Chapter 3: Datalink layer

- Functionalities:
  - Encapsulation, addressing
  - Error detection and correction
  - Flow control
  - Media access control

ONE LOVE. ONE FUTURE.

1

1

Overview of Data link layer

ONE LOVE. ONE FUTURE.

2

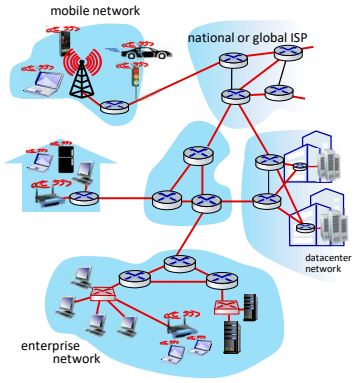
2

Link layer: introduction

terminology:

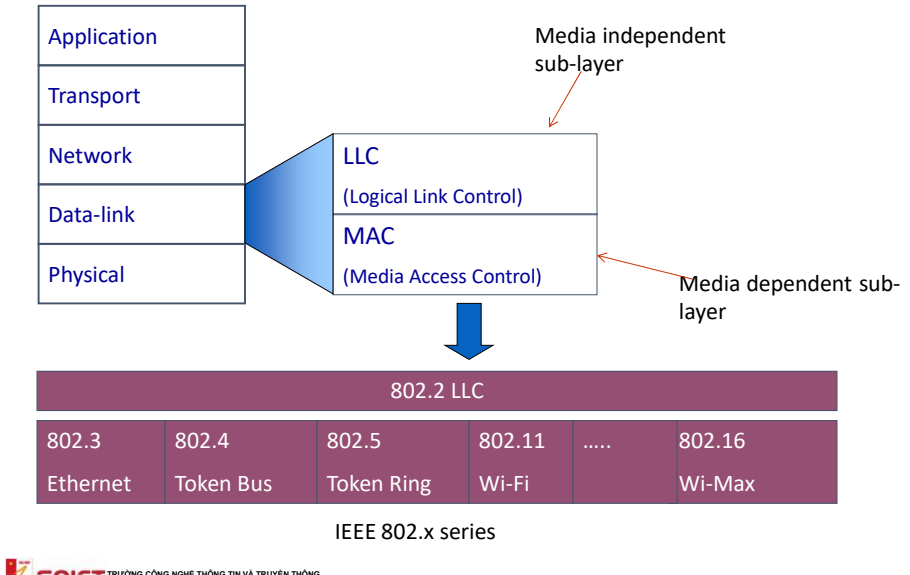
- hosts and routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired
  - wireless
  - LANs
- layer-2 packet: *frame*, encapsulates datagram

link layer has responsibility of transferring datagram from one node to physically adjacent node over a link



3

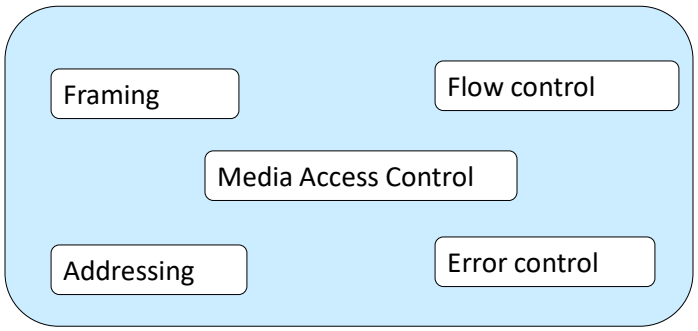
Datalink layer in Layer architecture



IEEE 802.x series

5

Functionalities



Datalink layer

6

Link layer: context

- datagram transferred by different link protocols over different links:
  - e.g., WiFi on first link, Ethernet on next link
- each link protocol provides different services
  - e.g., may or may not provide reliable data transfer over link

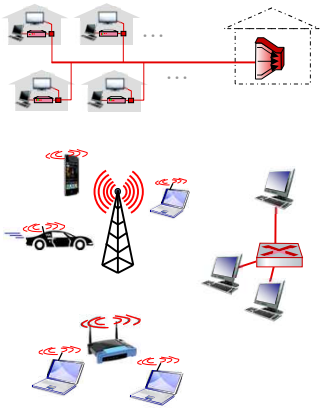
transportation analogy:

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link-layer protocol
- travel agent = routing algorithm

7

Link layer: services

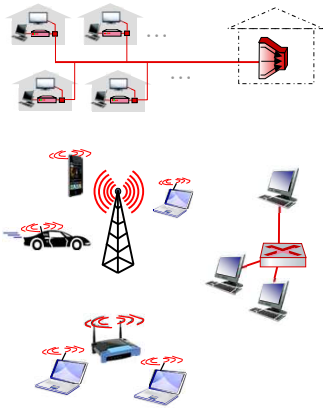
- framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - "MAC" addresses in frame headers identify source, destination (different from IP address!)
- Media access control:
  - If the nodes in the network share common media, a Media access control protocol is required



8

Link layer: services (more)

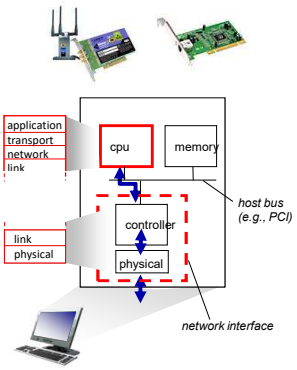
- flow control:
  - pacing between adjacent sending and receiving nodes
- error detection:
  - errors caused by signal attenuation, noise.
  - receiver detects errors, signals retransmission, or drops frame
- error correction:
  - receiver identifies *and corrects* bit error(s) without retransmission
- half-duplex and full-duplex:
  - with half duplex, nodes at both ends of link can transmit, but not at same time



9

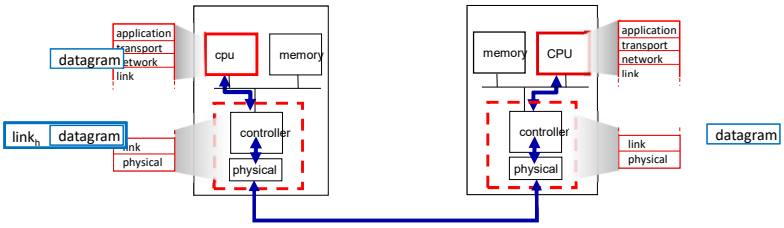
Where is the link layer implemented?

- in each-and-every host
- link layer implemented in *network interface card* (NIC) or on a chip
  - Ethernet, WiFi card or chip
  - implements link, physical layer
- attaches into host's system buses
- combination of hardware, software, firmware



10

Interfaces communicating



sending side:
- encapsulates datagram in frame
- adds error checking bits, reliable data transfer, flow control, etc.

receiving side:
- looks for errors, reliable data transfer, flow control, etc.
- extracts datagram, passes to upper layer at receiving side

11

Identifier: MAC address

- MAC address: 48 bit, organized by IEEE
- Each port is assigned one MAC
  - Cannot be changed
  - Physical address
- No hierarchical system, flexible
  - MAC Address is unchanged when changing networks
- Broadcast address in LAN:

  FF-FF-FF-FF-FF-FF

12

Error control

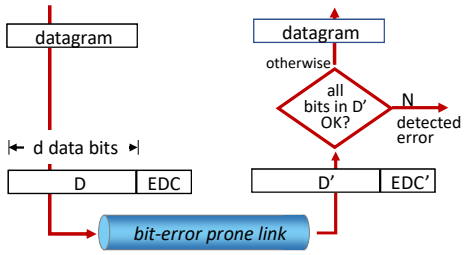
- Error detection
- Error correction

ONE LOVE. ONE FUTURE.

16

Principle of error detection

EDC: error detection and correction bits (e.g., redundancy)
D: data protected by error checking, may include header fields



Error detection not 100% reliable!

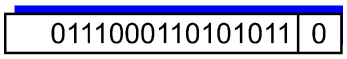
- protocol may miss some errors, but rarely
- larger EDC field yields better detection and correction

17

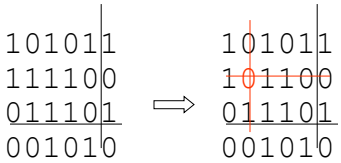
Parity code

A check bit is added to the original data to ensure that the total number of bit 1 is even (even parity code) or odd (odd parity code)

- Single code
  - Able to detect single bit error



- Two-dimension code
  - Detect and correct single bit error



- Application: mainly on hardware, ex: while sending data on PCI and SCSI bus

20

Parity code

- Sent data with Odd code:
  - 01010101 →Code: 1
- Case 1: Received data 01110101 Received code: 1
  - → Total number of 1 : 6→ even number→ Code does not match with data
  - → Error
- Case 2: Received data 011101000 Received code: 1
  - Total number of bit 1 → 5→ code matches with data
  - → No error
- Data of m bit long→ space of data is 2^m → expected to have different code for different data → codes must be >=m bit long.

