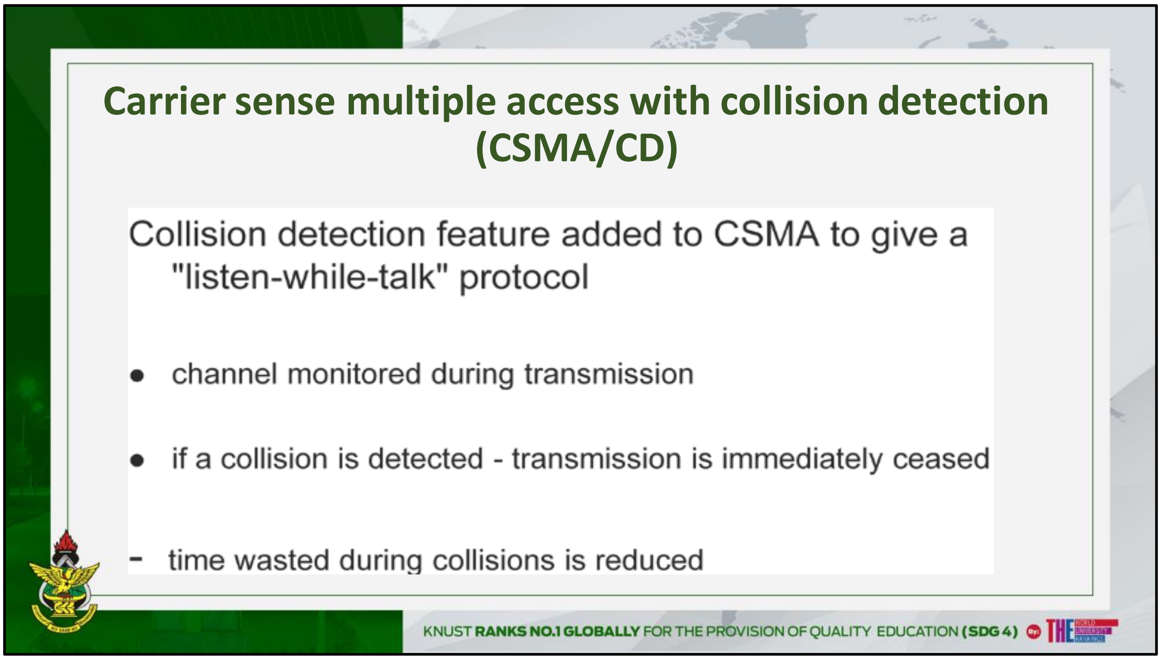
P/F = poll/final bit

S bits define:
RR – receiver ready
RNR – receiver not ready
REJ – reject
SREJ – selective reject

M indicates mode

LLC Type 2 uses “piggy-back acknowledgements”. This means that it is not necessary to send special acknowledgement frames if the information transfer is two-way.

When this are no return information frames, supervisory frames are used (for ACK and NAK).
3-bit sequence numbers allow for modulo-8 numbering. Extended sequence number fields of 7-
bits can also be used. Modes such as this, and link establishment/disconnection etc. are set by
the use of the unnumbered frames.
Extended numbering may be useful in higher-speed, longer distance links - but increase buffer
storage requirements.
The P/F bit is set in frames which must be acknowledged (and in their acknowledgements).
SDN uses unnumbered information frames.
SDA uses two new unnumbered information frames with 1 bit sequence number (1 or 0). The
number is the same in the data frame and acknowledgement frame.



Carrier sense multiple access with collision detection (CSMA/CD)

Collision detection feature added to CSMA to give a "listen-while-talk" protocol

- channel monitored during transmission
- if a collision is detected - transmission is immediately ceased

- time wasted during collisions is reduced

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

The CSMA/CD protocol was originally developed by the Xerox Corporation, and then by DEC, Intel and Xerox into the popular Ethernet standard. The IEEE 802.3 standard is based on Ethernet.

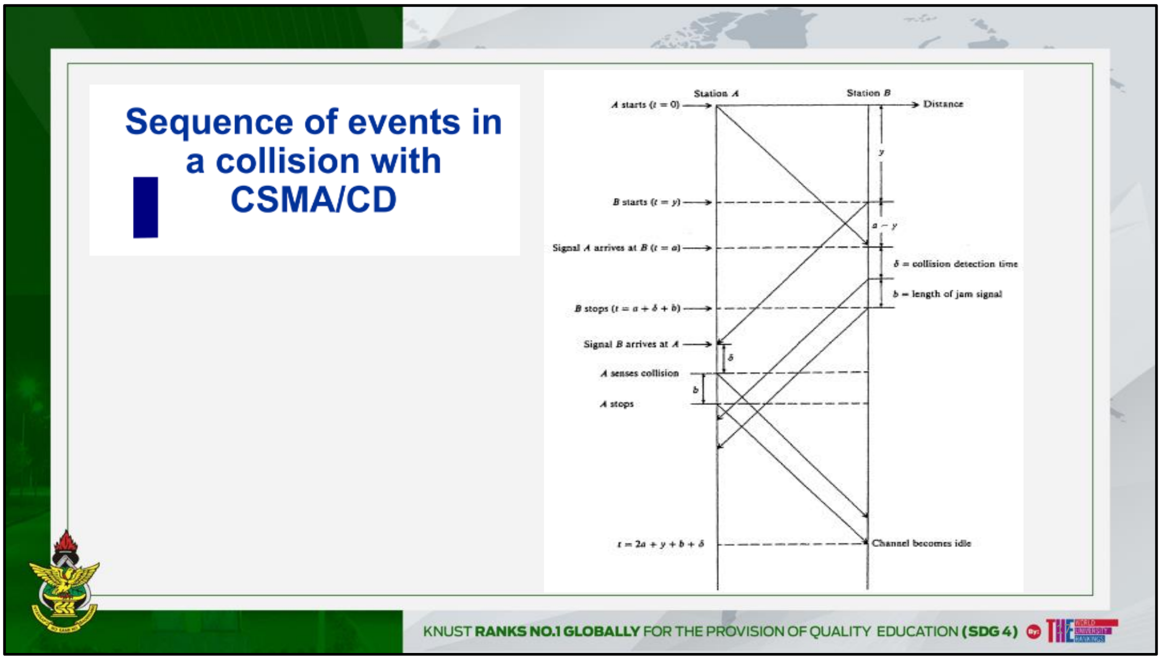
CSMA/CD is a listen-while-talk protocol - the channel is monitored not just before transmission but during transmission as well. If a collision is detected, then transmission is immediately ceased.

A brief jamming signal is sent to warn other stations that a collision has occurred - and the station then backs off.

The vulnerable period is the same as with CSMA - but the time wasted during collisions is reduced because transmission is ceased.

Although any of the three persistence algorithms specified for CSMA could be used, both Ethernet and IEEE 802.3 use 1-persistent to minimise wasted channel idle time.

Instability is minimised by the use of a "truncated binary exponential back-off" algorithm.



Sequence of events in a collision with CSMA/CD

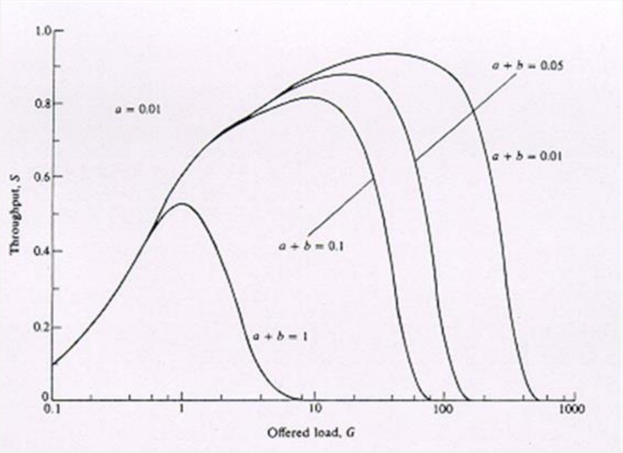
KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

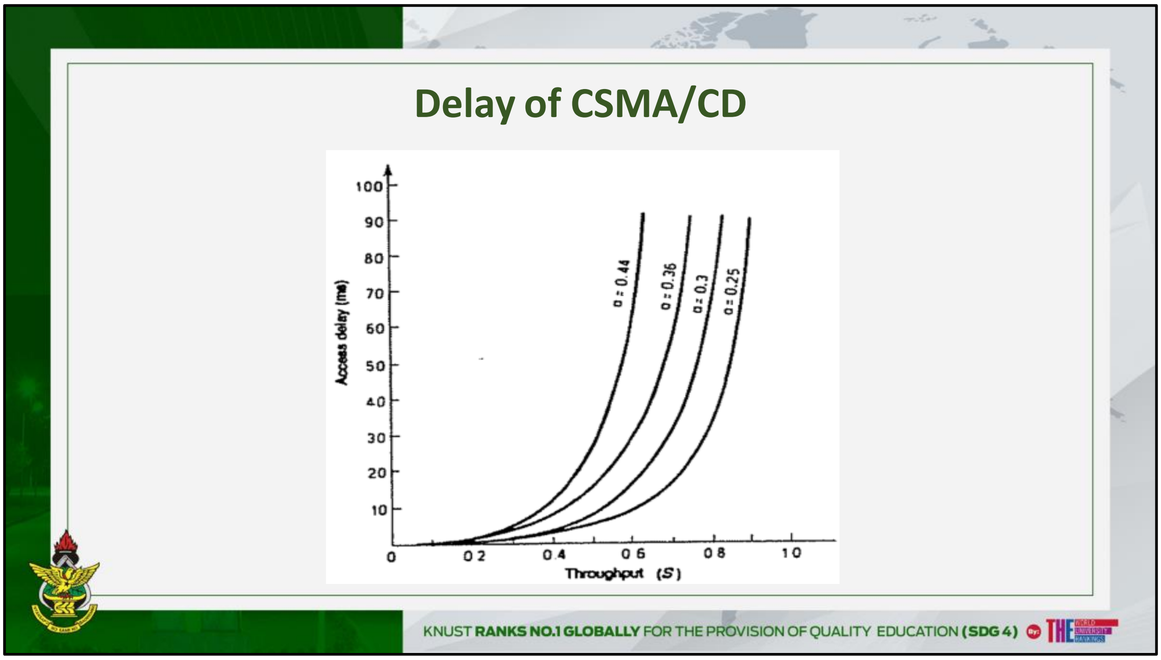
In the sequence of events in a collision using the CSMA/CD protocol, the variable *Y is again* random, dependent on the arrival statistics of packets - this is the same as the variable *Y in the* analysis of the collision for CSMA. It can be seen from the sequence of events that the busy period with a collision is $2a + b + \delta + Y$, *where b is the length of the jamming signal and δ is the* time it takes a station to identify a collision. This compares with an equivalent busy period of $1 + a + Y$ *for CSMA. Therefore, if* $a + b + \delta < 1$ *CSMA/CD reduces the wasted time due to* collisions. Usually $a + b + \delta << 1$, *with* $\delta \rightarrow 0$. It can also be seen that no advantage is gained if a > 1.

There is another more important reason why the packet transmission time should be kept long. If station A stopped transmitting its first packet, and then started transmitting a second packet before the signal from B arrived at A, then A would only detect a collision during its second packet, even though the first was in collision as well. In order that the packets involved in collisions are unambiguously identifiable, the packet transmission time must be

greater than twice
the end-to-end delay, or *a < 0.5. Short packets are "padded" out to ensure this.*