21

Checksum

Goal: detect errors (*i.e.,* flipped bits) in transmitted segment

sender:

- Divide data to n-bit segments
- Calculate the sums of segments. If having overflow bits, add them to the results
- checksum: addition (one's complement sum) of segment content

receiver:

- Divide data to n-bit segments
- Calculate the sums of segments. If having overflow bits, add them to the results
- Add the received checksum with the results
- Check the final outcome
  - Contains 0 - error detected
  - Only 1 - no error detected. *But maybe errors nonetheless?*

22

Checksum: Example

Data: 0011 0110 1000

Calculate checksum 4 bit:

```
   0011
 + 0110
   1000
  10001
      1
   0010
```

Overflow bit

Alter bit -> checksum code: 1101

Bits to send: 0011 0110 1000 1101

Checksum: Processing on receiver

Bits received: 0011 0110 1000 1101

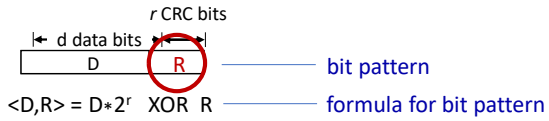
Verification:

```
   0011
   0110
 + 1000
   1101
  11110
      1
   1111 → no bit error
```

Overflow bit

Cyclic Redundancy Check (CRC)

- more powerful error-detection coding
- D: data bits (given, think of these as a binary number)
- G: bit pattern (generator), of *r+1* bits (given)



goal: choose *r* CRC bits, R, such that <D,R> exactly divisible by G (mod 2)

- receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
- can detect all burst errors less than r+1 bits
- widely used in practice (Ethernet, 802.11 WiFi)

27

CRC: How to find R

- <D, R> = D.2^r XOR R
- Since <D, R> divides G then
  - D.2^r XOR R = n.G
  - ➔ D.2^r = n.G XOR R (associativity)
- This means, R is the remainder of the division D.2^r by G (division modulo 2)

R= D.2^r mod G

R=110, the string to send is 10101001110

D R

- Ex: D= 10101001
- r= 3 bits
- G=1001

```
10101001000 | 1001
1001  D       1011110
  1110
  1001
   1110
   1001
    1111
    1001
     1100
     1001
      1010
      1001
       110
        R
```


28

CRC under polynomial form

- 1011 <-> $x^3 + x + 1$
- Example of some CRC generators using in the pratice:
  - CRC-8 = $x^8 + x^2 + x + 1$
  - CRC-12 = $x^{12}+x^{11}+x^3+x^2+x$
  - CRC-16-CCITT = $x^{16} + x^{12} + x^5 + 1$
  - CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$
- The longer G is, the more possible that CRC detects errors.
- CRC is widely used in the practice
  - Wi-fi, ATM, Ethernet…
  - Operation XOR is implemented in hardware
  - Capable to detect less than r+1 bits errors

29

CRC – Example

Frame : 1101011011

Generator : G(x) = $x^4 + x + 1$ → P = 10011

Dividend : Fk = 11010110110000

R = Fk mod P = 1110

Send : 11010110111110

30

CRC – Example

```
11010110110000 | 10011
10011
~~0~~10011
 10011
 ~~00000~~10110
      10011
      ~~00~~10100
        10011
        ~~00~~1110  → Remainder:CRC
```


31

CRC – Check 11010110111110

```
11010110111110 | 10011
10011
~~0~~10011
 10011
 ~~00000~~10111
      10011
      ~~00~~10011
        10011
        ~~000000~~  → No errors
```


32

CRC – Check 11010010111110

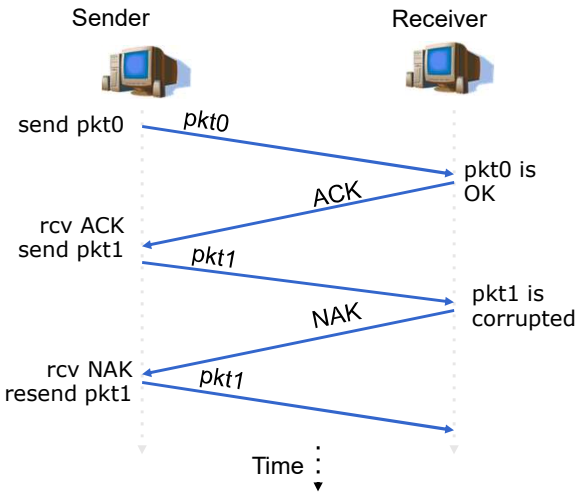
```
11010010111110 | 10011
10011
 ↓10010
  10011
  ↓0000011011
       10011
       ↓010001
        10011
        ↓000010110
           10011
           00101 → not 0 → errors
```


Reaction when errors detected

- Objective: to assure that data are received correctly even though the chanel is not realiable.
- Constraint
  - Data frame must be correctly received
  - Negligible transmission delay.
- Possible errors
  - Whole frame loss
  - Error frame
  - Loss of error warning message
- Popular techniques:
  - Error detection (as we seen)
  - Acknowledgement/confirmation
  - Retransmis after a clear confirmation that frame is not arrived
  - Retransmis after timeout
- ARQ technique: automatic repeat request). There are 3 versions:
  - Stop and Wait ARQ
  - Go Back N ARQ
  - Selective Reject ARQ
- Similar to techniques used in flow control.

Stop-and-wait ARQ

Normal case

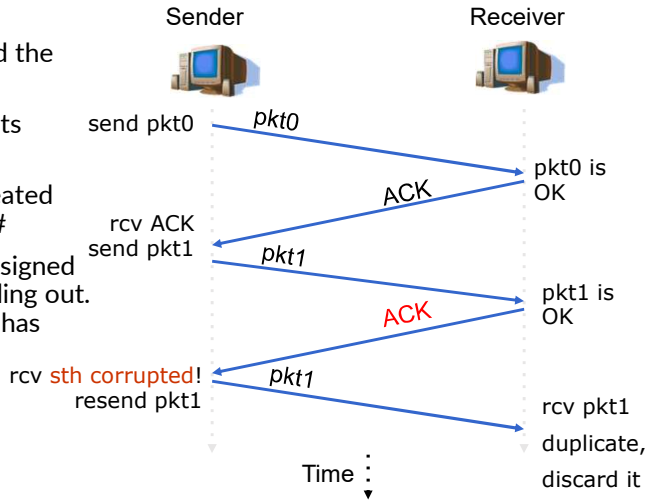


35

Stop-and-wait ARQ

Error ACK/NAK

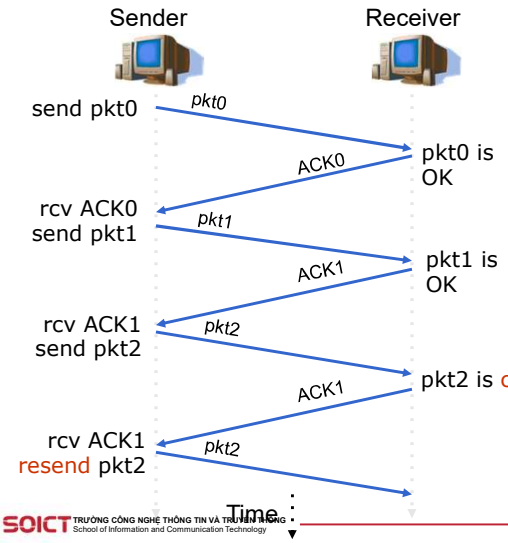
- ACK error, resend the previous packet
- Duplicated packets problem.
- To eliminate repeated packet: Use Seq.#
- All packets are assigned Seq# before sending out. Repeated packet has identical Seq#



36

Stop-and-wait ARQ

not using NAK



- ACK packet carries #Seq of the packet to be acknowledged. This number is called acknowledgment number
- An ACK with acknowledgment number n implicitly confirms that all packet with #seq number < =n have been well received

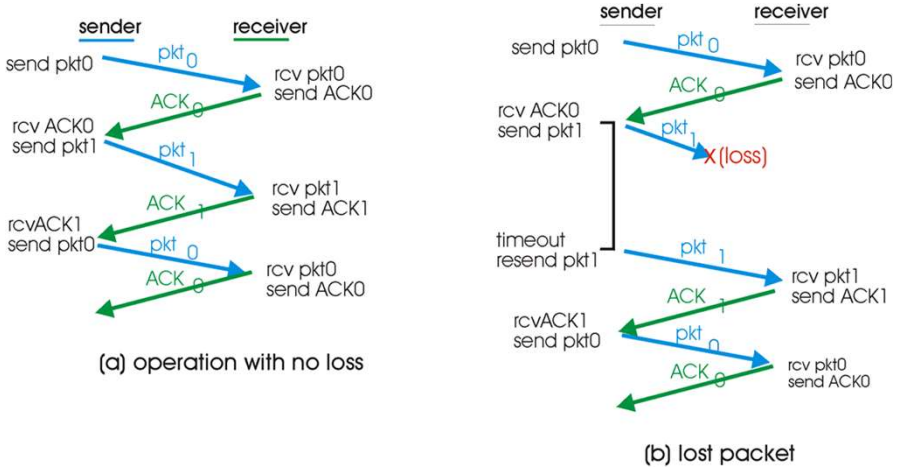
37

Stop-and-wait ARQ: When ACK is lost

- Data packet and ACK packet may be lost
  - No ACK is received at sender side
  - How a sender decides to resends data or not?
- Solution:
  - After sending out a packet, sender starts a timer specifying maximum waiting time (timeout) for an ACK of the packet.
  - When timeout expired sender re-sends the packet
- How long a Timeout should be?
  - At least 1 RTT (Round Trip Time)
- If a packet arrives at the destination but its ACK is lost, the packet is still resent because associated timeout expired.
  - The duplicated packets are eliminated at the receiver side according to repeated #seq.

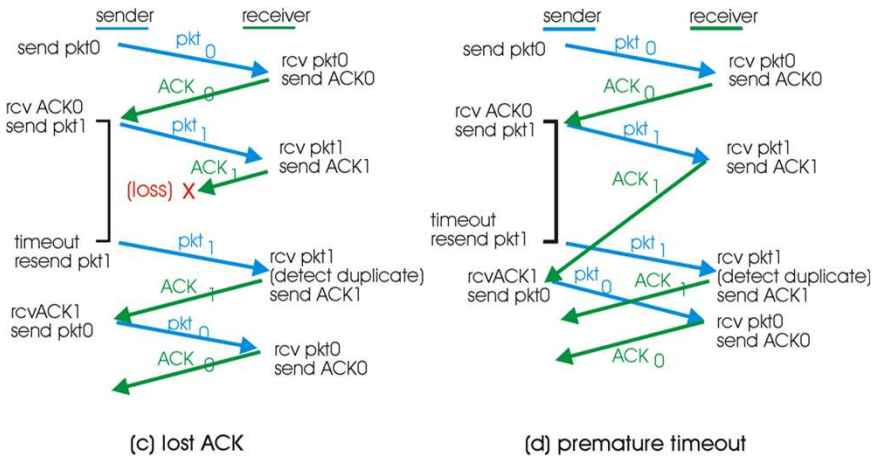
38

ARQ with timeout



39

ARQ with timeout



40

Flow control

ONE LOVE. ONE FUTURE.

41

41

What is flow control

- Goal: Make sure that the sender does not overload the receiver
- Why overloading?
  - The receiver stores data frame in buffer.
  - Receiver performs some processing before deliver data to the upper level.
  - Buffer could be full, leaving no space for receiving more frame → some data frame must be dropped.
- Problem of errors in transmission is excluded
  - All frames are transmitted to correct receiver without error
  - Propagation time is small and could be ignored
- Solution
  - Stop-and-wait mechanism
  - Sliding window mechanism

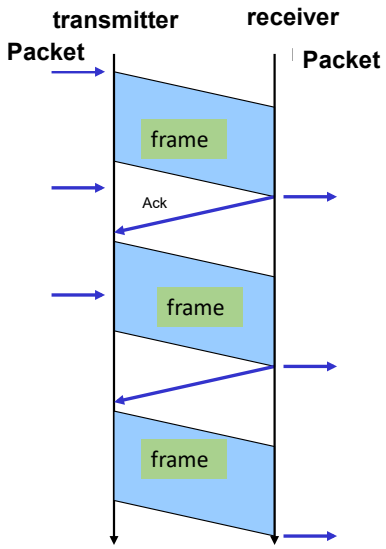
42

Stop-and-wait

- Principles
  - Transmitter sends a single frame
  - Receiver receives the frame, process and then informs the transmitter that it is ready to receives next frames by a clear acknowledgement (ACK).
  - Transmitter waits until reception of the ACK before sending next frames.

43

Stop-and-wait



44

Stop-and-wait

- Advantage
  - Simple, suitable for transmission of big size frames
- Weakness
  - When frames are small, the transmission channel are not used efficiently.
  - Cannot use often for big size frame due to
    - Limitation in buffer size
    - Big size frame prones to bigger error probability
    - In shared medium, it is not convenient to leave one station using medium for long time

45

Sliding window: principle

- Transmitter sends more than one frame without waiting in order to reduce waiting time
- Transmitted frame without ACK will still be stored in buffer.
- Number of frames to be transmitted without ACK depends on the size of buffer at transmitter
- When transmitter receives ACK, it realises the succesfully transmitted frame from buffers
- Transmitter continues sending a number of frame equivalent to the number of succesfully trasmitted frames.

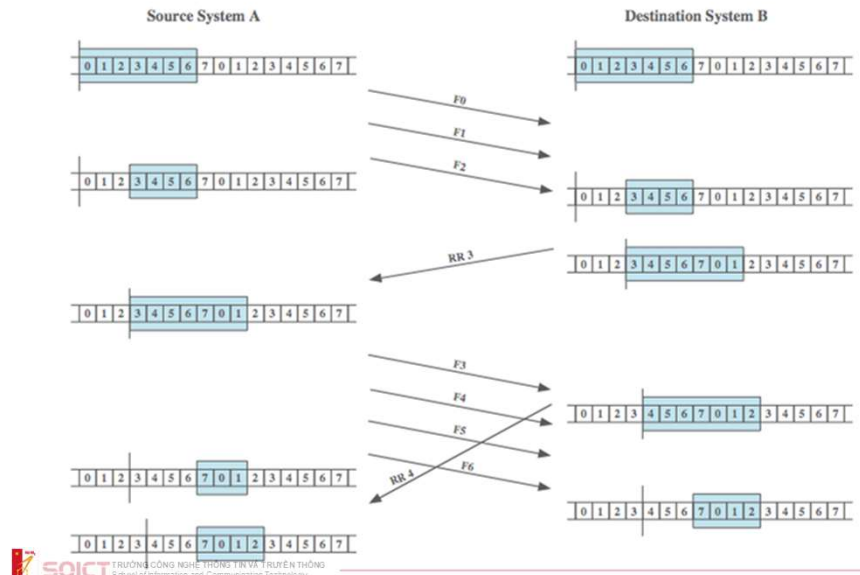
46

Sliding window: principle

- Assume that A and B are two stations connected by a full duplex media
  - B has a buffer size of n frame.
  - B can receives n frame without sending ACK
- Acknowledgement
  - In order to keep track of ACKed frames. It is neccessary to number frames.
  - B acknowledge a frame by telling A which frame B is waiting for (by number of frame), implicitely saying that B receives well all other frame before that.
  - One ACK frame serves for acknowledes several frames.

47

Sliding windows: principle

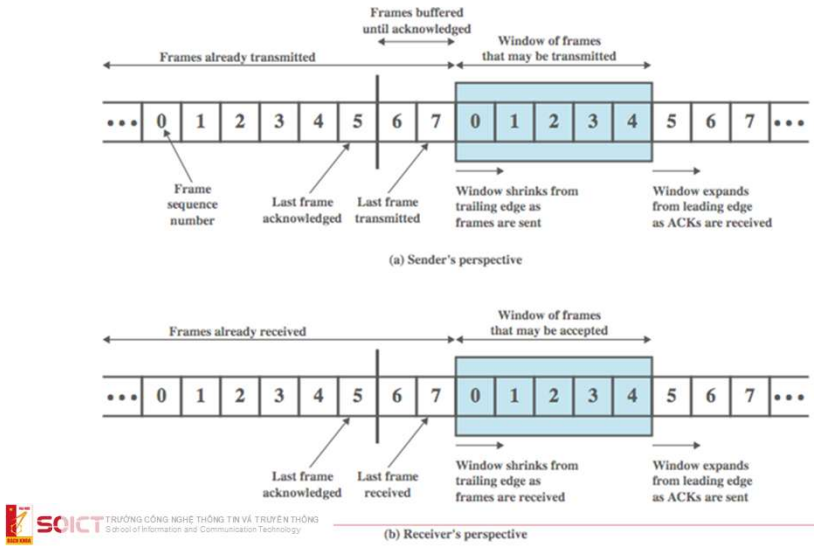


Window list the frames to transmit

Window list the frames in waiting to receive

48

Sliding windows



49

Sliding windows

- Frame are numbered. The maximum number must not be smaller than the size of the window.
- Frame are ACKed by another message with number
- Accumulated ACK: If frame 1,2,3,4 are well received, just send ACK 4
- ACK with number k means all frame k-1, k-2 …already well received.

50

Sliding windows

- Transmitter needs to manage some information:
  - List of frames transmitted sucessfully
  - List of frames transmitted without ACK
  - List of frames to be sent immediately
  - List of frames NOT to be sent immediately
- Receiver keep tracks of
  - List of frames well received
  - List of frames expected to receive

51

Piggy backing

- A and B transmit data in both sides
  - When B needs to send an ACK while still needs to send data, B attaches the ACK in the Data frame: Piggybacking
  - Otherwise, B can send an ACK frame separately
  - After ACK, if B sends some other data, it still put the ACK information in data frame.
- Sliding window is much more efficient than Stop-and-Wait
- More complicated in management.

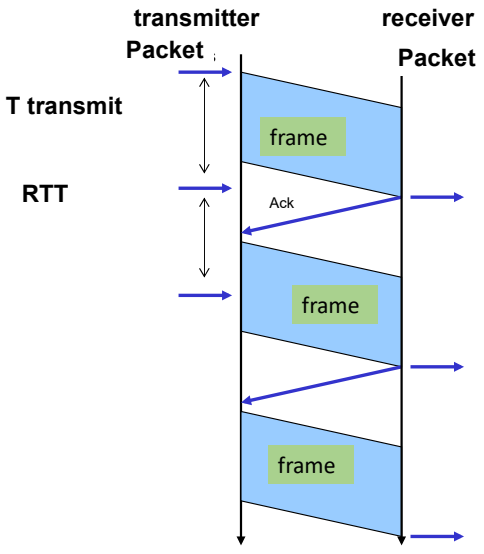
52

Exercices

- Given a link with rate R=100Mbps
- We need to send a file over data link layer with file size L=100KB
- Assume that the size of a frame is: 1KB, header size is ignored
- Round trip time (RTT) between 2 ends of the link is 3ms
- An ACK message is sent back from receiver whenever a frame is arrived. Size of ACK message is negligible
- What is the transmission time required if using Stop-and-wait mechanism?
- Transmission time with sliding window if the window size is =7?
- Which size of window allow to obtain the fastest transmission?

53

Transmission time with Stop-and-wait



54

Media access control

ONE LOVE. ONE FUTURE.

56

56

Connection types

- Point-to-point
  - ADSL
  - Telephone modem
  - Leased Line....
- Broadcast
  - LAN using bus topology
  - Wireless LAN
  - HFC:
  - ...
- Broadcast networks need media access control protocol in order to avoid collision when nodes try to send data.