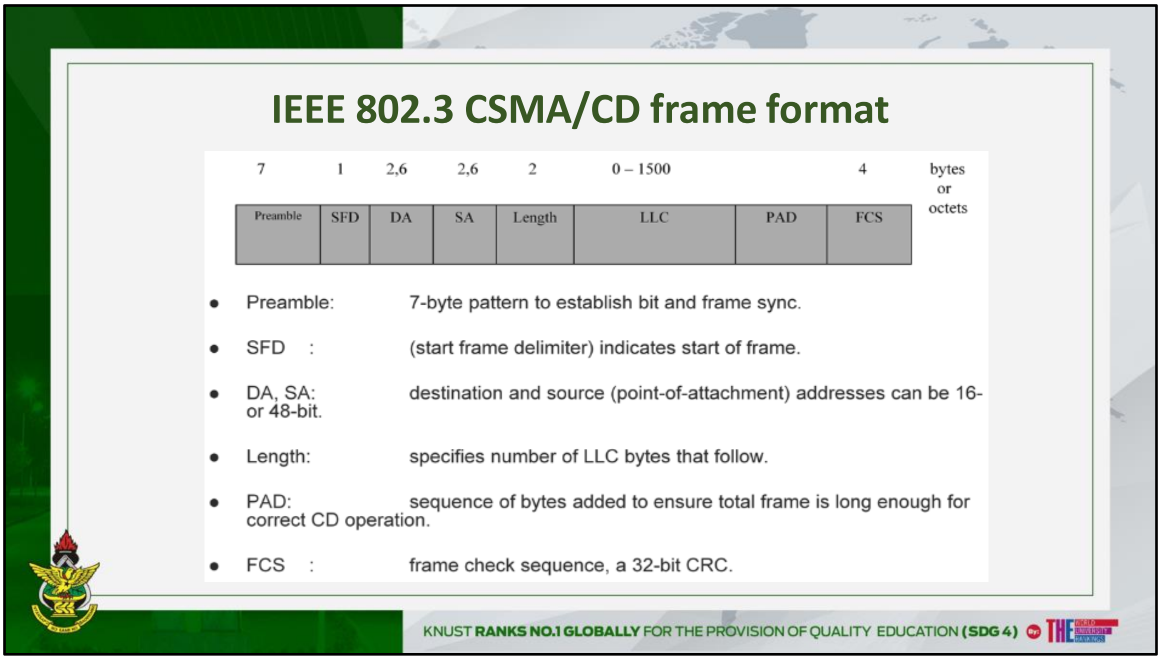
Throughput of CSMA/CD





Delay of CSMA/CD

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS



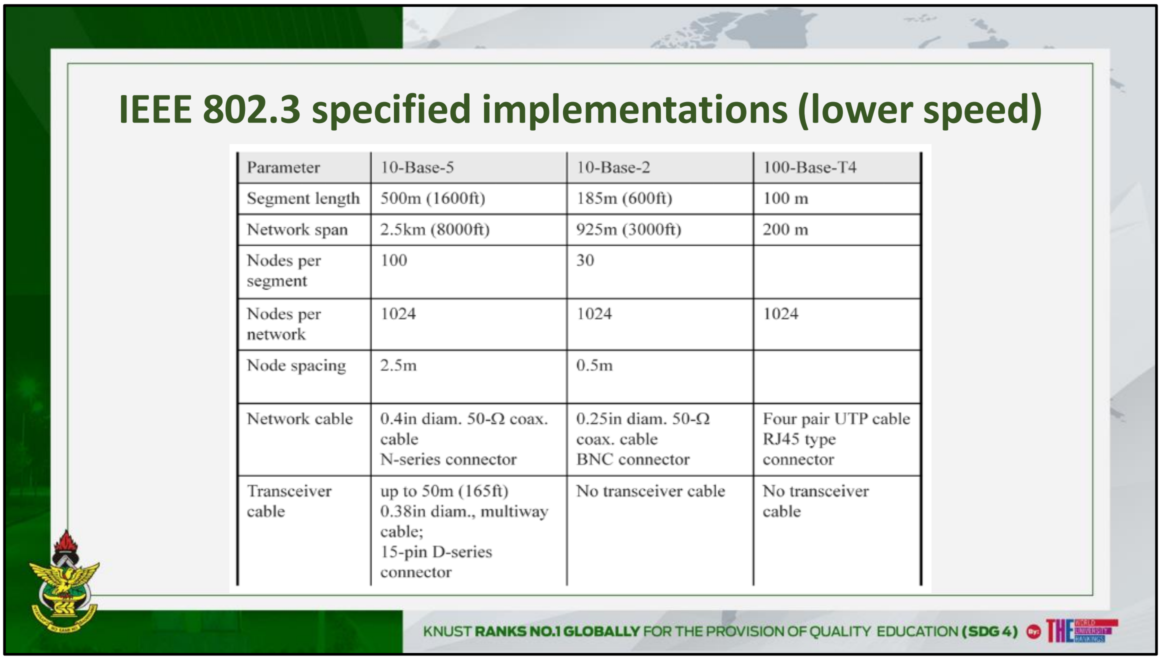
IEEE 802.3 CSMA/CD frame format

7	1	2,6	2,6	2	0 – 1500		4	bytes or octets
Preamble	SFD	DA	SA	Length	LLC	PAD	FCS	

- Preamble: 7-byte pattern to establish bit and frame sync.
- SFD : (start frame delimiter) indicates start of frame.
- DA, SA: destination and source (point-of-attachment) addresses can be 16- or 48-bit.
- Length: specifies number of LLC bytes that follow.
- PAD: sequence of bytes added to ensure total frame is long enough for correct CD operation.
- FCS : frame check sequence, a 32-bit CRC.

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

The preamble enables bit synchronisation and the location of the start of the frame. The destination and source addresses correspond to stations attached to the LAN; through SAPs a number of processes may be communicating via these points of attachment. The PAD field is required to maintain the condition for correct collision detection operation that $a < 0.5$. *IEEE 802.3* specifies that the combined length of the LLC and PAD fields must be between 46 and 1500 bytes. If the length field indicates that the LLC data is less than 46 bytes then an integer number of bytes are added in the PAD field to bring this combined length up to 46.

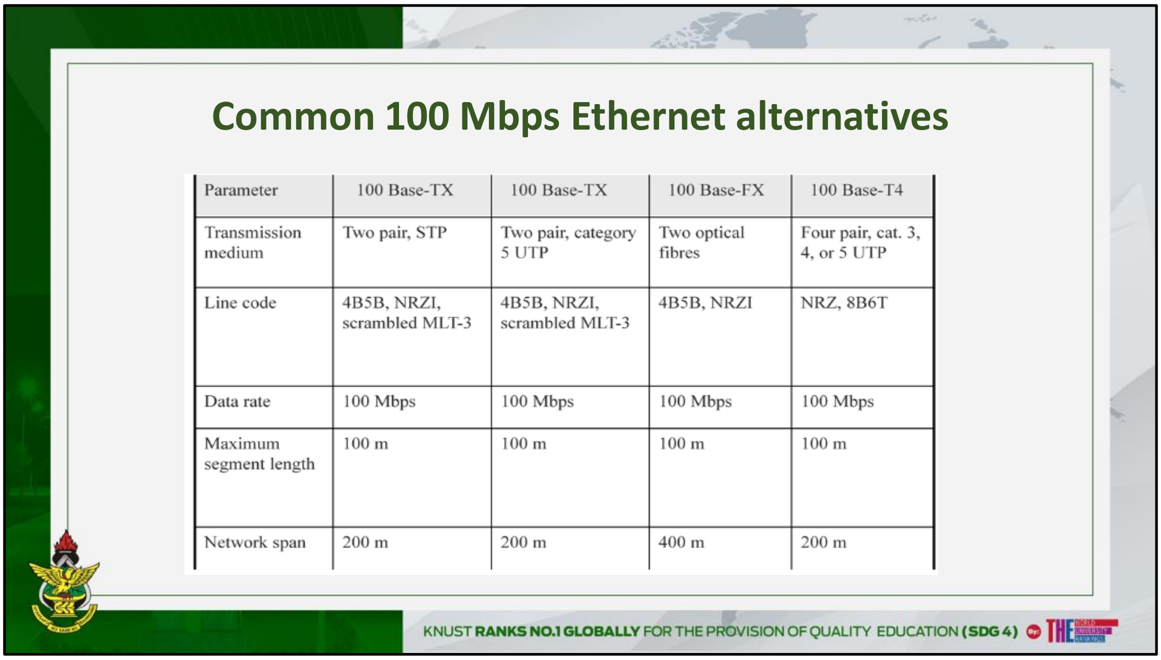


IEEE 802.3 specified implementations (lower speed)

Parameter	10-Base-5	10-Base-2	100-Base-T4
Segment length	500m (1600ft)	185m (600ft)	100 m
Network span	2.5km (8000ft)	925m (3000ft)	200 m
Nodes per segment	100	30	
Nodes per network	1024	1024	1024
Node spacing	2.5m	0.5m	
Network cable	0.4in diam. 50-Ω coax. cable N-series connector	0.25in diam. 50-Ω coax. cable BNC connector	Four pair UTP cable RJ45 type connector
Transceiver cable	up to 50m (165ft) 0.38in diam., multiway cable; 15-pin D-series connector	No transceiver cable	No transceiver cable

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

Signal attenuation cannot be too great otherwise collision detection cannot function, this usually operates on signal levels. This sets a limit on the segment length.
To allow the network to meet allowable propagation delay criteria, the network span is limited. 10-Base-5 also allows only two repeaters between any two stations.
Other CSMA/CD implementations based on IEEE 802.3 have been developed.
StarLAN, developed by AT & T, operates using twisted-pair (telephone) cable bundles at 1 Mbps.
A hierarchial configuration of hubs is used.
In the 1 and 10 Mbps implementations Manchester code is used.
Optical-fibre and high-speed Ethernets also tend to use hub configurations. The 100-Base-T4
specification allows the use of ordinary voice grade twisted pair cable for 100 Mbps operation.



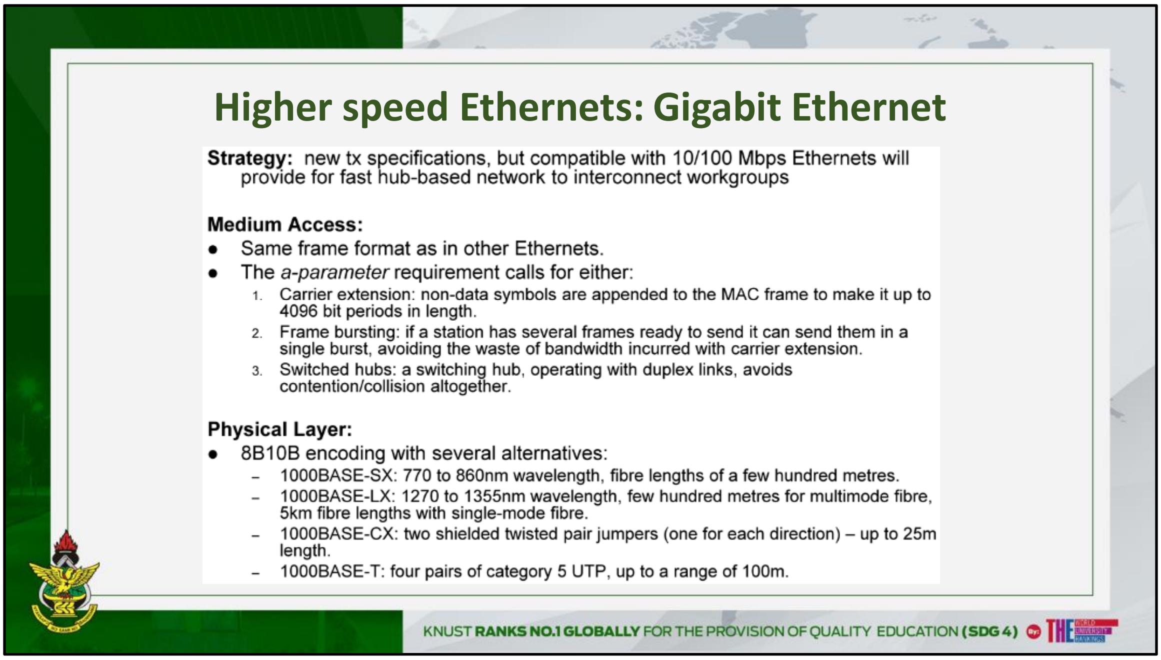
Common 100 Mbps Ethernet alternatives

Parameter	100 Base-TX	100 Base-TX	100 Base-FX	100 Base-T4
Transmission medium	Two pair, STP	Two pair, category 5 UTP	Two optical fibres	Four pair, cat. 3, 4, or 5 UTP
Line code	4B5B, NRZI, scrambled MLT-3	4B5B, NRZI, scrambled MLT-3	4B5B, NRZI	NRZ, 8B6T
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m

The increased use of mulitmedia and other high network usage applications led to the
development of higher bandwidth Ethernet standards.
Hub configurations are used. Collision detection is carried out by the hub - it can detect if it
receives two overlapping transmissions. It then transmits a jamming signal on all of its outputs.
Otherwise non-colliding frames are repeated on all output links. Thus although we have a star
wiring topology, logically the network performs in the same manner as a bus topology CSMA/CD
system.
Manchester code is not used in these 100 Mbps as it would require a signalling rate of 200
Mbaud. The 4B5B code increases the signalling rate to just 125 Mbaud. This code with NRZI
(inversion for 1, same level for 0) can be used to directly intensity modulate optical transmitters.
For twisted pair cable, the signalling rate is still too high and dc balance is required.

These requirements are met by scrambling and using a ternary level code (MLT-3).

In some installations it may be preferable to use already installed lower grade unshielded twisted pair. Four pairs are required to transmit the 100 Mbps data. Two pairs are unidirectional and provide for the collision detection and jamming signals. The other two pairs are bidirectional.
Thus three pairs are used for transmission in each direction. Together with the use of ternary 8B6T signalling (which aids synchronisation and balance) this reduces the overall signalling rate on each pair to 25 Mbaud.
Again, whereas attenuation restricts the segment length (ie for each hub repeater), the network span is limited by the maximum “collision domain” - the *a parameter requirement for CSMA/CD* networks.



Higher speed Ethernets: Gigabit Ethernet

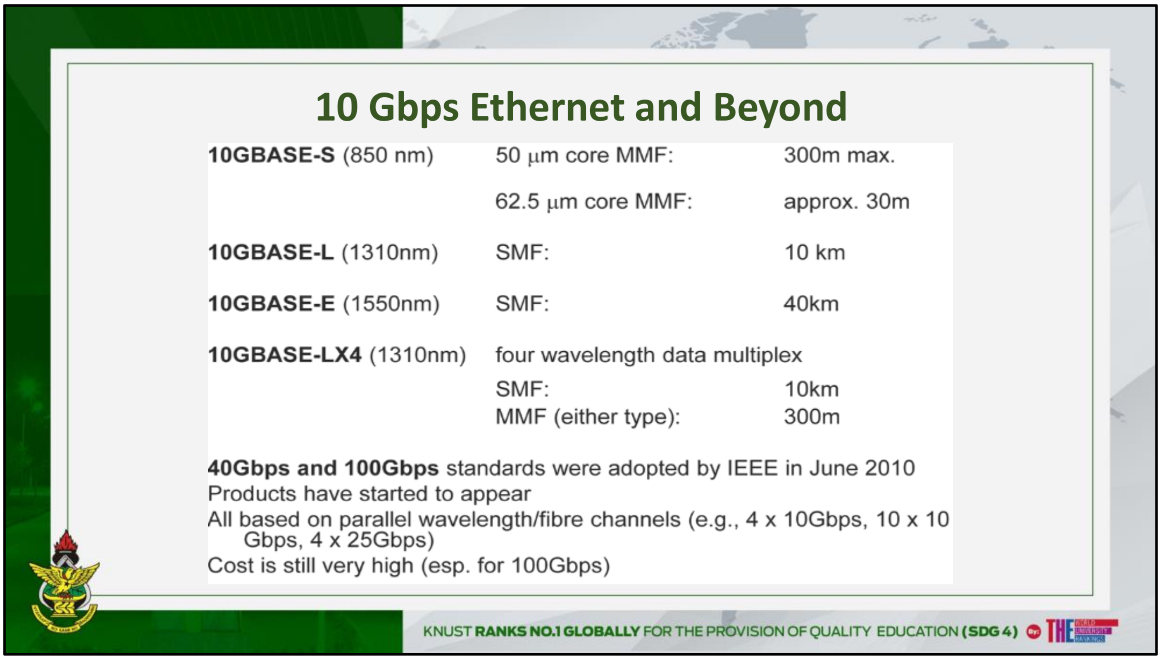
Strategy: new tx specifications, but compatible with 10/100 Mbps Ethernets will provide for fast hub-based network to interconnect workgroups

Medium Access:

- Same frame format as in other Ethernets.
- The *a-parameter* requirement calls for either:
  1. Carrier extension: non-data symbols are appended to the MAC frame to make it up to 4096 bit periods in length.
  2. Frame bursting: if a station has several frames ready to send it can send them in a single burst, avoiding the waste of bandwidth incurred with carrier extension.
  3. Switched hubs: a switching hub, operating with duplex links, avoids contention/collision altogether.