57

Multiple access links, protocols

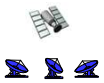
two types of "links":

- point-to-point
  - point-to-point link between Ethernet switch, host
  - PPP for dial-up access
- broadcast (shared wire or medium)
  - old-fashioned Ethernet
  - upstream HFC in cable-based access network
  - 802.11 wireless LAN, 4G/4G. satellite


shared wire (e.g., cabled Ethernet)


shared radio: 4G/5G


shared radio: WiFi


shared radio: satellite


humans at a cocktail party (shared air, acoustical)

58

Multiple access protocols

- single shared broadcast channel
- two or more simultaneous transmissions by nodes: interference
  - *collision* if node receives two or more signals at the same time

multiple access protocol

- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- communication about channel sharing must use channel itself!
  - no out-of-band channel for coordination

59

An ideal multiple access protocol

given: multiple access channel (MAC) of rate *R* bps

desiderata:

1. when one node wants to transmit, it can send at rate *R*.
2. when M nodes want to transmit, each can send at average rate *R/M*
3. fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. simple

60

MAC protocols: taxonomy

three broad classes:

- channel partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
  - e.g. time - TDMA, frequency- FDMA, Code- CDMA
- *random access*
  - channel not divided, allow collisions
  - "recover" from collisions
  - e.g. Pure Aloha, Slotted Aloha, CSMA/CD, CSMA/CA…
- "taking turns" (sequence access)
  - nodes take turns, but nodes with more to send can take longer turns
  - Token Ring, Token Bus

61

Channel division

- FDMA: frequency division multiple access
- TDMA: time division multiple access
- CDMA: code division multiple access

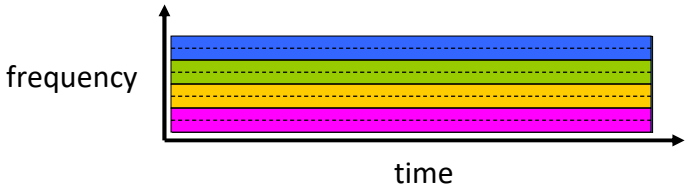
63

TDMA và FDMA

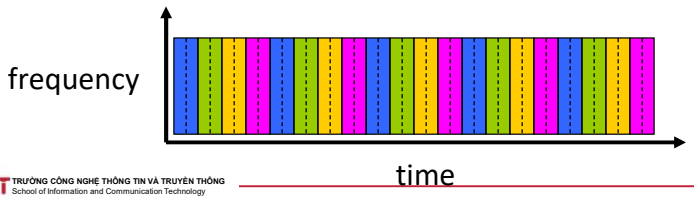
example

4 stations 

FDMA



TDMA:



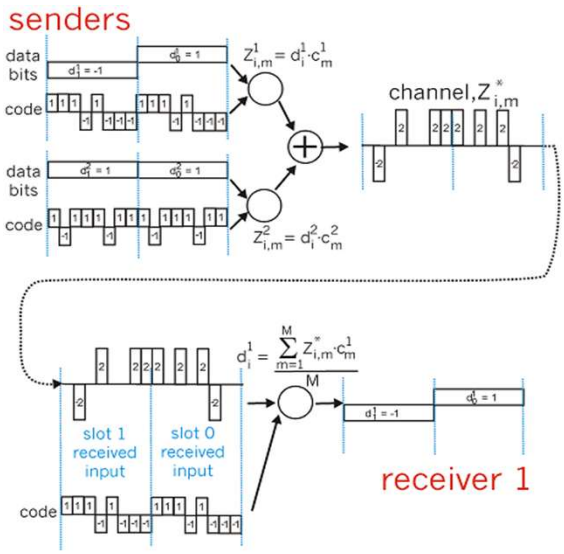
64

CDMA

- Several senders can share the same frequency on a single physical channel.
- Signals come from different senders are encoded (multiplied) with different random code. Those code must be orthogonal.
- Encoded signals are mixed and then transmit on a common frequency.
- The signals are recovered at the receiver by using finding the correlation with the same codes as at sender side.
- **CDMA** shows a lot of advantages that other technology cannot achieve. For example, the same frequency can be used in adjacent mobile cell without interference as if TDMA or FDMA are used

65

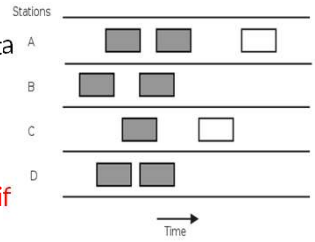
CDMA (example)



66

Random access: Pure Aloha

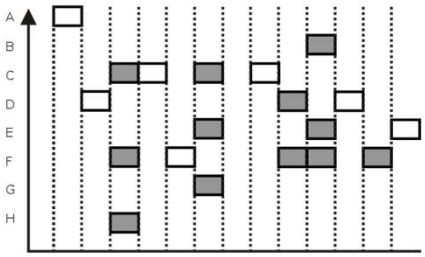
- Aloha is used in mobile network of 1G, 2.5G, 3G using GSM technology .
- Pure Aloha:
  - When one sender has data to send, just sends it
  - If while sending, the senders receive data from other stations → there is collision. All stations need to resend their data.
    - There are possibility to have collision when retransmit.
  - Problem: Sender does not check to see if the chanel is free before sending data
  - Grey package are having overlap in time→ causing collision



68

Random access: Slotted Aloha

- Times axe is divided into equal slots.
- Each station sends data only at the beginning of a time slot.
- → Collision possibility is reduced
- Still have collision in grey package



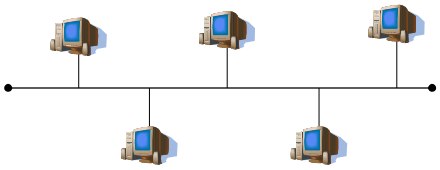
Slotted ALOHA protocol (shaded slots indicate collision)

69

Random access: CSMA

- CSMA: Carrier Sense Multiple Access
- CSMA idea is similar to what happens in a meeting.
- CSMA:
  - The sender "Listen before talk"
  - If the channel is busy, wait
  - If the chanel is free, transmit

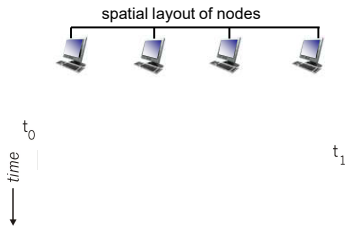
CSMA



- CSMA: Sender listens before transmission:
  - If the channel is free, send all the data
  - If the channel is busy, wait.
- Why there are still collision?
  - Due to propagation delay

Collision in CSMA

- Assume that there are 4 nodes in the channel
- The propagation of the signal from one node to the other requires a certain delay.
- Ex:
  - Transmissions from B and D cause collision

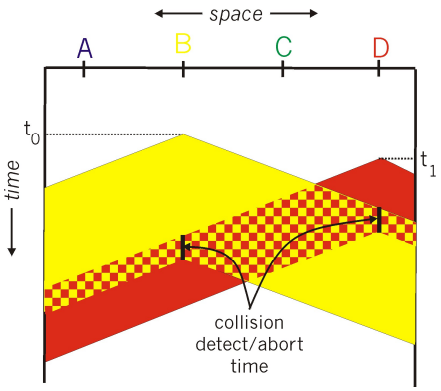


CSMA/CA (Collision Avoidance)

- CSMA/CA is used WIFI standard IEEE 802.11
- If two stations discover that the channel is busy, and both wait then it is possible that they will try to resend data in the same time.
  - → collision
- Solution CSMA/CA.
  - Each station wait for a random period → reduce the collision possibility

CSMA/CD

- Used in Ethernet
- CSMA with Collision Detection:
  - "Listen while talk".
- A sender listen to the channel,
  - If the channel is free then transmit data
    - While a station transmit data, it listens to the channel. If it detects a collision then transmits a short signal warning the collision then stop
    - Do not continue the transmission even in collision as CSMA
  - If the channel is busy, wait then transmit with probability p
- Retransmit after a random waiting time.



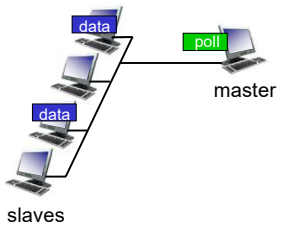
Comparison between channel division and random access

- Channel division
  - Efficient, treat stations equally.
  - Waste of resources if one station has much smaller data to send than the others
- Random access
  - When total load is small: Efficient since each station can use the whole chanel
  - When total load is large: Collision possibility increases.
- Token control: compromise between the two above methods.

"Taking turns" MAC protocols

polling:

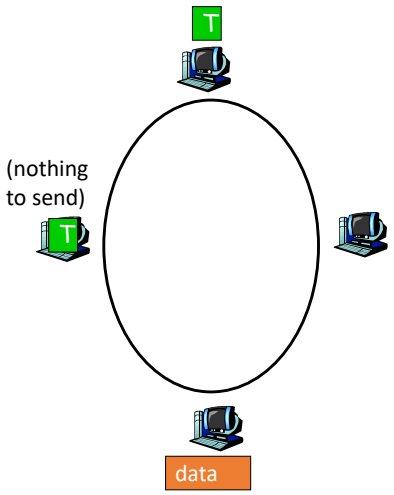
- master node "invites" other nodes to transmit in turn
- typically used with "dumb" devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)



76

Token Ring

- A "token" is passed from one node to the other in a ring topo
- Only the token holder can transmit data
- After finishing sending data, the token need to be passed to next nodes.
- Some problem
  - Time consuming in passing token
  - Loss of token due to some reasons



77

Summary on Media access control mechanisms

- Channel division
- Random access
- Token
- What do you thinks about their advantages and weaknesses ?

78

Point-to-Point forwarding mechanism

Hub, Switch, Bridge

ONE LOVE. ONE FUTURE.

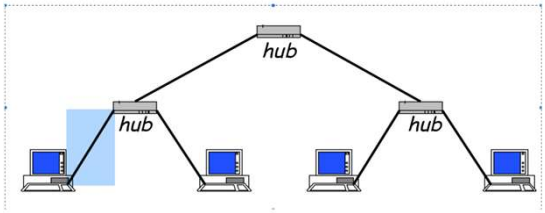
79

Devices of LAN

- Repeater, Hub, bridge and switch
  - All are LAN devices with many ports
- Repeater:
  - Repeats the bits received in one port to the other port
  - One network with repeaters = one collision domain
  - Repeater is a physical layer system.
- Hub:
  - Receive the signal from one port (amplify) and forward to the remaining ports
  - Do not offer services of datalink layer
  - Layer 1 intermediate system

80

Hub



Hub=Multiple port repeater
Single collision domain

Receive the signal from one port (amplify) and forward to the remaining ports

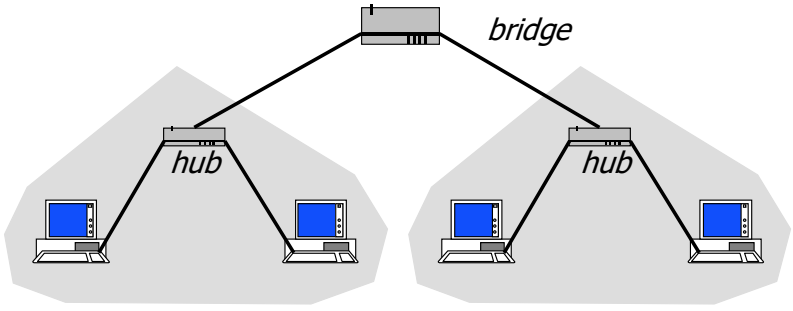
81

Devices of LAN (cont.)

- Bridge
  - More intelligent than hub
  - Can store and forward data (Ethernet frame) according to MAC address.
  - Bridge breaks the network into two collision domains.
  - Layer 2 intermediate system
- Switch
  - More ports than bridge
  - Can store and forward data according to MAC address
    - Receive full frame, check error, forward

82

Bridge

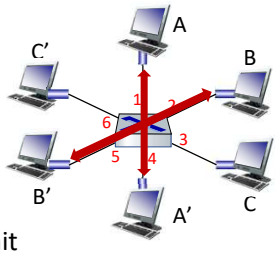


Two ports systems
- Forward frames from one port to the other based on MAC address
- Create two collision domains

83

Switch: multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions

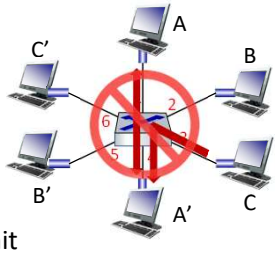


switch with six interfaces (1,2,3,4,5,6)

84

Switch: multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions
  - but A-to-A' and C to A' can *not* happen simultaneously



switch with six interfaces (1,2,3,4,5,6)

85

Switch forwarding table

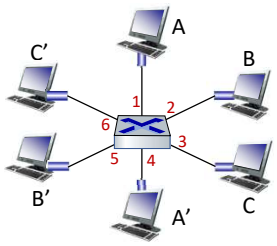
Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

A: each switch has a switch table, each entry:

- (MAC address of host, interface to reach host, time stamp)
- looks like a routing table! (Network layer)

Q: how are entries created, maintained in switch table?

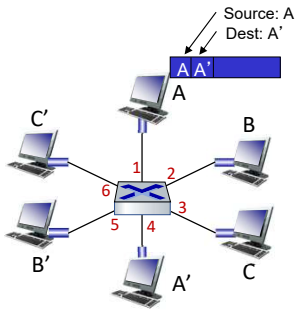
- something like an algorithm?



86

Switch: self-learning

- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table



MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

87

Switch: frame filtering/forwarding

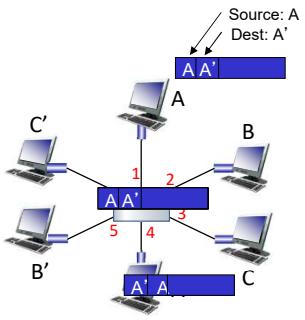
when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived
   then drop frame
   else forward frame on interface indicated by entry
   }
   else flood /* forward on all interfaces except arriving interface */

88

Self-learning, forwarding: example

- frame destination, A', location unknown: flood
- destination A location known: selectively send on just one link



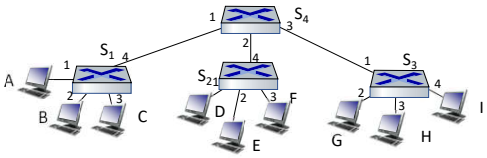
MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

89

Interconnecting switches

self-learning switches can be connected together:



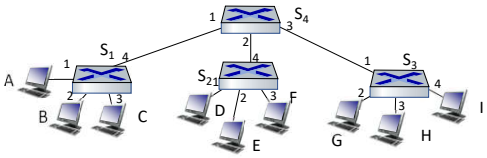
Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

- A: self learning! (works exactly the same as in single-switch case!)

90

Self-learning multi-switch example

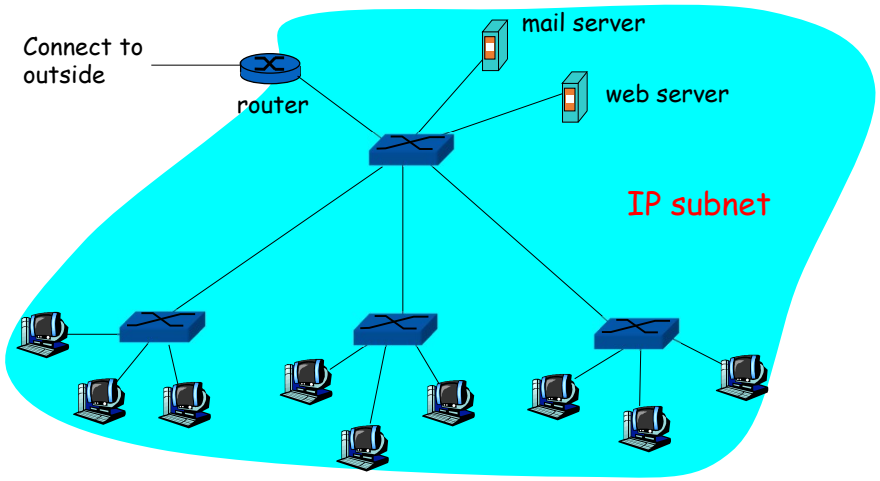
Suppose C sends frame to I, I responds to C



Q: show switch (MAC) tables and packet forwarding in S_1, S_2, S_3, S_4

91

A typical LAN



92

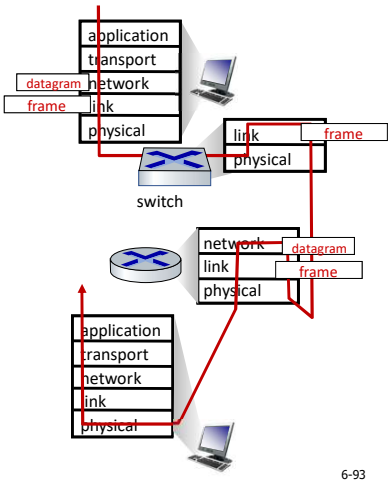
Switches vs. routers

both are store-and-forward:

- *routers*: network-layer devices (examine network-layer headers)
- *switches:* link-layer devices (examine link-layer headers)

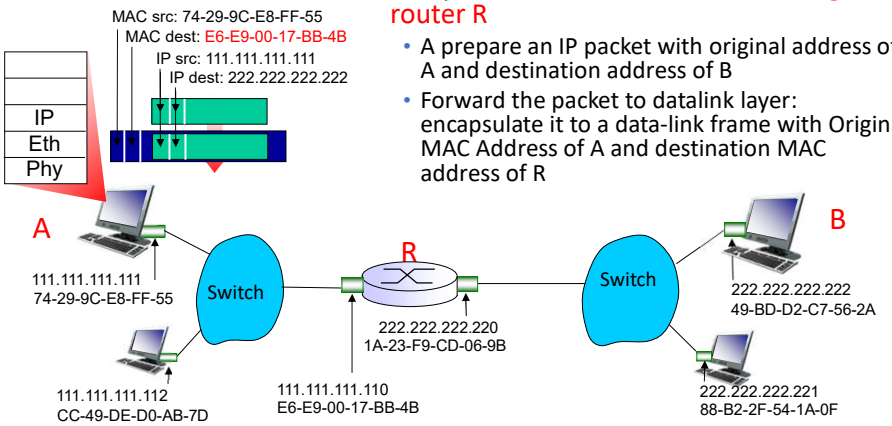
both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses



93

Router connects LANs

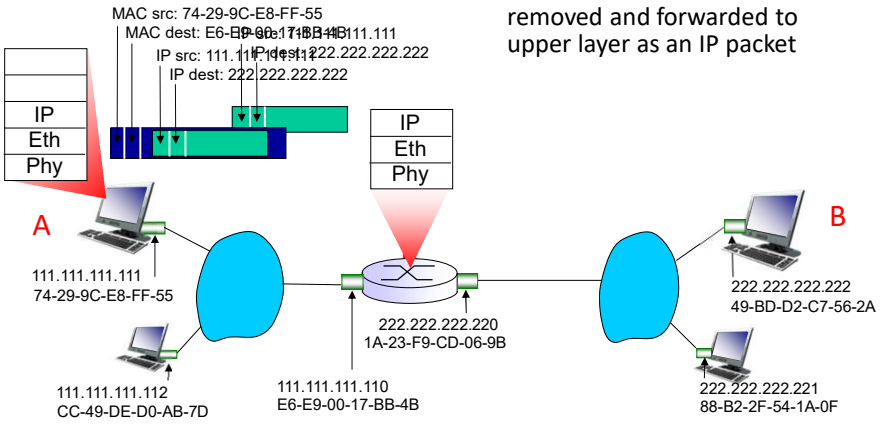


Example: Send data from A to B through router R

- A prepare an IP packet with original address of A and destination address of B
- Forward the packet to datalink layer: encapsulate it to a data-link frame with Original MAC Address of A and destination MAC address of R

Forward data to other LANs

- The frame is forwarded from A to R
- At R: the frame header is removed and forwarded to upper layer as an IP packet



LAN: Local Area Network

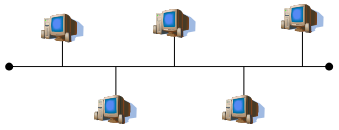
Reading: 4.3 Computer Networks, Tanenbaum

ONE LOVE. ONE FUTURE.