Physical Layer:

- 8B10B encoding with several alternatives:
  - 1000BASE-SX: 770 to 860nm wavelength, fibre lengths of a few hundred metres.
  - 1000BASE-LX: 1270 to 1355nm wavelength, few hundred metres for multimode fibre, 5km fibre lengths with single-mode fibre.
  - 1000BASE-CX: two shielded twisted pair jumpers (one for each direction) – up to 25m length.
  - 1000BASE-T: four pairs of category 5 UTP, up to a range of 100m.



10 Gbps Ethernet and Beyond

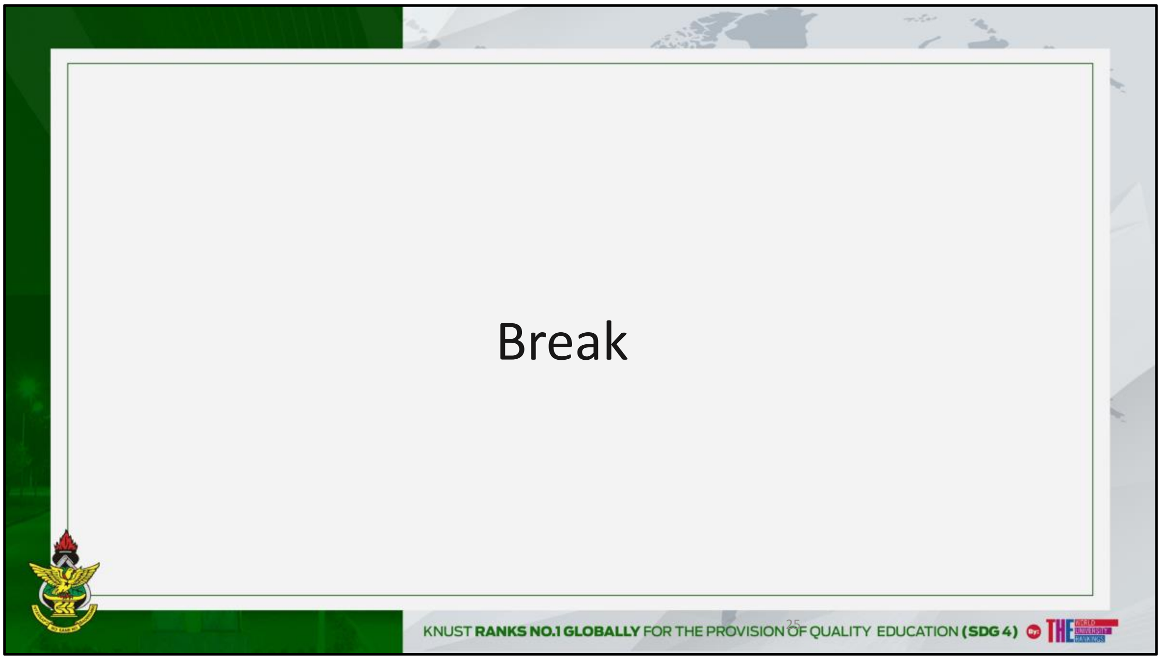
10GBASE-S (850 nm)	50 μm core MMF:	300m max.
	62.5 μm core MMF:	approx. 30m
10GBASE-L (1310nm)	SMF:	10 km
10GBASE-E (1550nm)	SMF:	40km
10GBASE-LX4 (1310nm)	four wavelength data multiplex	
	SMF:	10km
	MMF (either type):	300m

40Gbps and 100Gbps standards were adopted by IEEE in June 2010
Products have started to appear
All based on parallel wavelength/fibre channels (e.g., 4 x 10Gbps, 10 x 10 Gbps, 4 x 25Gbps)
Cost is still very high (esp. for 100Gbps)

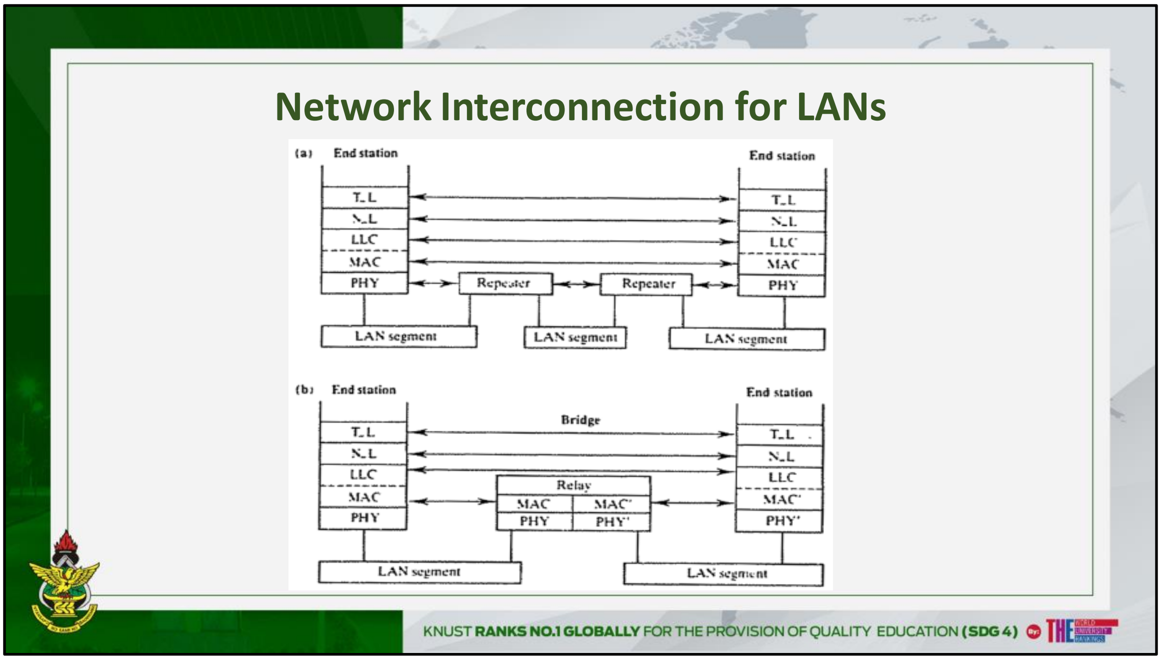
10 Gbps Ethernet products are now around. Initially 10 Gbps Ethernet has been used to provide
high-speed backbone interconnection between LAN segments. It can be expected to migrate
nearer to end stations in the future, much as Gigabit Ethernet is doing.
Gigabit Ethernet and 10Gbps Ethernet technology is also being looked at by network service
providers to create high-speed links in their access and metropolitan area networks.
The fact that the networks (frames) are Ethernet, end-to-end, offers considerable advantages over
networks using other technologies (such as ATM, and even SDH/SONET).

TCP/IP (which is hugely compatible with Ethernet) must look after the Quality of Service issues
that an ATM network would deal with.
Since late 2010, 40 and 100 Gbps products have started to appear. They will be used in hightraffic
network core applications. The transmission links consist of a number of parallel channels

(using WDM or separate fibres).



Break

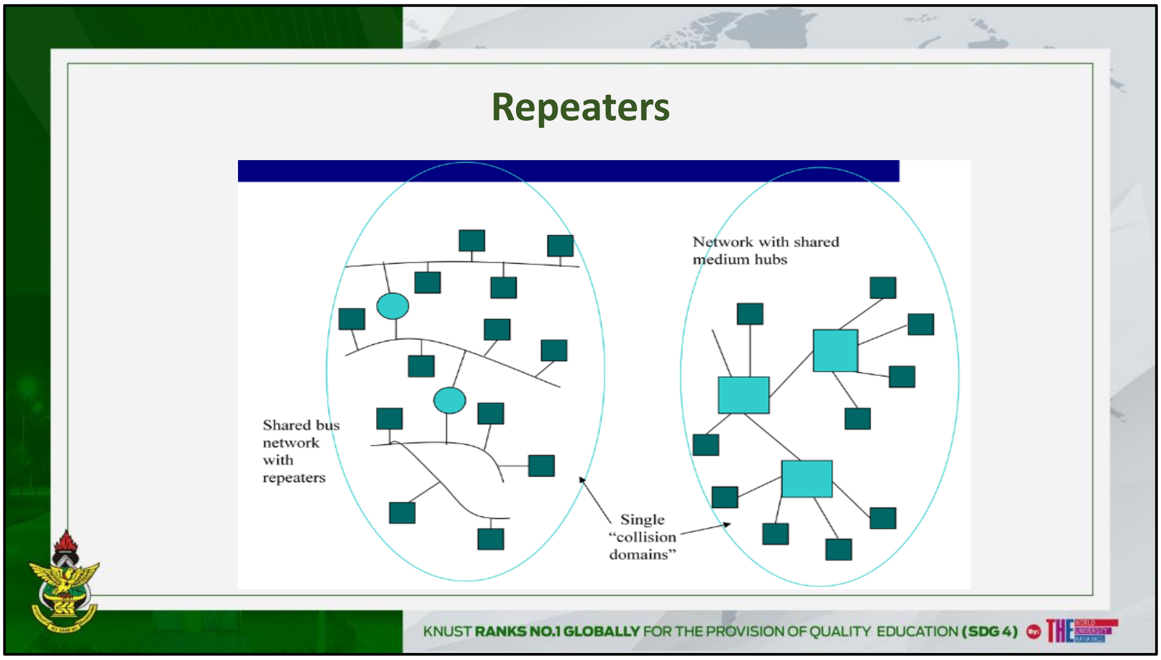


Network Interconnection for LANs

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)**

In general, a real LAN will consist of a number of interconnected segments, sub-networks or networks. The segments may use different bit-rates, protocols and topologies; this means that different levels of interconnection must be considered.

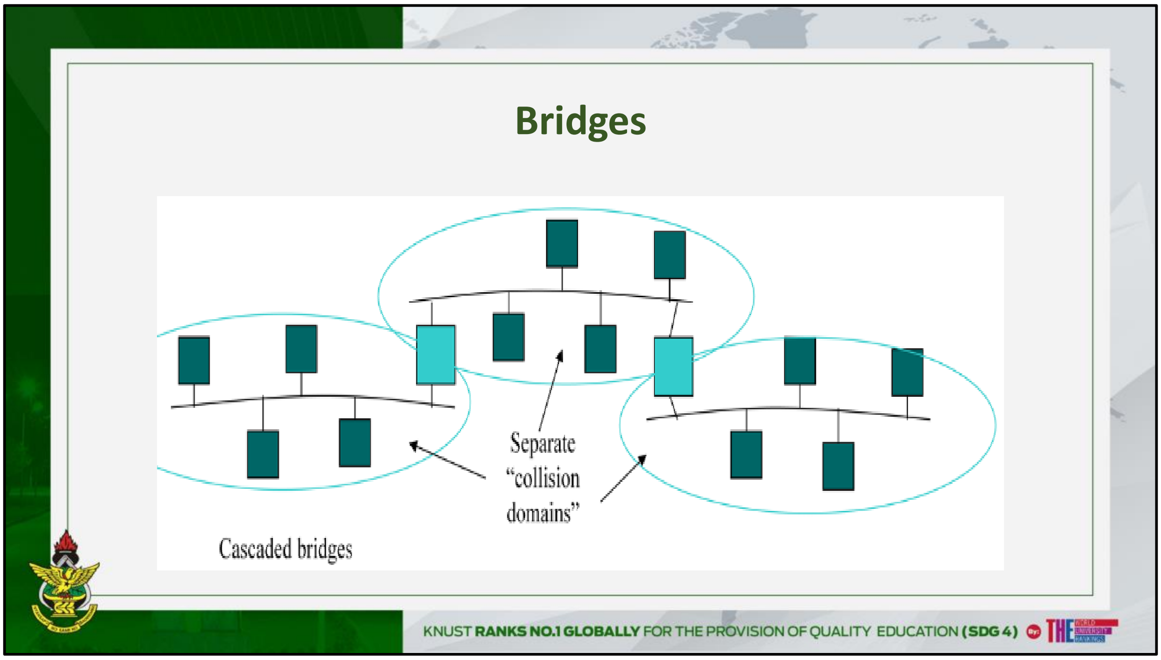
As only the lower 2 layers of the OSI model are specifically involved in LAN operation, we will
confine ourselves to interconnection involving only these layers.
Two possibilities exist, as shown above:
(a) using *repeaters which operate at the physical layer*
(b) using *bridges which operate at layer 2.*



Repeaters

Network with shared medium hubs
Shared bus network with repeaters
Single "collision domains"

A repeater regenerates the signals received on one port and transmits the regenerated signals on
the other port - all transmissions are relayed. This means that transmissions are always
transmitted on all segments (and hence load all segments).
As far as access is concerned, there is no significant difference to a single segment network.
The repeater allows longer transmission distances (cable length) than may otherwise have been
possible by negating the effects of signal attenuation. However, there may be other constraints on
the cable length, for example the propagation delay ("*a" parameter), which must take into account*
the whole network.



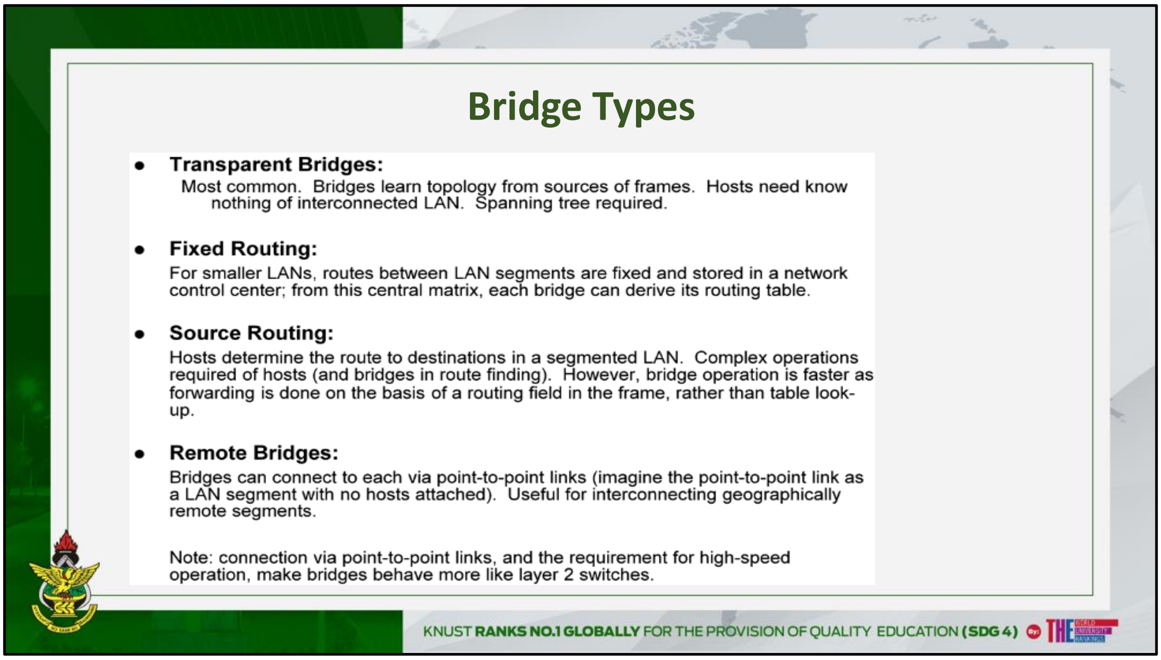
Bridges

Bridges operate at layer 2 - the MAC sublayer in IEEE LANs. MAC addresses are used to decide whether to forward packets on to other segments; a packet may only be forwarded if it is received error-free and is addressed to another segment. If the MAC address is the address of a station connected to the local segment, the packet may not be forwarded and so does not load the rest of the network. This is useful if the local traffic is much greater than the remote traffic.