96

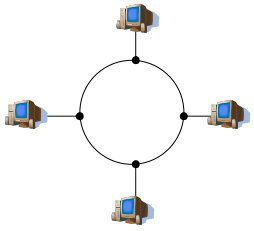
96

LAN topology

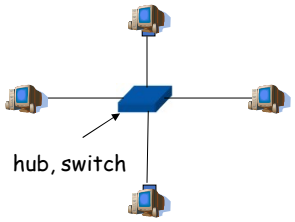


Traditional bus topo

WLAN



Ring



Star

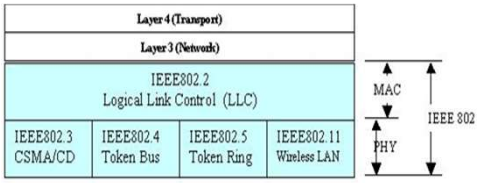
SOICT TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
School of Information and Communication Technology

97

97

LAN standards: IEEE 802.x

- IEEE 802.1 Network Management
- IEEE 802.2 Logical link control
- IEEE 802.3 Ethernet (CSMA/CD)
- IEEE 802.4 Token bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Networks
- IEEE 802.7 Broadband LAN using Coaxial Cable
- IEEE 802.8 Fiber Optic TAG
- IEEE 802.9 Integrated Services LAN
- IEEE 802.10 Interoperable LAN Security
- IEEE 802.11 Wireless LAN



- IEEE 802.12 demand priority
- IEEE 802.14 Cable modems
- IEEE 802.15 Wireless PAN
- IEEE 802.15.1 (Bluetooth)
- IEEE 802.15.4 (ZigBee)
- IEEE 802.16 WiMAX
- V.v…

98

LLC: IEEE802.2

- Roles:
  - Connect with protocols of Network Layer: IPX, DCE, IP, v.v..
  - With different physical layers: cable, wireless, optical
- Functionalities:
  - Multiplexing/ Demultiplexing
  - Flow control with 3 different modes:
    - Unacknowledged connectionless
    - Acknowledged connectionless
    - Connection mode

802.2 LLC Header			Information
DSAP address	SSAP address	Control	
8 bits	8 bits	8 or 16 bits	multiple of 8 bits

- Frame structure:
  - DSAP & SSAP: Destination/Source SAP, for Multiplexing/ Demultiplexing of the upper layer (which entity of the Network Layer is sending/ receiving LLC frames)
  - Control: define PDU to transfer and control:
    - U-frame: send/receive in connectionless mode (U: Unnumbered)
    - I-frame: frame with information (I: Information), used in acknowledged mode
    - S-frame: for controlling (S: Supervisor)

99

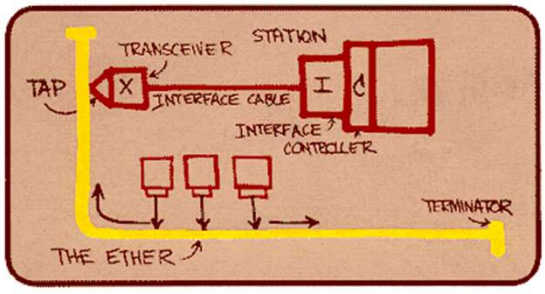
Practical LLC

- Error checking and flow control (I-frame and S-frame) are used by some upper protocols (NetBIOS).
- U-frame encapsulate PDU without numbering (unnumbered) and therefore NO flow control or error checking are provided.
- Most upper protocols of LLC (TCP/TP) support error checking and flow control
  - Only use LLC as "Unacknowledged connectionless" with U-frame.

100

Ethernet LAN

- Layer 2 technology for communication in LAN, invented in 1976
- Standardized in IEEE 802.3
- Ethernet LAN could have different speeds: 3 Mbps – 10 Gbps
  - Ethernet: 10BaseT, 10Base2...
  - Fast Ethernet: 100BaseT
  - Giga Ethernet

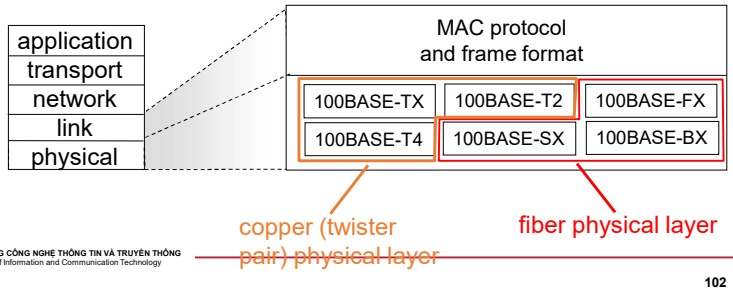


Metcalfe's Ethernet sketch

101

IEEE 802.3 and Ethernet Standards

- Datalink & Physical Layers
- Datalink= LLC + MAC
- MAC: CSMA/CD in classical Ethernet
- Several type of Ethernet
  - Same MAC and frame structure
  - Different rate: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10G bps
  - Different cable: Optical fiber, coaxial, twisted pair



102

Ethernet frame

- Preamble: Marking the starting of a frame
- Address: Physical addresses of source and destination
  - 6 bytes
- Type: Upper layer protocol (IP, Novell IPX, AppleTalk, ...)
- Checksum: Error detection code. CRC??

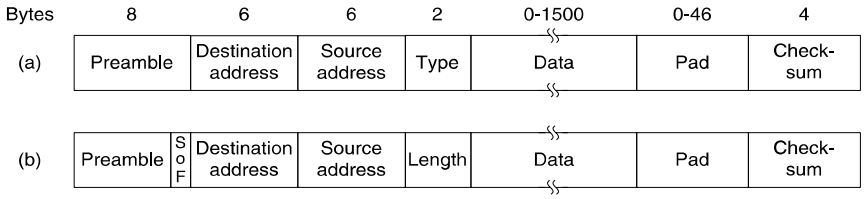
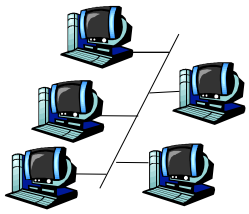


Figure 4-14. Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

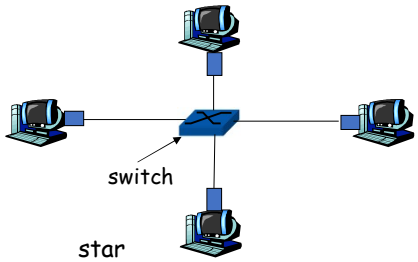
105

Switched Ethernet

- Switched Ethernet (popular nowdays):
  - Star topology,
  - Use a central switch Ethernet
  - The switch outputs a frame only to the port linking to the destination ➔ independent connection for each pair of two nodes
  - No collision
  - No media access control is needed.



bus: coaxial cable



star

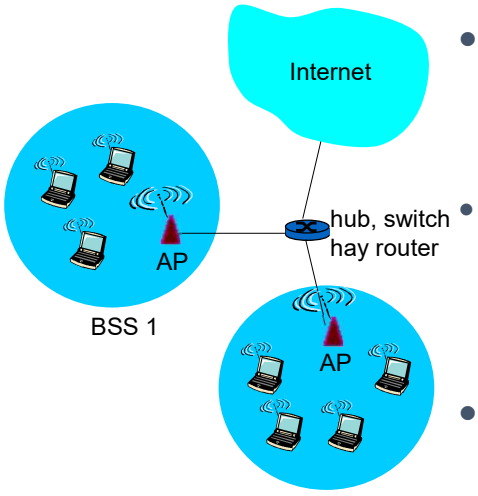
106

Wireless LAN

ONE LOVE. ONE FUTURE.

107

Overview of 802.11 LAN



- Include base station = access point) and stations with wireless network interfaces
- Base station mode
  - Basic Service Set (BSS)
    - wireless hosts
    - access point (AP): base station
- Ad hoc mode:
  - Stations pay also the role of AP

108

Standards

- 802.11b
  - Band 2.4-5 GHz (unlicensed spectrum)
  - Maximum speed 11 Mbps
- 802.11a
  - Band 5-6 GHz
  - Maximum speed 54 Mbps
- 802.11g
  - Band 2.4-5 GHz
  - Maximum speed 54 Mbps
- 802.11n: use multiple antennas (MIMO)
  - Band 2.4-5 GHz
  - Maximum speed 200 Mbps

- Employ CSMA/CA for multiple access control
- Working in 2 modes : base-station and ad hoc

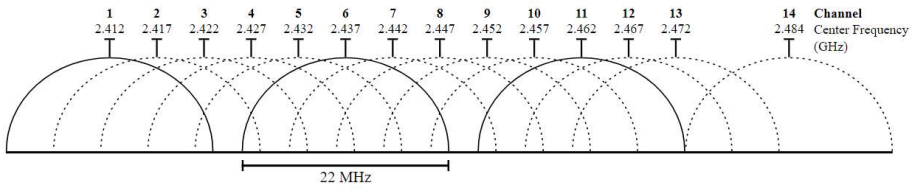
109

802.11: Chanel and connection

- Band is divided into 14 channels spaced 5MHz apart. Europe uses 13 channels, America uses 11 channels, Japan uses 14 channels.
  - Admin chooses a working frequency for AP (may leave AP to choose automatically)
- Station: need to connect to an AP
  - Scan channels, listen to initial frames (*beacon frames)* containing the ID (SSID) and MAC address of the AP
  - Choose one AP.

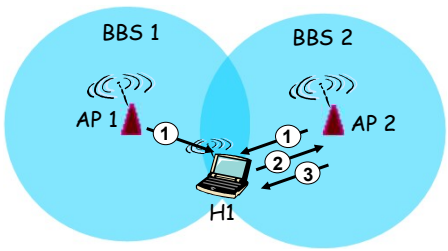
110

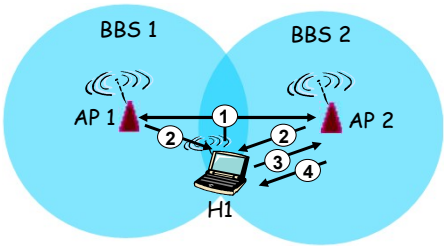
802.11: Chanel and connection



111

Scanning mechanism: active/passive



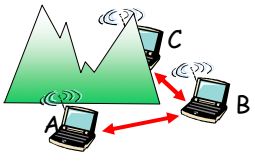


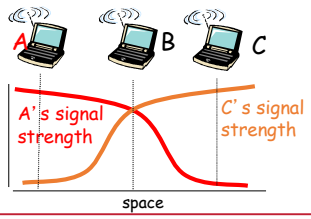
Passive Scanning:
(1) Beacon frames are sent from APs
(2) H1 send a connection request to AP2
(3) AP2 accepts the request

Active Scanning:
(1) H1 broacast the request to find an AP
(2) APs reply with their information
(3) H1 send a connection request to AP2
(4) AP2 accepts the requests

IEEE 802.11: Multiple access control

- 802.11: CSMA
- 802.11: CA – Collision Avoidance
  - It is difficult to implement Collision detection (CD) in wireless environment.
  - In some cases, it is even impossible to detect the collision : hidden terminal, fading





IEEE 802.11 MAC Protocol: CSMA/CA

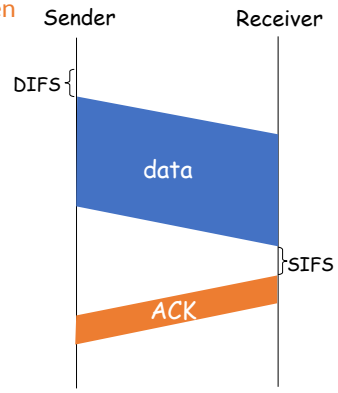
Sender

1 If the channel is available during **DIFS** time then
Send the entire frame (no CD)

2 if channel is busy then
Starting random back-off (waiting)
At the end of back-off time, send data
If no ACK is received, double the back-off time and try again.

Receiver

- If receive well a frame then
reply by an ACK after **SIFS**



Why need ACK?

DIFS: Distributed Inter Frame Space

SIFS: Short Inter Frame Space

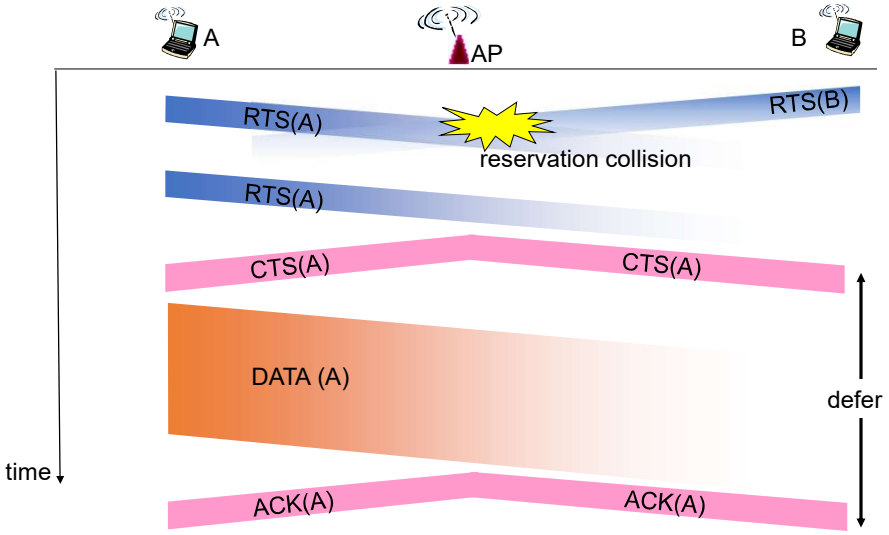
Avoid Collision mechanism

Idea: Sender can reserve channel without random access→ avoid collision for long frame

- Sender send frame RTS (request-to-send) to BS using CSMA
  - RTS may meet a collision (with low probability because the frame is short)
- BS broadcast the frame CTS (clear-to-send CTS) to answer
- All stations receive CTS
  - Sender send data frame
  - All other stations has to cancel the intention to send frames.

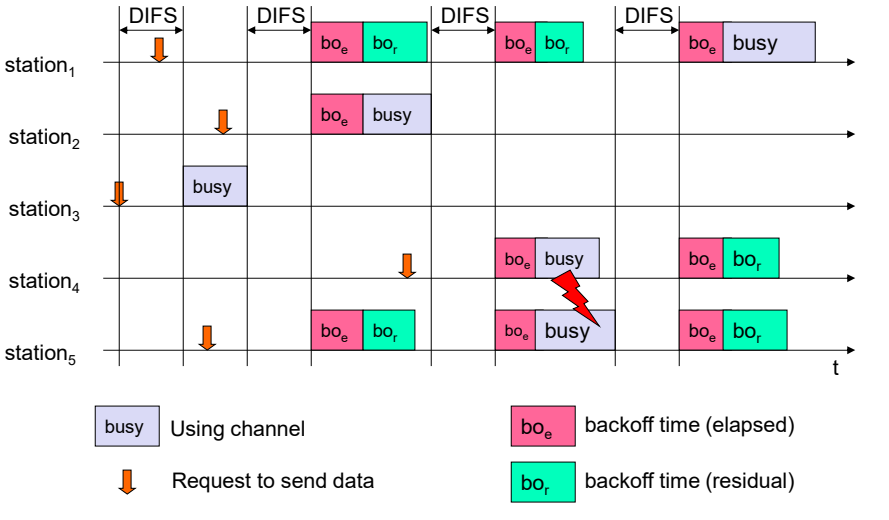
Avoid collision thanks to the reservation made by small size control frames

Collision Avoidance using RTS-CTS



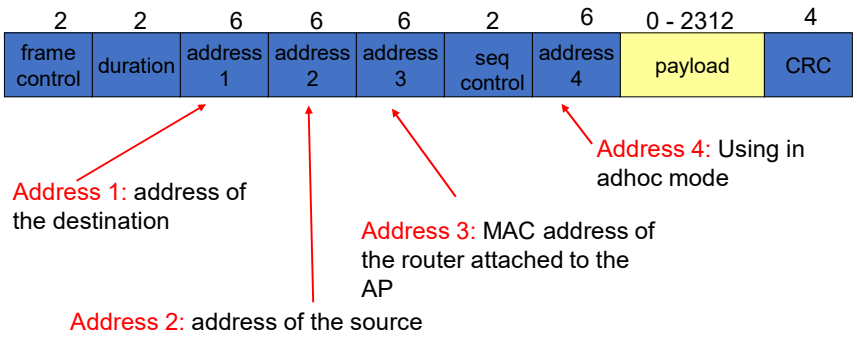
116

Example of CSMA/CA on 802.11



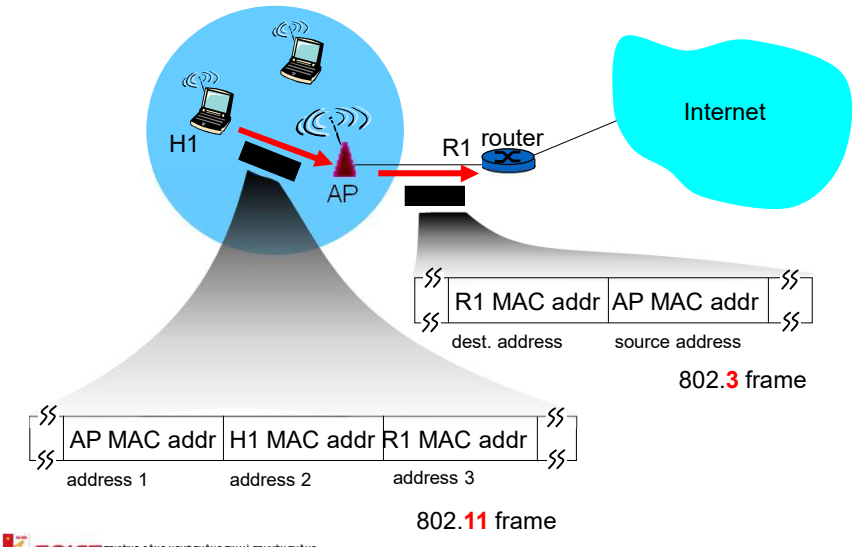
117

802.11 frame: Addressing



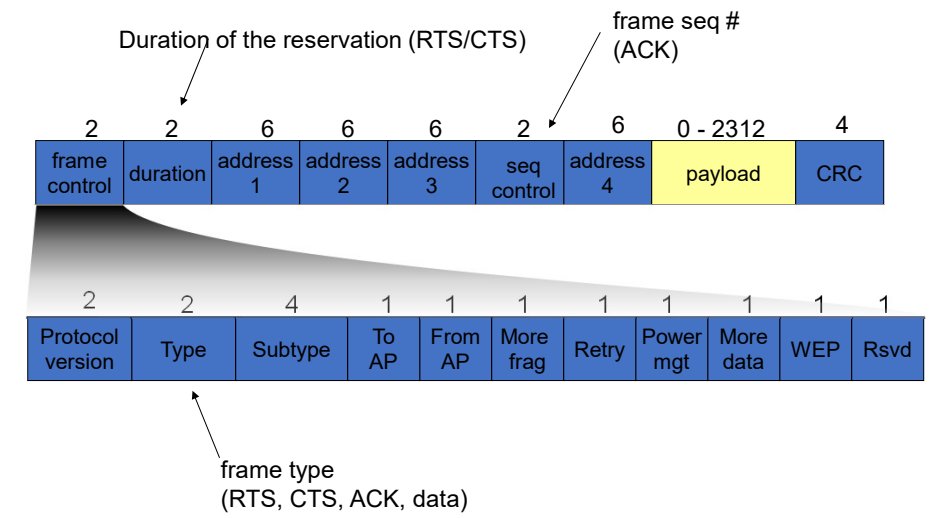
118

802.11 frame: Addressing



119

802.11 frame



120

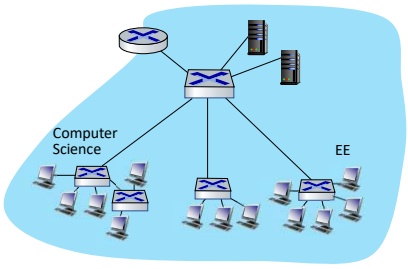
Virtual LAN

ONE LOVE. ONE FUTURE.

121

Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?