The MAC protocol is for access to that segment only and so does not limit the total network size.

The bridge port is seen as another station for that segment.

Some segments may function only or mainly to interconnect other segments; these are known as *backbones.*



Bridge Types

- **Transparent Bridges:**

  Most common. Bridges learn topology from sources of frames. Hosts need know nothing of interconnected LAN. Spanning tree required.

- **Fixed Routing:**

  For smaller LANs, routes between LAN segments are fixed and stored in a network control center; from this central matrix, each bridge can derive its routing table.

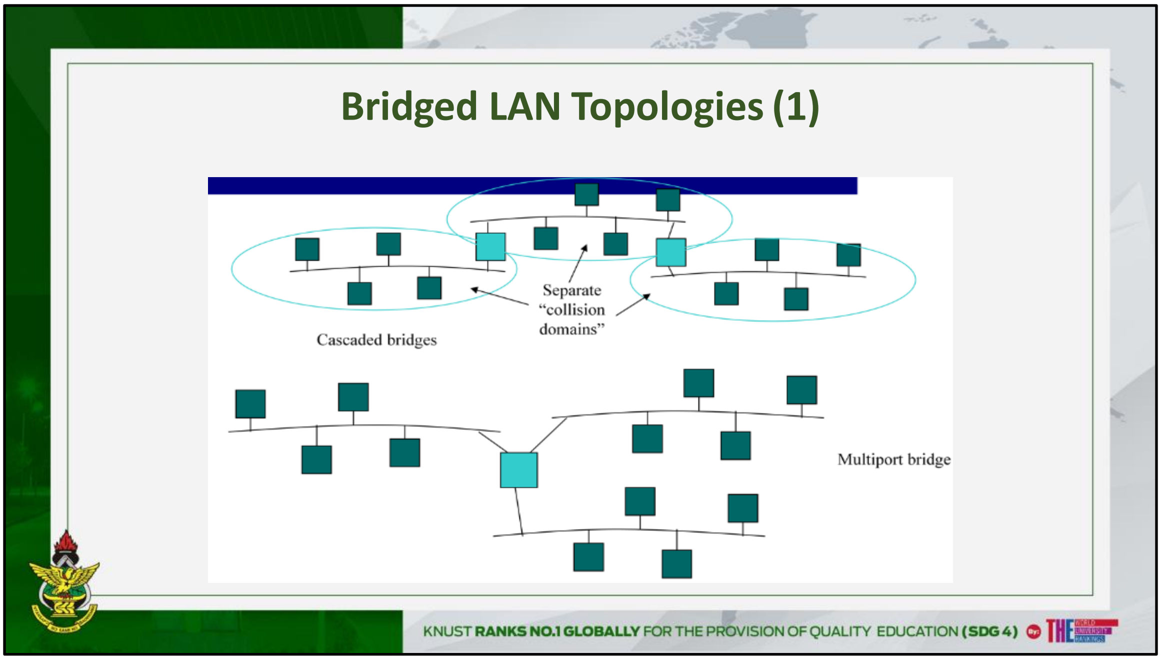
- **Source Routing:**

  Hosts determine the route to destinations in a segmented LAN. Complex operations required of hosts (and bridges in route finding). However, bridge operation is faster as forwarding is done on the basis of a routing field in the frame, rather than table look-up.

- **Remote Bridges:**

  Bridges can connect to each via point-to-point links (imagine the point-to-point link as a LAN segment with no hosts attached). Useful for interconnecting geographically remote segments.

  Note: connection via point-to-point links, and the requirement for high-speed operation, make bridges behave more like layer 2 switches.



Bridged LAN Topologies (1)

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

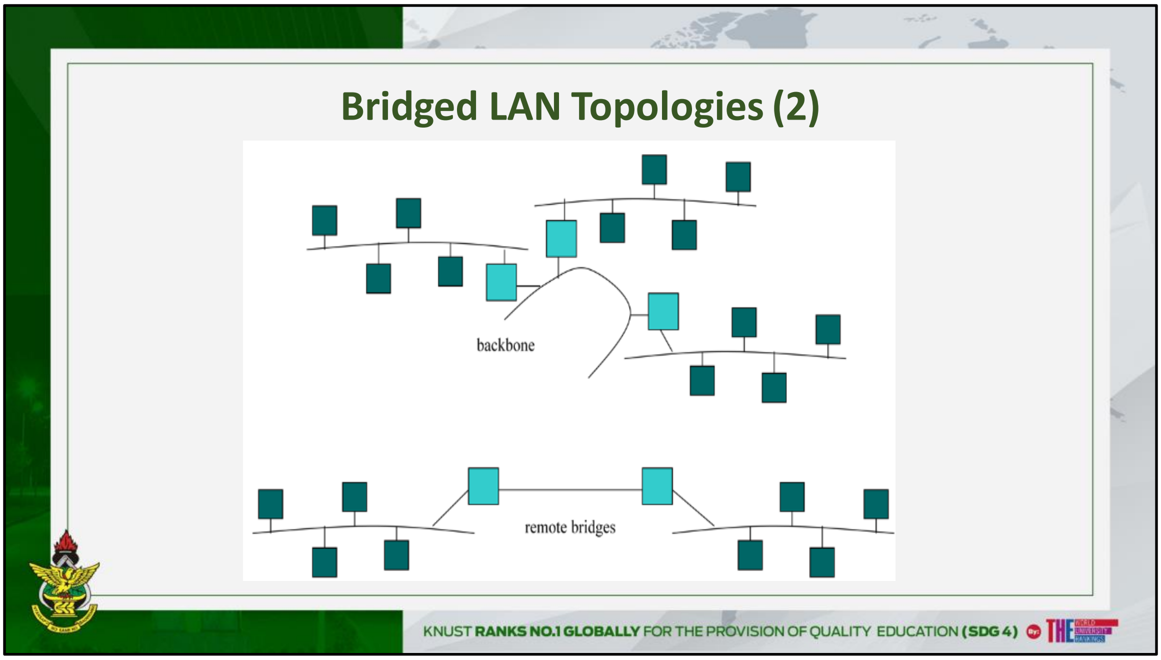
Cascaded bridges

This is the simplest method of extending LANs. The improvement in performance will decrease as the number of segments increases, especially with higher levels of remote traffic. The method is usually limited to 2 or 3 cascaded segments.

Multiport bridge

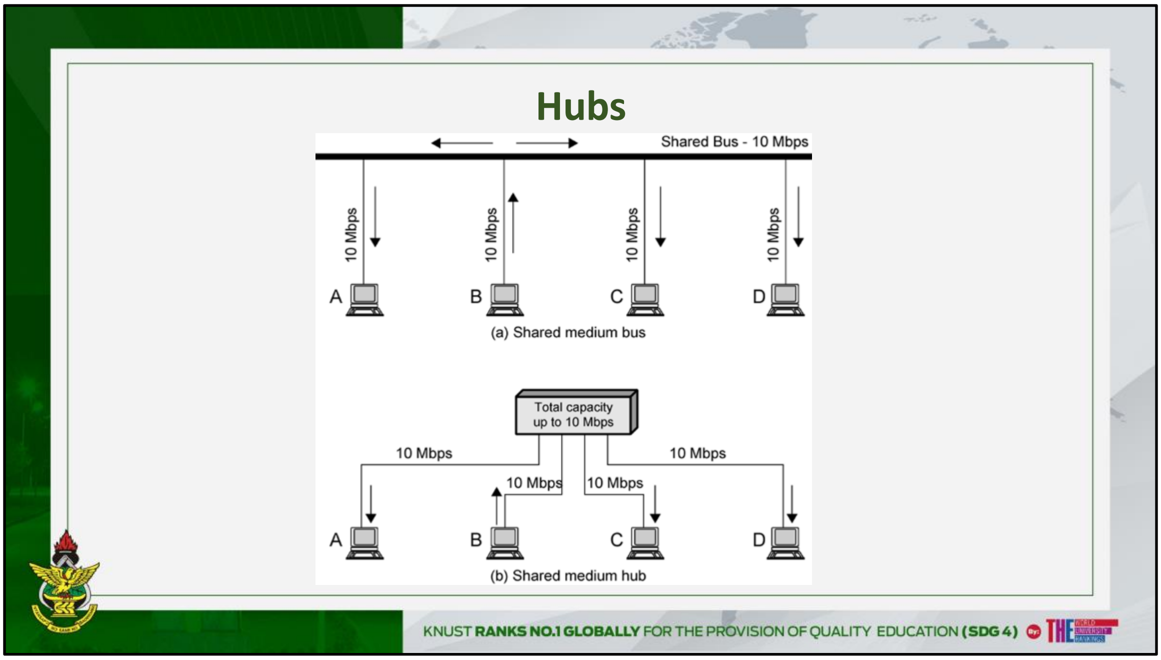
Only the segments to which the end stations are attached are loaded by remote traffic. The problem with multiport bridges is that implementation is technically demanding; the bridge must forward frames rapidly onto multiple segments, while allowing access to memory for other received transmissions. The forwarding rate needs to be high if the bridge is not to restrict flow.

Multiport bridges are typically limited to a maximum of 5 to 10 ports; they are also expensive.



Bridged LAN Topologies (2)

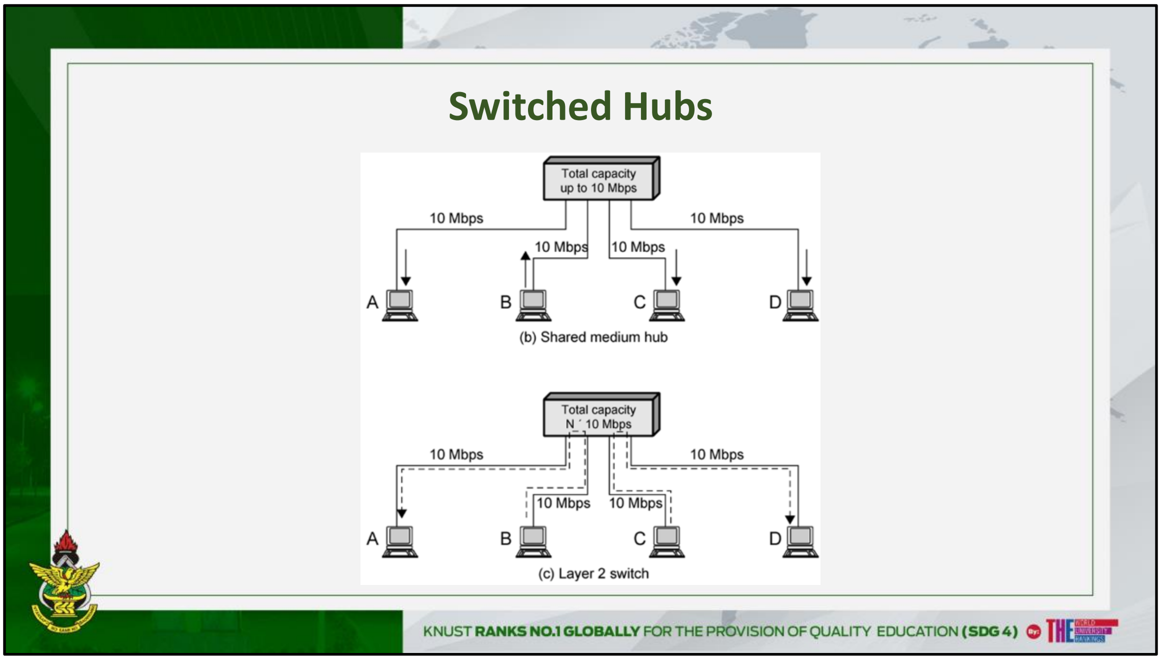
Backbone
The use of a backbone bridged LAN will give a similar performance improvement as the multiport
bridge if the transmission rate is the same. The backbone is useful in connecting geographically
dispersed segments. The backbone will saturate if the number of connected segments is high
and/or the remote traffic is high. In this case, the solution is to use a high-bandwidth backbone.



Hubs

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

Up to now, we have seen hubs as layer 1 centralised repeaters. Bus type networks can be
configured geographically in star wiring configurations, but the access protocol covers the
“hubbed” LAN, still operating as if it were a shared-medium bus.



Switched Hubs

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)**

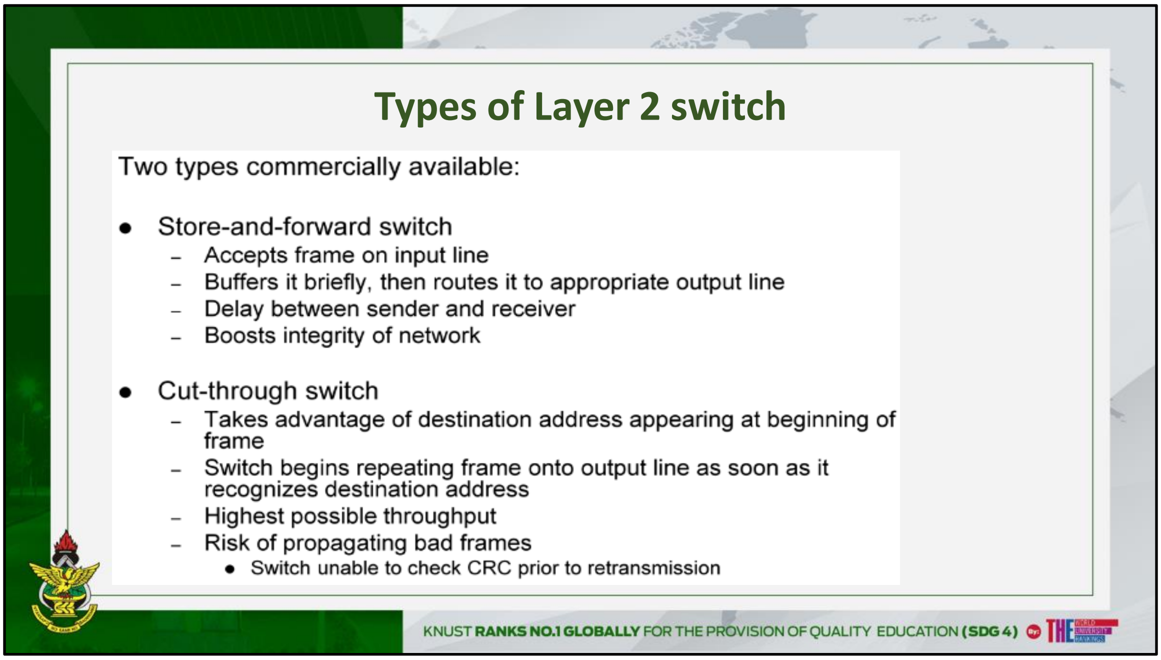
New LAN implementations make use of switching hubs, operating at layer 2. Greater performance can be achieved as frames are only sent to their destinations and simultaneous frame switching can be carried out. For example, the hub above may switch a frame from station A to station D at the same time as switching a frame from C to B. Current throughput is then 20 Mbps rather than 10 Mbps.

Layer 2 switches have become attractive as:

No changes to the attached devices are required to convert shared medium (bus/hub) networks to switched hub networks.

Each attached device now sees a dedicated capacity equal to the capacity of the entire original LAN.

The switched hubs scale easily.

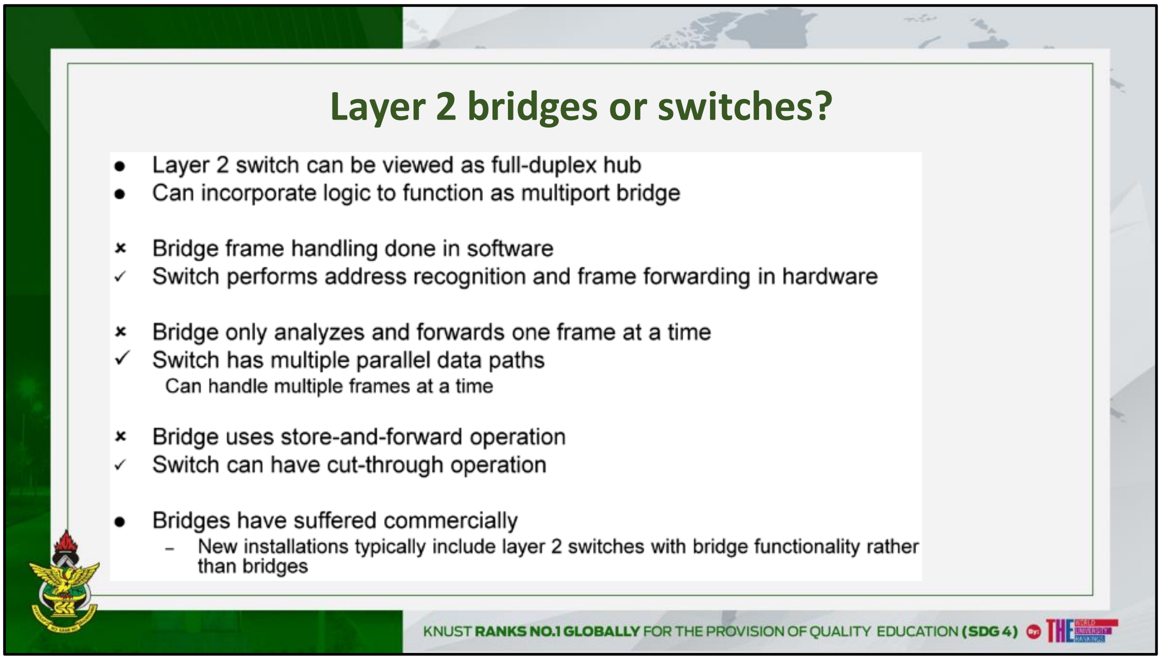


Types of Layer 2 switch

Two types commercially available:

- Store-and-forward switch
  - Accepts frame on input line
  - Buffers it briefly, then routes it to appropriate output line
  - Delay between sender and receiver
  - Boosts integrity of network
- Cut-through switch
  - Takes advantage of destination address appearing at beginning of frame
  - Switch begins repeating frame onto output line as soon as it recognizes destination address
  - Highest possible throughput
  - Risk of propagating bad frames
    - Switch unable to check CRC prior to retransmission

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS



Layer 2 bridges or switches?

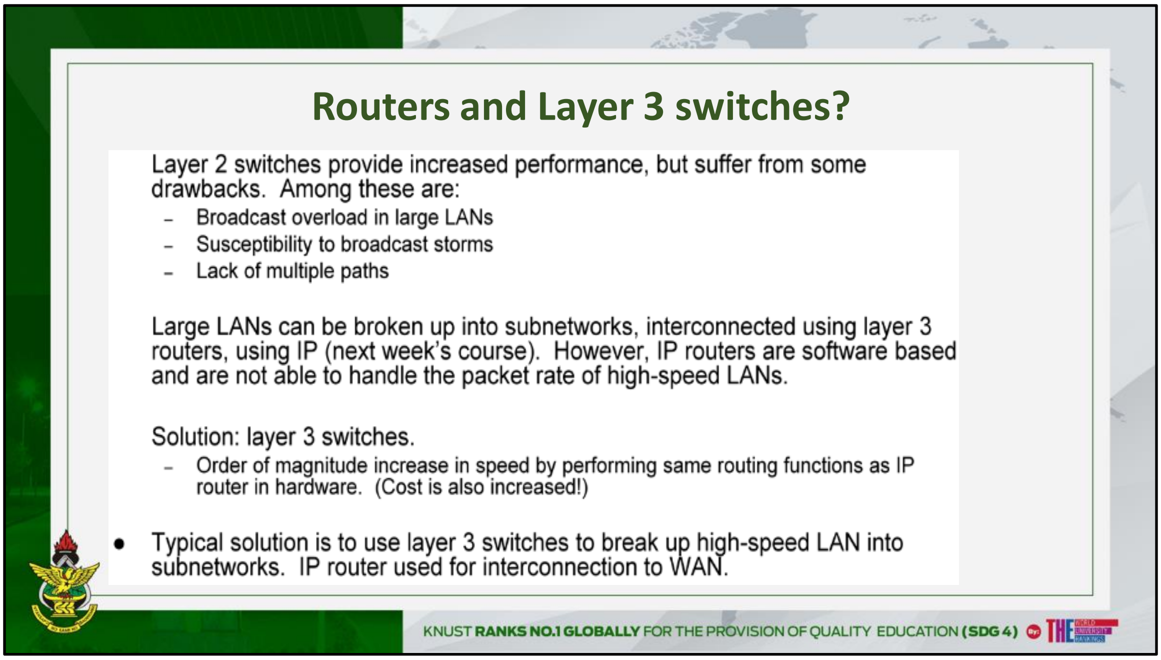
- ● Layer 2 switch can be viewed as full-duplex hub
- ● Can incorporate logic to function as multiport bridge

- × Bridge frame handling done in software
- ✓ Switch performs address recognition and frame forwarding in hardware

- × Bridge only analyzes and forwards one frame at a time
- ✓ Switch has multiple parallel data paths
  - Can handle multiple frames at a time

- × Bridge uses store-and-forward operation
- ✓ Switch can have cut-through operation

- ● Bridges have suffered commercially
  - – New installations typically include layer 2 switches with bridge functionality rather than bridges



Routers and Layer 3 switches?

Layer 2 switches provide increased performance, but suffer from some drawbacks. Among these are:

- Broadcast overload in large LANs
- Susceptibility to broadcast storms
- Lack of multiple paths

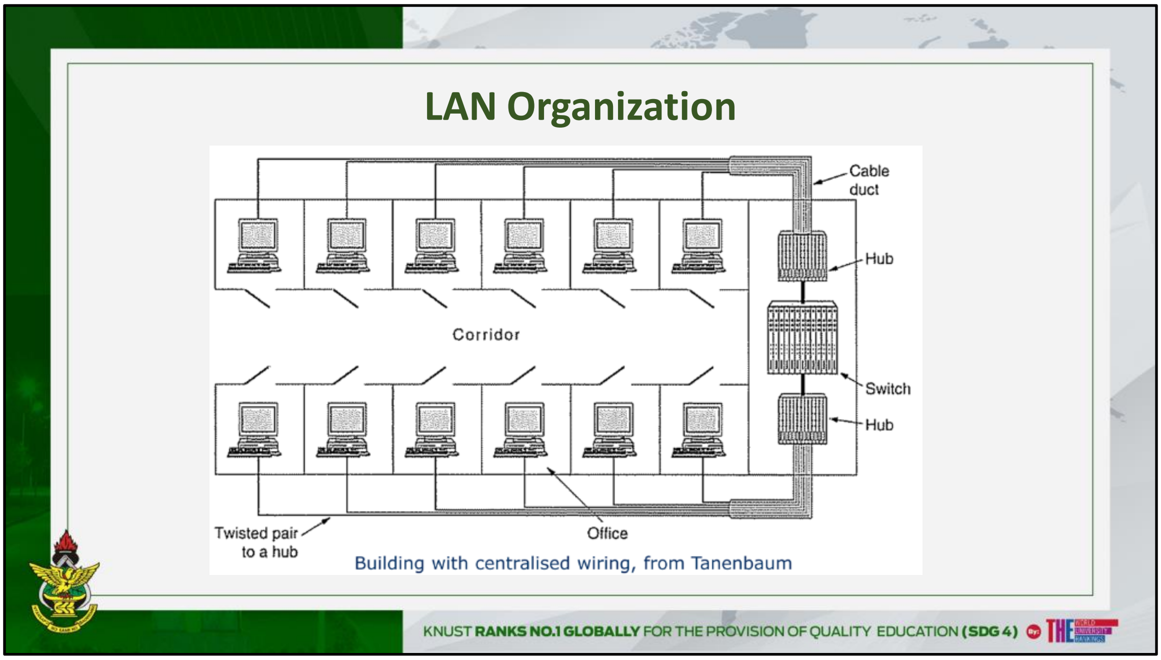
Large LANs can be broken up into subnetworks, interconnected using layer 3 routers, using IP (next week's course). However, IP routers are software based and are not able to handle the packet rate of high-speed LANs.

Solution: layer 3 switches.

- Order of magnitude increase in speed by performing same routing functions as IP router in hardware. (Cost is also increased!)

- Typical solution is to use layer 3 switches to break up high-speed LAN into subnetworks. IP router used for interconnection to WAN.

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS



LAN Organization

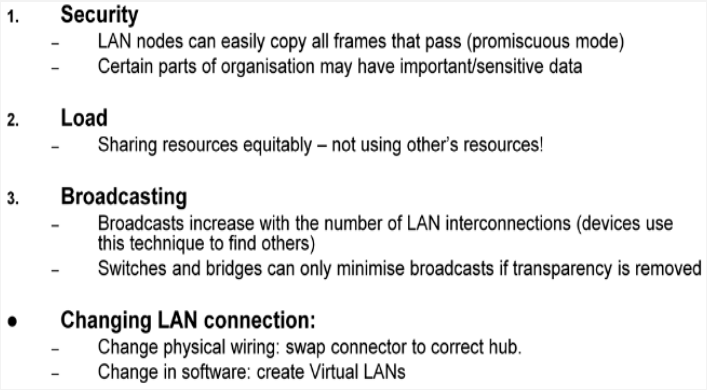
Building with centralised wiring, from Tanenbaum

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

Today’s LANs will usually be connected using a centralised wiring scheme with hubs and switches as shown above. Patching cables to hubs and switches affords flexibility to network managers, and segments networks in manageable portions.

Connection to a particular LAN will normally be done on geographical considerations, both because offices close to each other typically have those with related roles and responsibilities working in them, and also for the operation of LAN protocols (e.g. the “*a”-parameter restriction will* limit the distance to a hub).

Organisational / logical considerations for LAN topologies

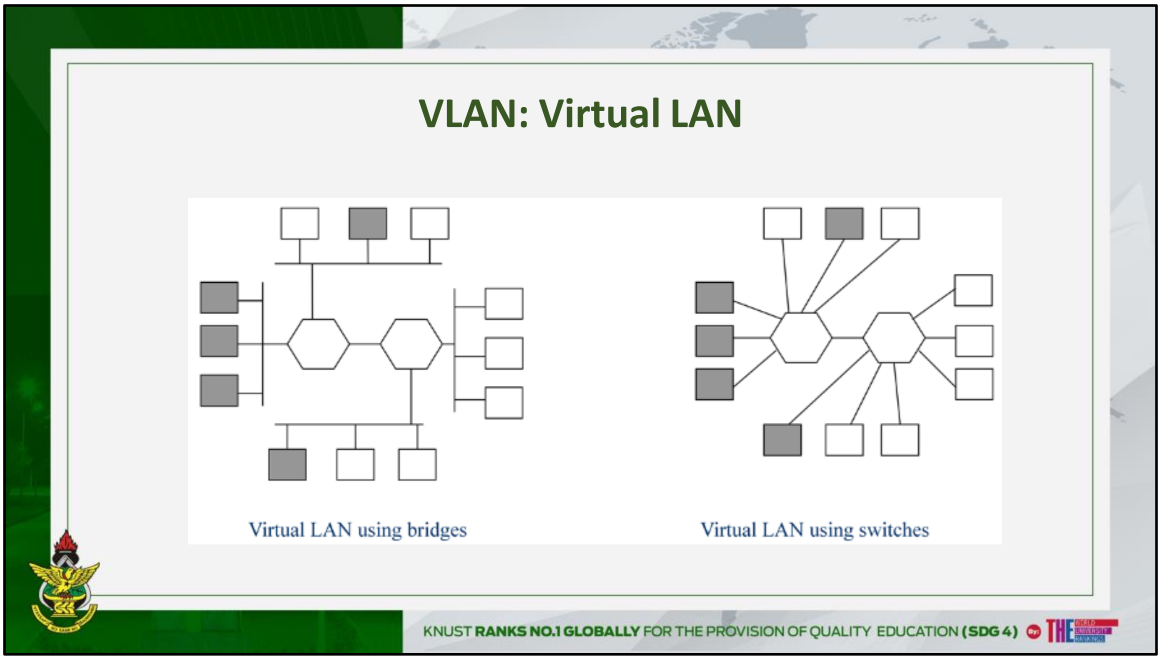


1. **Security**
   - LAN nodes can easily copy all frames that pass (promiscuous mode)
   - Certain parts of organisation may have important/sensitive data

2. **Load**
   - Sharing resources equitably – not using other's resources!

3. **Broadcasting**
   - Broadcasts increase with the number of LAN interconnections (devices use this technique to find others)
   - Switches and bridges can only minimise broadcasts if transparency is removed

- **Changing LAN connection:**
  - Change physical wiring: swap connector to correct hub.
  - Change in software: create Virtual LANs



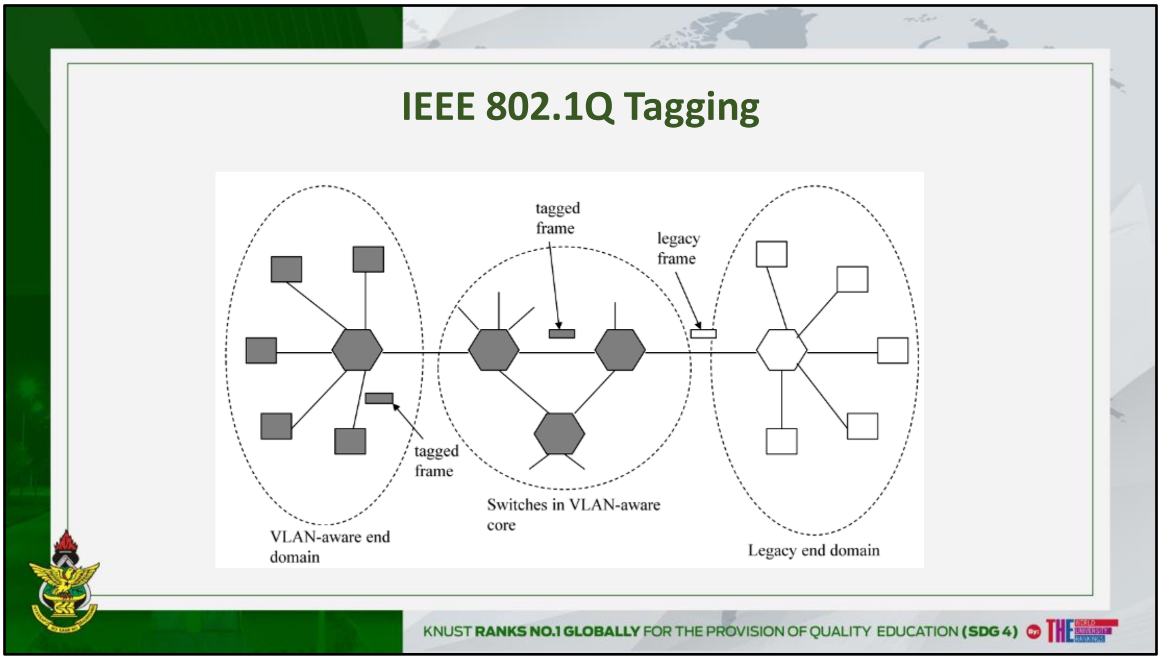
VLAN: Virtual LAN

Virtual LAN using bridges

Virtual LAN using switches

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE

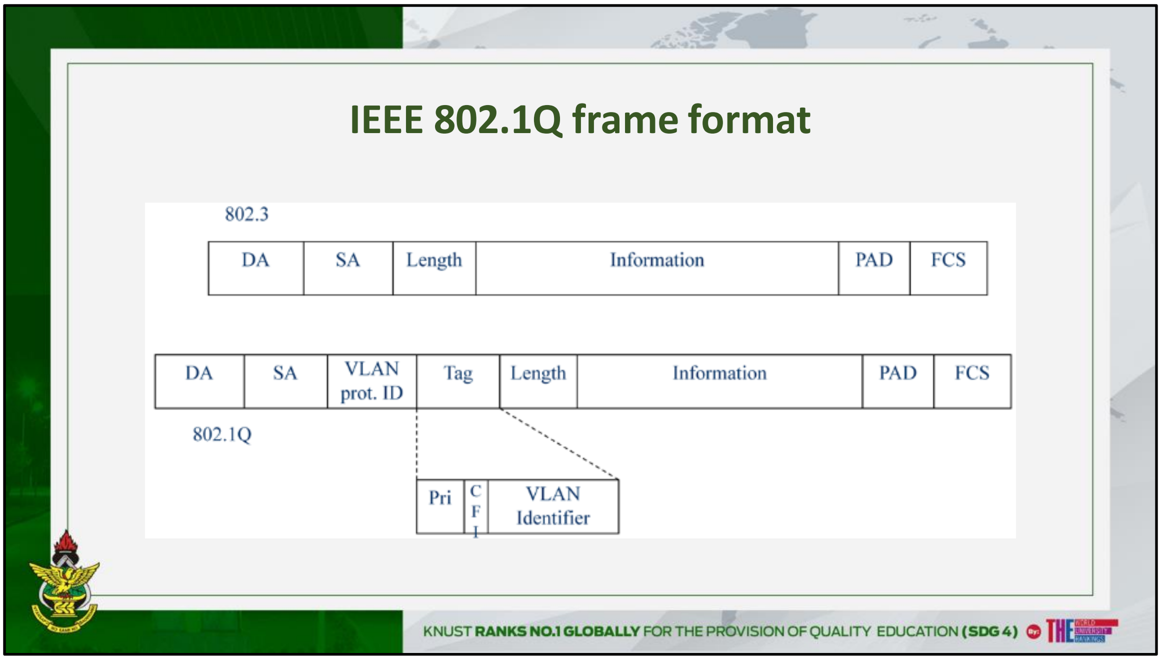
VLANs depend on specially-designed VLAN-aware switches, bridges and/or routers.
Configuration tables must be set up.
For switches, generally each port of the switch can be assigned its VLAN (colour), as it corresponds to an end device. But, this depends on hierarchy.
For bridges, ports may have multiple colours, as attached devices may belong to different VLANs.
Frames are forwarded according to VLAN colour. This can be through one of the following
methods:
Ports can be given a colour. (Problem with bridges, or higher level switches)
MAC address can be assigned colours. (MAC address may correspond to docking station, not
machine. Note: even with machine, anyone logging in automatically becomes part of that VLAN)
IP address can be assigned a colour. (Requires looking into higher layer protocol information)



IEEE 802.1Q Tagging

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

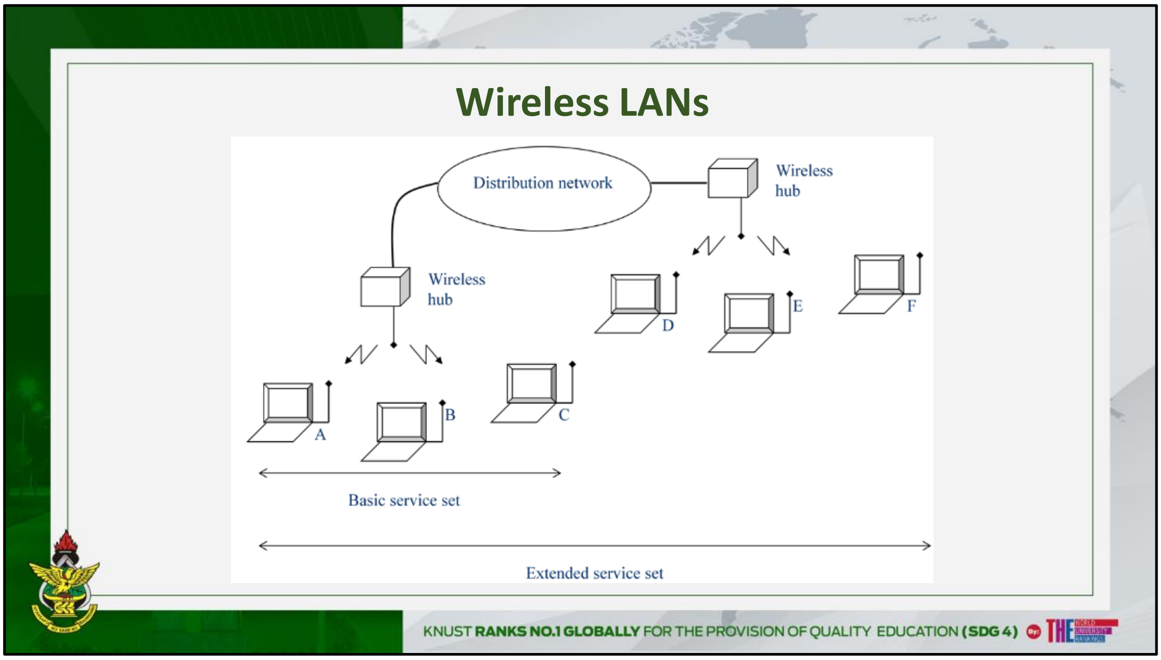
Frames are tagged by IEEE 802.1Q VLAN aware switches (or bridges). These will generally be
newer devices. Hosts need not be VLAN aware. Legacy machines (including switches/bridges)
need not be VLAN aware, as the first VLAN aware machine on the path takes responsibility for
tagging the frame.
Further switching is then based on the tags, and the last VLAN aware machine on the path
removes the tags.
The association of tags to addresses and ports can be manually configured, but devices can also
auto-configure themselves using a learning algorithm. This requires the use of a spanning tree
and an algorithm based on the bridge learning (802.1D).



IEEE 802.1Q frame format

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

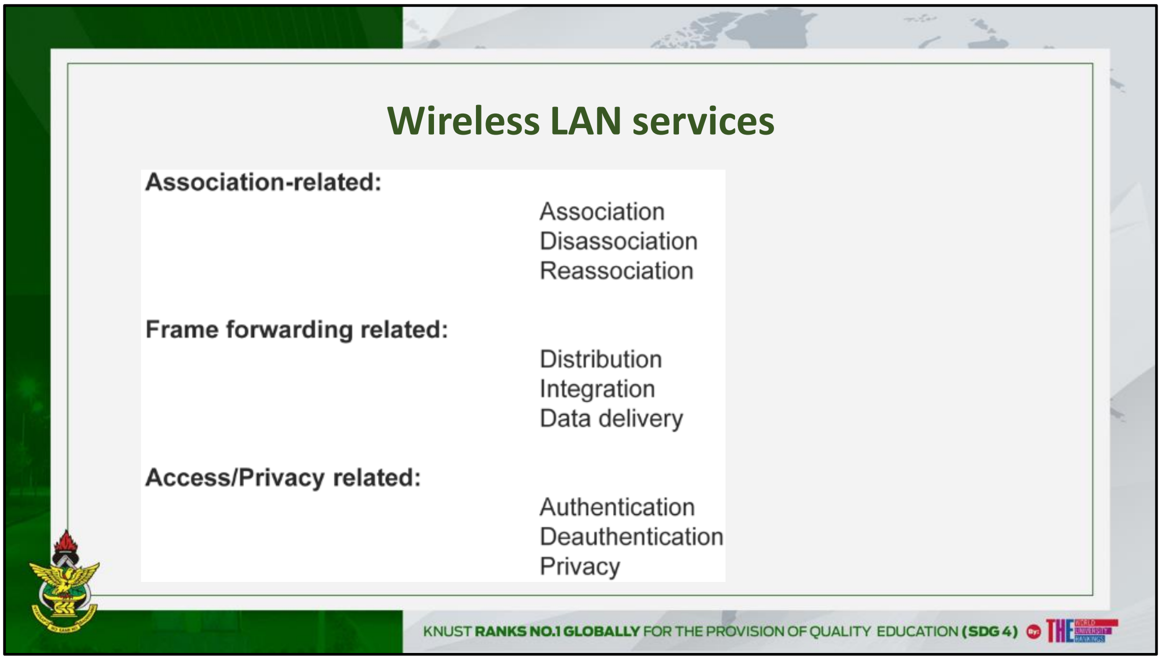
Additional fields are added to the standard Ethernet frame.
This is possible because the maximum length that can be specified in an Ethernet frame is 1500;
a value greater than this can be interpreted differently. The VLAN protocol ID is given the value
0x8100.
The first 4 bits of the following 2-byte field (the Priority and CFI subfields) have nothing to do with
VLAN operation. The lower-order 12 bits make up the VLAN identifier, and allow up to 4,094
VLANs to be identified.
It is worth considering that the VLAN identifier is something akin to a connection identifier –
something generally disliked by Ethernet and IP enthusiasts!



Wireless LANs

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

The IEEE wireless LAN working group have developed standards (and are continuing to do so) for
cell-based wireless networks. Within each cell an access point provides a bridge function to a
distribution system which is typically a wired (backbone) LAN.
The access point (hub in the above) provides wireless mobility for the stations in its cell. This is
the smallest building block for the wireless LAN and is called a basic service set.
The whole wireless LAN may consist of a number of BSSs interconnected by a distribution system
(such as a wired LAN). This LAN, which appears to the LLC layer as a single logical LAN, is
called an extended service set (ESS).



Wireless LAN services

Association-related:

Association
Disassociation
Reassociation

Frame forwarding related:

Distribution
Integration
Data delivery

Access/Privacy related:

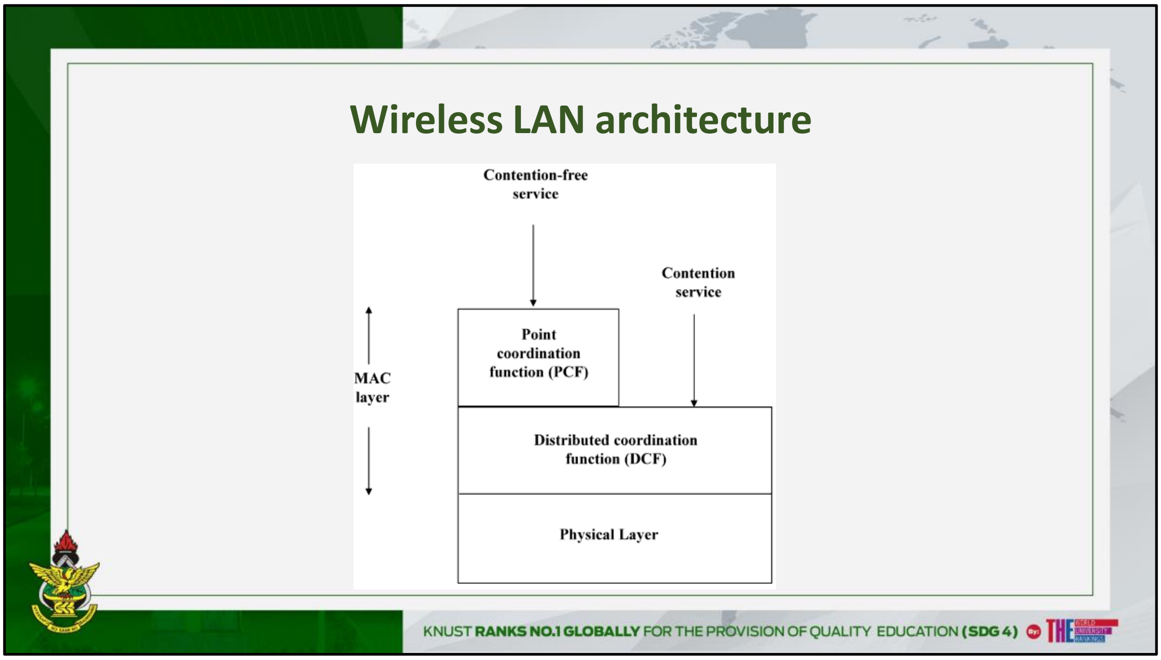
Authentication
Deauthentication
Privacy

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The services provided by a Wireless LAN provide a level of functionality at least equivalent to that
provided in wired LANs.
The association service is required when stations move into the range of an AP and request use
of it; the station will announce its identity, capabilities and requirements (e.g. data rates supported,
use of polling service). The AP may accept or reject the mobile station. Disassociation may be
used by either AP or mobile station to break the relationship. Reassociation is used when a
mobile station moves from one cell (BSS) to another.
The distribution service determines how an AP decides to route frames, including those to be sent
over a wired network distribution system. The integration service handles translation of frame
formats from 802.11 to a format required by the destination network. The data delivery service
refers to the main best-effort frame delivery that is the core function of the wireless

LAN.

When association has been accepted there must be an authentication process; several schemes
are supported, it is only important that the stations agree the scheme to be used. Authentication
is required as in wired LANs the physical wiring of a station to a LAN is seen as a guarantee of
authorisation to use the LAN – such an assumption cannot be used in a wireless LAN.
Deauthentication is invoked to terminate a previously authenticated association. Privacy is
provided through the optional use of an encryption algorithm.



Wireless LAN architecture

Contention-free service

Contention service

MAC layer

Point coordination function (PCF)

Distributed coordination function (DCF)

Physical Layer

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

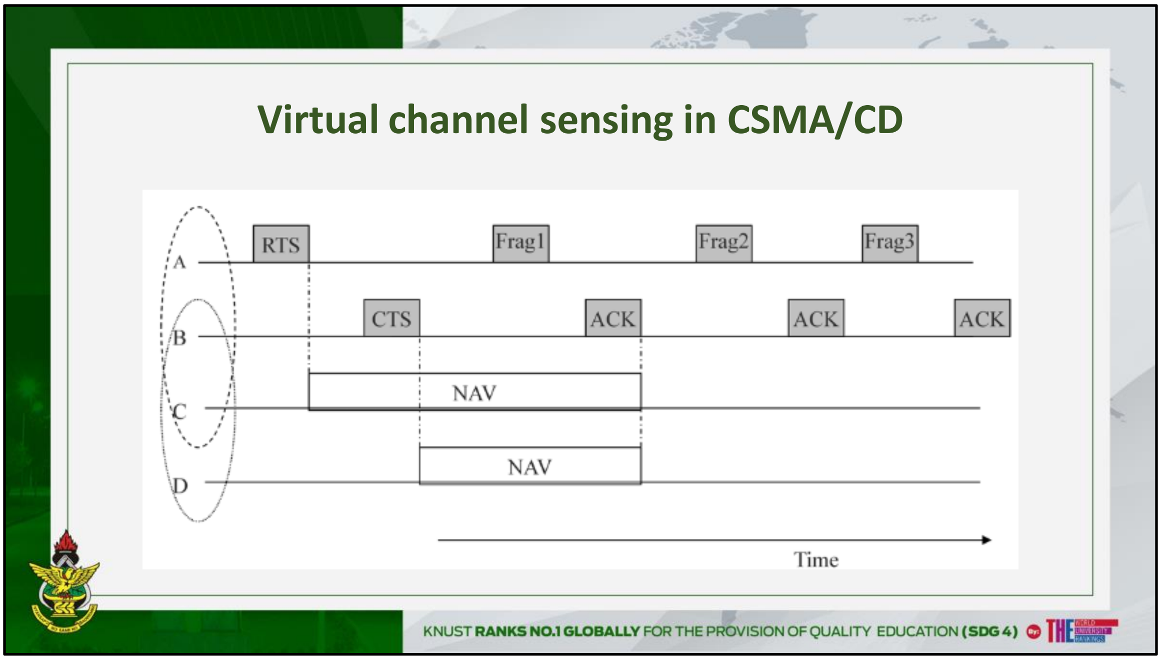
The above diagram shows the protocol layers defined for the IEEE WLAN standards.

The whole LAN system will use a common LLC. The MAC and Physical layers for each cell operate independently.

The MAC protocol is called Distributed Foundation Wireless MAC – DFWMAC. It consists of a distributed access scheme based on CSMA – the DCF above – and an optional higher sublayer – PCF above – which provides a contention-free service through a centralised (polling) algorithm.

The DCF sublayer makes use of a simple CSMA protocol, with a few refinements for interframe spaces but no collision detection (collision detection is too difficult to implement in a wireless environment).

In addition to a basic sensing function (Basic Access), the protocol can use a form of “virtual channel sensing” to improve performance – a Request to Send/Clear to Send function.



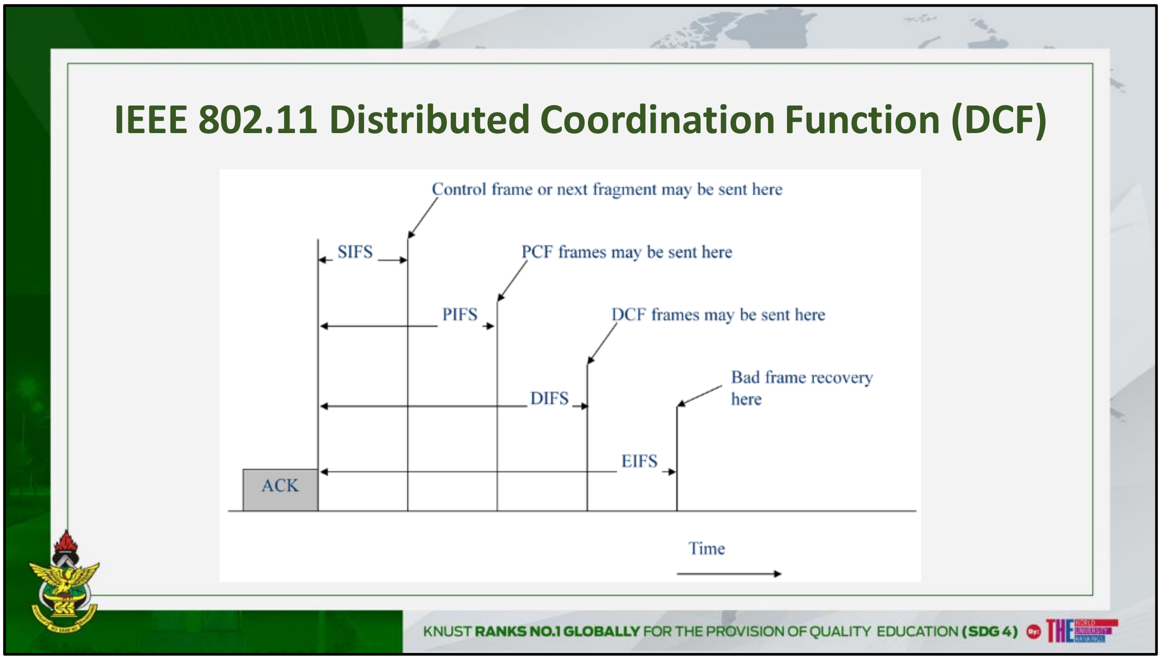
Virtual channel sensing in CSMA/CD

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

There is a hidden station problem in wireless networks. For example, station A might try transmitting to stations B or C without being aware that station D is transmitting (because it is out of radio range). There is also an exposed station problem: B might back-off from transmitting to A because it can hear D transmitting; but D is transmitting to another station which is out of radio range interference from A anyway. For these reasons CSMA/CD cannot be employed. Instead, a form of virtual channel sensing is used.

A wants to transmit to B and sends a request-to-send (RTS) frame. B responds with a clear-tosend (CTS) frame. When C hears the RTS it desists from transmission for a period during which it expects the data to be sent and acknowledged – what is termed a network allocation vector (NAV). D does not hear the RTS, but does hear the CTS and also backs off. The NAV is asserted until an acknowledgement can be expected to have been received. However, in wireless networks, frames are broken up into smaller fragments, each of which is acknowledged. Then only a corrupted fragment needs to retransmitted.

However, we wouldn’t want only parts of the frame to be received before moving to another frame transmission, so fragments are granted easier access to the medium through the use of different interframe spaces.



IEEE 802.11 Distributed Coordination Function (DCF)

Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
PIFS
DCF frames may be sent here
DIFS
Bad frame recovery here
EIFS
ACK
Time

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

Instead of transmitting immediately – either on sensing the medium idle or on waiting for a current transmission to cease – a station waits for a period called the interframe space (IFS). If the medium had been busy, the station also waits for an additional period defined by a binary exponential backoff scheme.

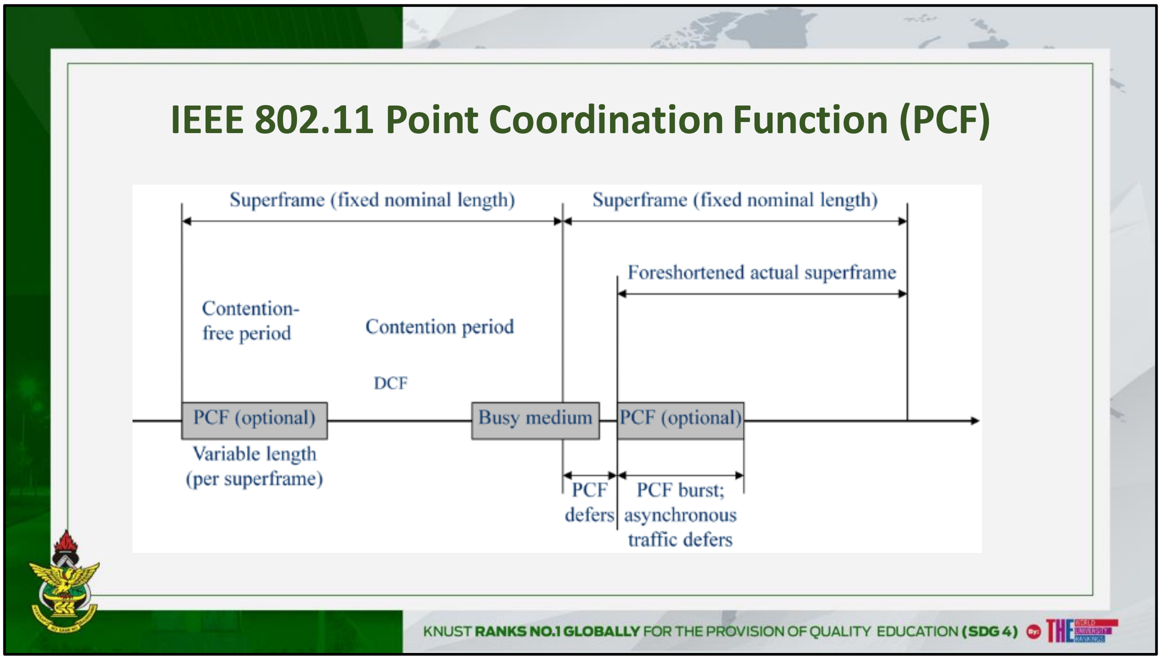
Priority is provided within this algorithm by specifying different types of IFS.

Short IFS (SIFS) are used by immediate response actions such as sending CTS frames, next fragments, acknowledgements and responses to polls (see later).

Point coordination function IFS (PIFS) are used by the centralised controller (access point) when issuing polls or broadcasting its periodic beacon frames (typically 10 to 100 per second).

Distributed coordination function IFS (DIFS) are used for normal contention frames.

The Extended IFS (EIFS) is used by stations waiting to report a bad or unknown frame.



IEEE 802.11 Point Coordination Function (PCF)

Superframe (fixed nominal length)

Superframe (fixed nominal length)

Foreshortened actual superframe

Contention-free period

Contention period

DCF

PCF (optional)

Busy medium

PCF (optional)

Variable length (per superframe)

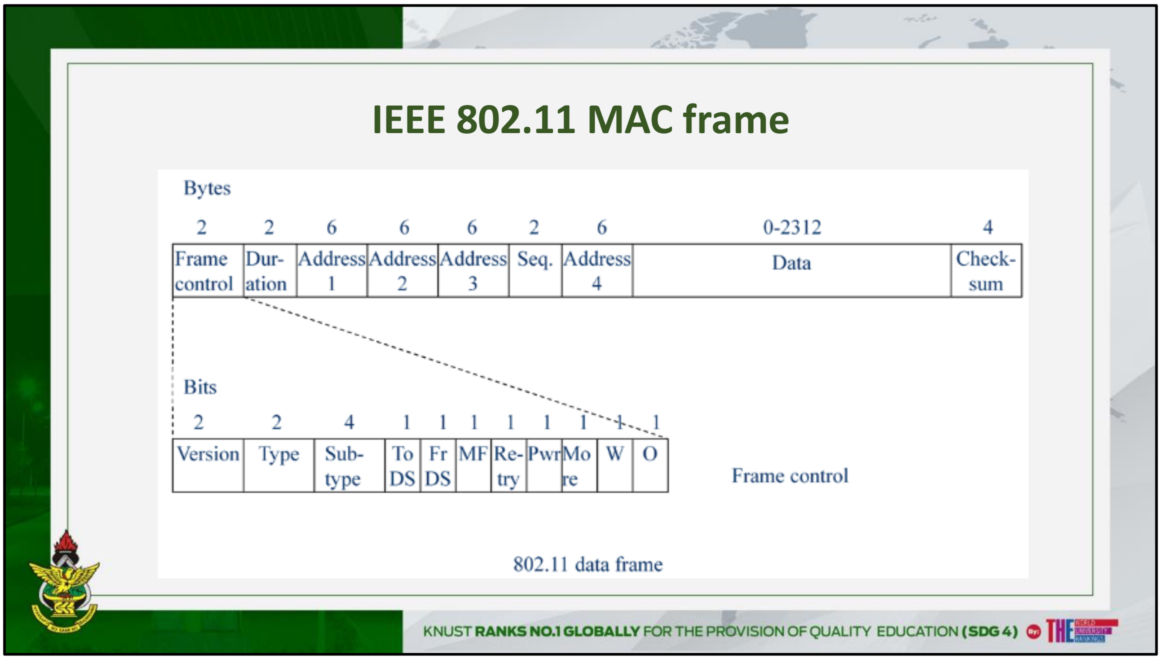
PCF defers

PCF burst; asynchronous traffic defers

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE

PCF is implemented on top of DCF to provide for services with time-critical requirements.
A polling master (point coordinator) – really this will be in the access point (AP) - makes use of the
PIFS in issuing polls to individual stations. These can respond making use of SIFS.
If PCF were simply implemented as described so far, it would be possible for the PCF to lock out
all of the contention traffic. To prevent this, an interval known as the superframe is defined. The
point coordination function (when used) operates only for the first part of the superframe, allowing
a contention period in the later part of the frame.

Actual superframe lengths may vary slightly as the coordinator has to seize control of the medium
at the end of the previous superframe and has to contend to do so. Also, the time allocated to
PCF operation may vary, according to the number of stations with contention-free traffic.



IEEE 802.11 MAC frame

Bytes

2	2	6	6	6	2	6	0-2312	4
Frame control	Duration	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Checksum

Bits

2	2	4	1	1	1	1	1	1	1	1
Version	Type	Sub-type	To DS	Fr DS	MF	Retry	Pwr	More	W	O

Frame control

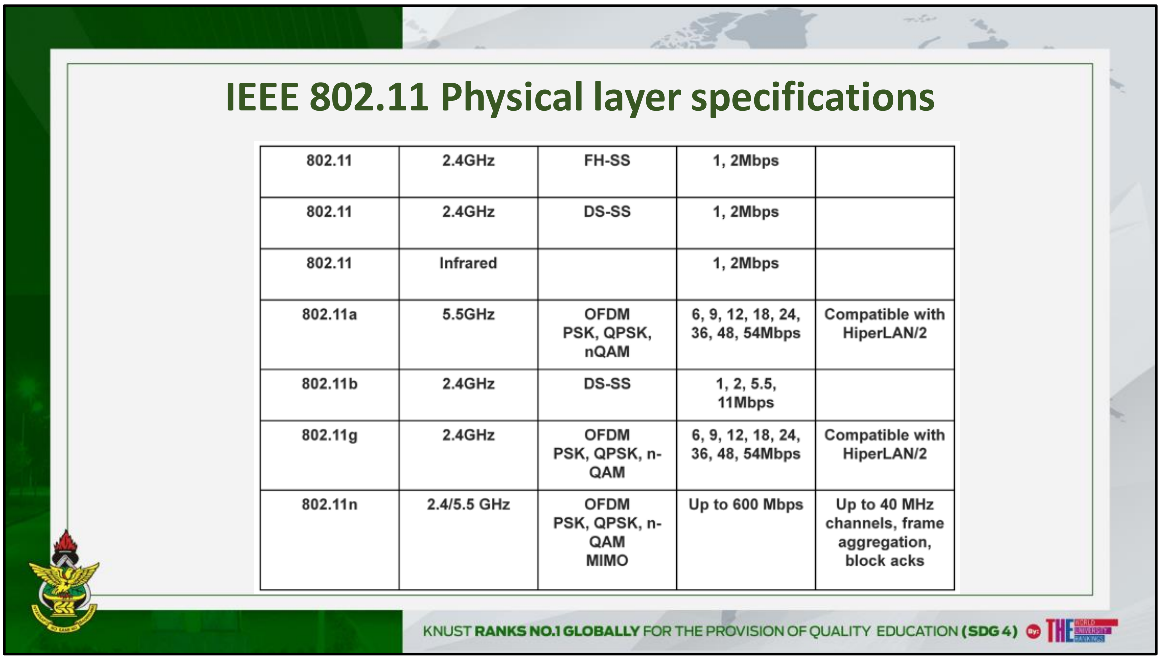
802.11 data frame

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The *Frame Control field has 11 subfields:*
Version – allows two versions of the protocol to operate simultaneously in the same cell.
Type – defines data, management or control frames; Sub-type, may define, e.g., RTS or CTS
To/From DS – indicate that the frame is going to/from a distribution system (e.g. Ethernet).
MF – indicates more fragments follow. Retry – indicates a retransmission.
Pwr – is the power management bit (used by APs to put receivers into sleep state or take them
out).
More – indicates the sender has more frames for the receiver.
W – indicates the use of the WEP (Wired Equivalent Privacy) encryption algorithm.
O – indicates that a receiver must process frames in strict sequence.
The *Duration field of the frame informs how long the frame and any acknowledgement will occupy*
the channel and is used by other stations in the NAV mechanism.
Four address fields are present in data frames to allow for the addresses of APs in intercell traffic.

Management and control frames are only used within a cell and do not require more than 2 address fields.

The *Sequence field is used to identify the frame (12 bits) and allows for the numbering of* fragments (4 bits). The *Data field contains the payload of up to 2,312 bytes. Control frames* contain no Sequence or Data fields.



IEEE 802.11 Physical layer specifications

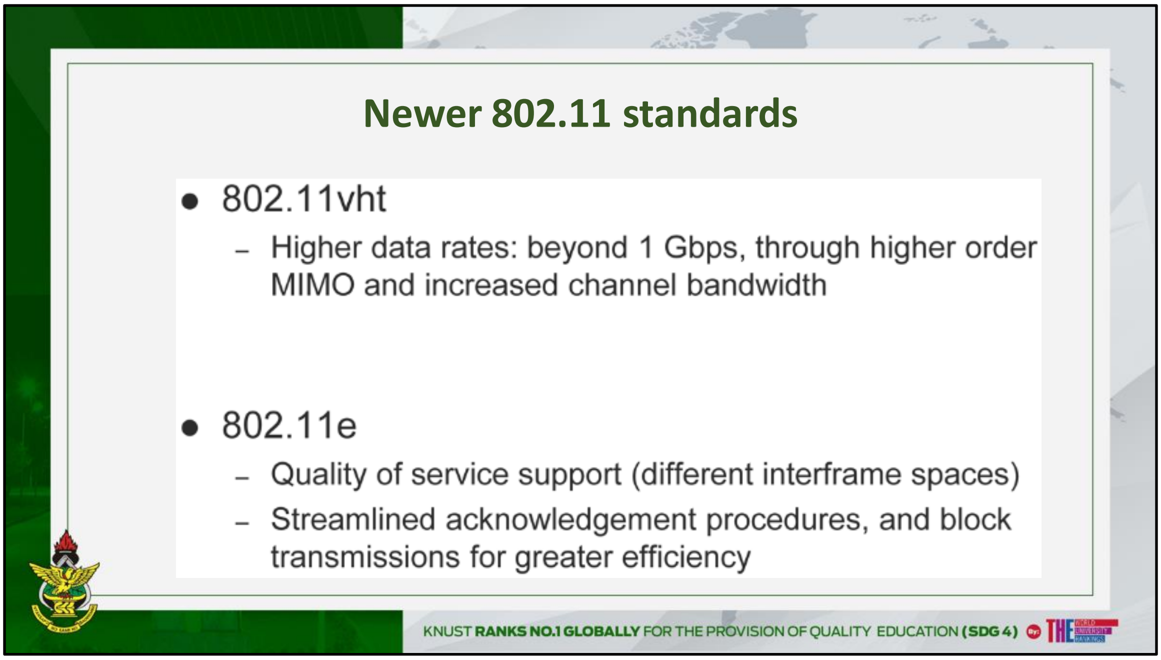
802.11	2.4GHz	FH-SS	1, 2Mbps	
802.11	2.4GHz	DS-SS	1, 2Mbps	
802.11	Infrared		1, 2Mbps	
802.11a	5.5GHz	OFDM PSK, QPSK, nQAM	6, 9, 12, 18, 24, 36, 48, 54Mbps	Compatible with HiperLAN/2
802.11b	2.4GHz	DS-SS	1, 2, 5.5, 11Mbps	
802.11g	2.4GHz	OFDM PSK, QPSK, n-QAM	6, 9, 12, 18, 24, 36, 48, 54Mbps	Compatible with HiperLAN/2
802.11n	2.4/5.5 GHz	OFDM PSK, QPSK, n-QAM MIMO	Up to 600 Mbps	Up to 40 MHz channels, frame aggregation, block acks

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The original 802.11 Physical layer standards were limited to data rates of 1 or 2 Mbps.
Infrared
transmission uses diffused transmission (not line-of-sight) at 850 or 950 nm. There
are
advantages in that infrared signals do not penetrate walls, for example, so different
rooms are well
isolated; but noise, from sunlight etc., causes problems and the bandwidth must
therefore be low.
The FHSS system provided good resilience to multipath effects, interference and
eavesdropping
but also had limited bandwidth.
The first higher speed standard to be defined was 802.11b, a DSSS system which uses
11 million
chips/second. The data rate can be dynamically adjusted during operation to cater for
different
load and noise conditions. The 802.11a standard uses OFDM technology with 52
carriers being
used to deliver up to 54 Mbps in the 5.5 GHz ISM band. The range is, however, less
than that for

802.11b. The 802.11g standard was then approved and uses the OFDM modulation of 802.11a but in the narrower, but more popular, 2.4GHz band – it can also provide up to 54 Mbps. Because the RF front-end can be similar, most devices are b/g compatible, so that they can revert to the b system when signal strengths are low.

In 2009, the 802.11n standard was ratified (pre-standard products were already appearing). The highest data rate of 600 Mbps is only achievable with changes to the MAC as well as PHY layer. PHY layer changes include the use of 40 MHz, rather than 20 MHz, channels and the possibility to use two spatially separate streams. There is also a possibility to reduce the guard interval. MAC changes involve the use of frame aggregation and block acknowledgments.



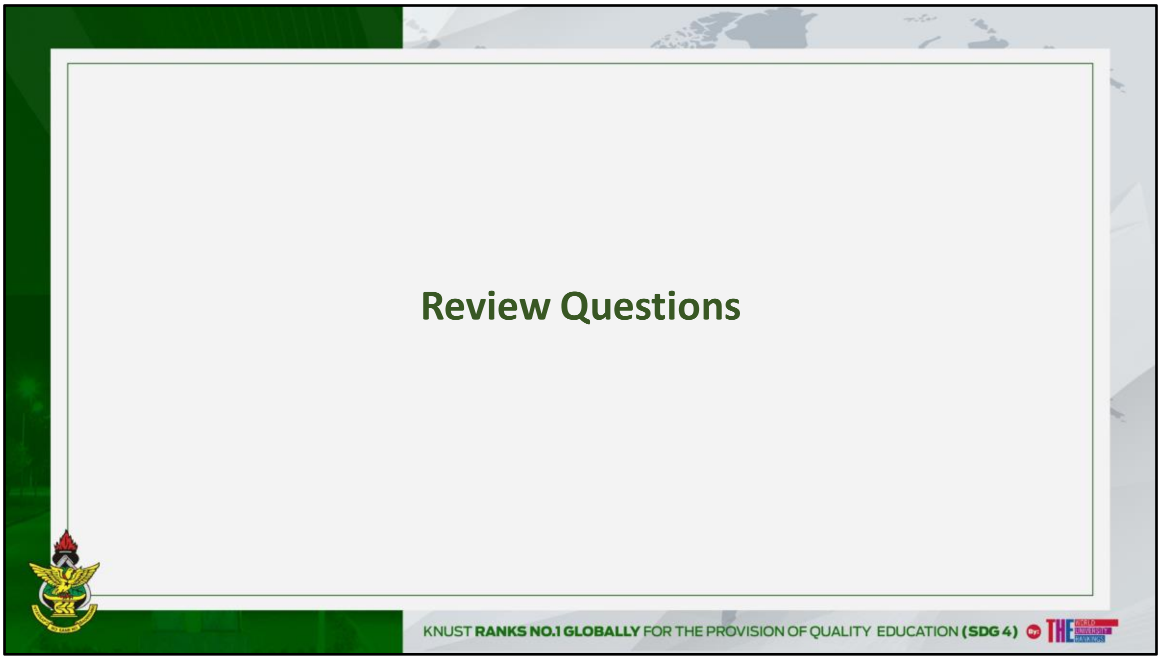
Newer 802.11 standards

- 802.11vht
  - Higher data rates: beyond 1 Gbps, through higher order MIMO and increased channel bandwidth
- 802.11e
  - Quality of service support (different interframe spaces)
  - Streamlined acknowledgement procedures, and block transmissions for greater efficiency

KNUST RANKS NO.1 GLOBALLY FOR THE PROVISION OF QUALITY EDUCATION (SDG 4) By: THE WORLD UNIVERSITY RANKINGS

The 802.11 standards are continually being updated.
802.11vht (very high throughput): both below 6 GHz and 60 GHz systems have been studied in this working group. The idea is to provide more than 1 Gbps throughput (not just data rate), which will require increases in available bandwidth even at below 6 GHz. Several different standards were agreed in 2011, e.g. 802.11ac (operating in the 5.5/5.8 GHz region and using 80MHz bandwidth channels) and 802.11ad (operating in the 60 GHz region with around 7 GHz of available bandwidth).

802.11e: will provide for quality of service differentiation by defining different interframe spaces. It also permits burst transmission, and different acknowledgement policies, including block acknowledgement and no acknowledgement which can help improve efficiency. Products implementing some of these features have already appeared. (Note 802.11e does not specify its own PHY – it will operate with 802.11a/b/g/n). 802.11n incorporates some of the features proposed.



Review Questions

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE WORLD UNIVERSITY RANKINGS

KNUST
Kwame Nkrumah University of Science and Technology, Kumasi | Leaders In Change
Visit us at www.knust.edu.gh
uro@knust.edu.gh
Follow KNUST on:

End of Lecture 2