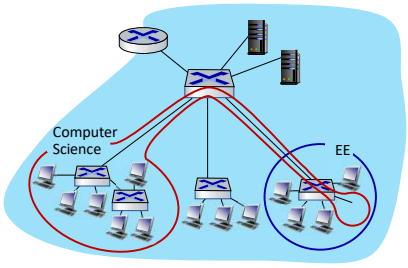
single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy issues

122

Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy, efficiency issues

administrative issues:

- CS user moves office to EE - *physically* attached to EE switch, but wants to remain *logically* attached to CS switch

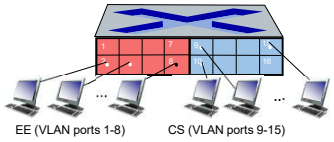
123

Port-based VLANs

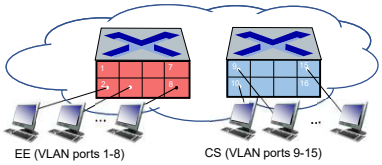
Virtual Local Area Network (VLAN)

switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



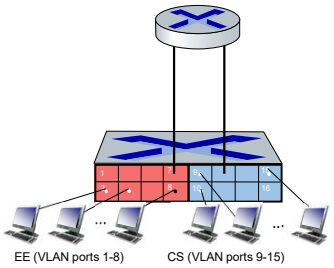
… operates as multiple virtual switches



124

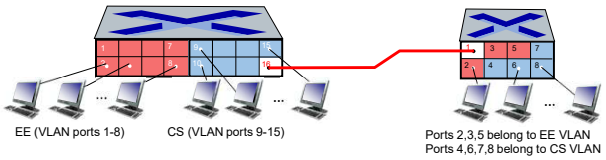
Port-based VLANs

- traffic isolation: frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- dynamic membership: ports can be dynamically assigned among VLANs
- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers



125

VLANS spanning multiple switches

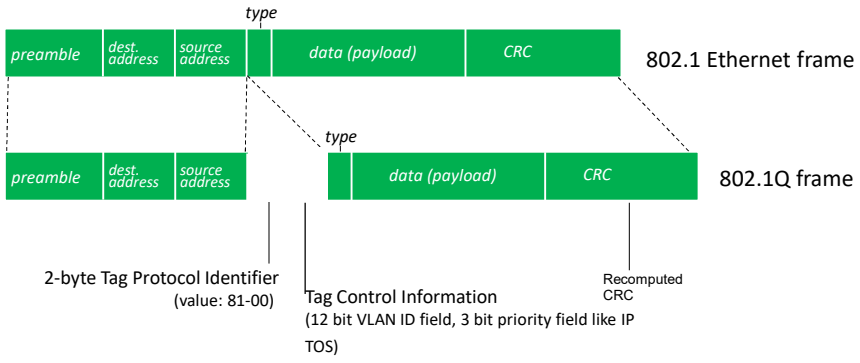


trunk port: carries frames between VLANS defined over multiple physical switches

- frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
- 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

126

802.1Q VLAN frame format



127

Access networks using optical fiber

ONE LOVE. ONE FUTURE.

128

Access networks

- Access networks gather data from users to feed to core network
- Popular access networks for providing services to users
  - Public telephone network
  - TV Cable network
  - Internet to home network.

129

Architecture of access network

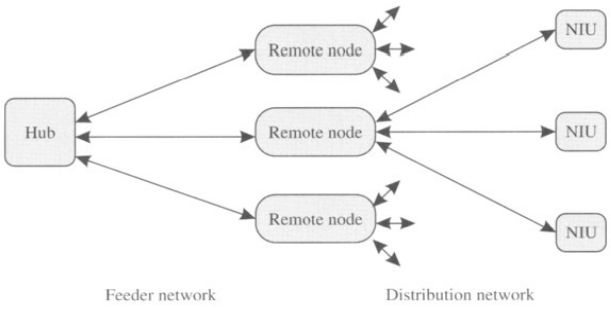


Figure 11.1 Architecture of an access network. It consists of a hub, which is a telephone company central office or cable company head end, remote nodes deployed in the field, and network interface units that serve one or more individual subscribers.

130

Architecture of access network

- Hub
  - Device on the service provider side receiving data
- Network Interface Unit (NIU)
  - Device on the user side connecting an user or an organization
- Remote Node (RN)
  - In broadcasting networks, RN distribute data from Hub to NIUs
  - In switched networks, RN receive data from Hub and distribute different flows to NIUs

131

Technologies for connecting to ISP using cable

- Dial-up:
  - speed 56kbps,
  - Using telephone line
  - Data is transmitted using the same frequency with voice → either data or voice communication available
  - Obsolete technology, used before 2000
- ADSL technology:
  - Speed few Mbps,
  - Using telephone line
  - Data is transmitted in different frequency than voice, technology used in 2000-2010
- Technology using TV cable
- FTTH technology:
  - Speed dozens Mbps,
  - Using optical fiber
  - Popular technology nowadays

132

Optical access network: FTTx

- Data is distributed on the fiber cable in the distribution network until ONU (Optical Network Unit)
  - Expectation: fiber approaches the customers
- **FTTCab** (*Fiber To The Cabinet*): Optical fiber ends at a cabinet in less than 1 km distance to the subscriber using copper cable.
- **FTTC** (*Fiber To The Curb*) / **FTTB**(*Fiber To The Building*); ONU serves some subscribers (8 to 64); from ONU to NIU using copper cable (< 100m)
- **FTTH** (*Fiber To The Home*); ONUs performs the functionality of NIUs;

133

Optical access network: FTTx

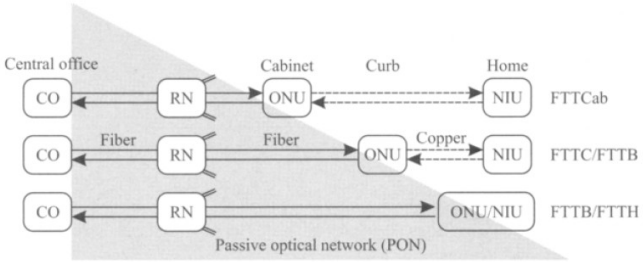


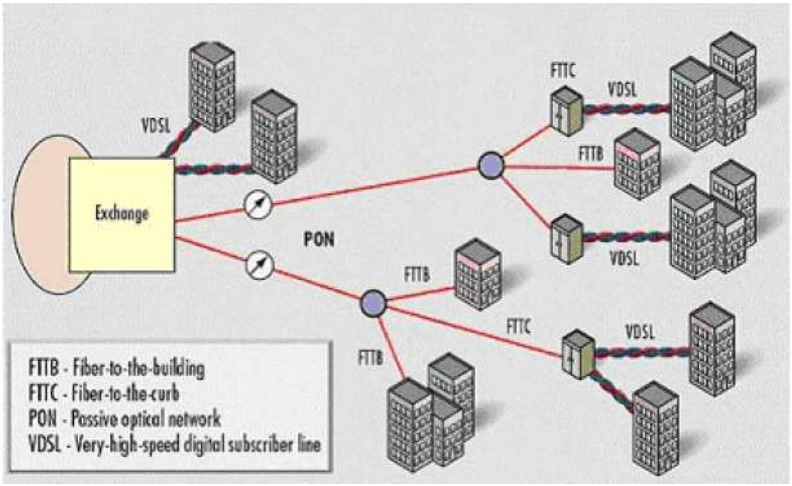
Figure 11.5 Different types of fiber access networks, based on how close the fiber gets to the end user. In many cases, the remote node may be located at the central office itself. The ONUs terminate the fiber signal, and the links between the ONUs and the NIUs are copper based.

An example of ONU: optical modem

Figure taken from book Optical Networks: A Practical Perspective, Rajiv Ramaswami, Kumar Sivarajan

134

Optical access networks: FTTx



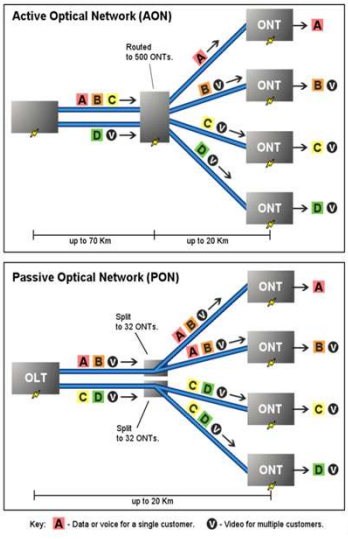
135

AON vs. PON

Remote Note (Distribution nodes) distribute data toward destinations.

AON: Active Optical Network
-Remote Node consume electricity
-Remote node analyse and forward packets to destination according to addresses
-Cable distance can go up to 100 km.

PON: Passive Optical Network
-Remote Node does not consume electricity
-Remote node (Splitter) does not analyze but repeat signal to all out ports
-Upstream: MUX from different sources using TDM (TDM PON) or WDM (WDM PON)
-Cable distance is limited within 20km



SOICT TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
School of Information and Communication Technology

136

EPON: Ethernet PON

- EPON: PON transport Ethernet frames
- Down stream
  - Broadcast common data

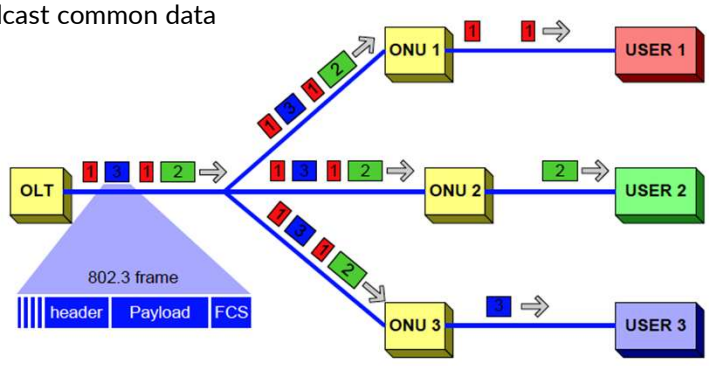


Figure 8-6. Downstream traffic in EPON.

SOICT TRƯỜNG C
School of Inf

137

EPON

- Upstream: Mux Ethernet frames from users to the common link OLT-RN using TDM

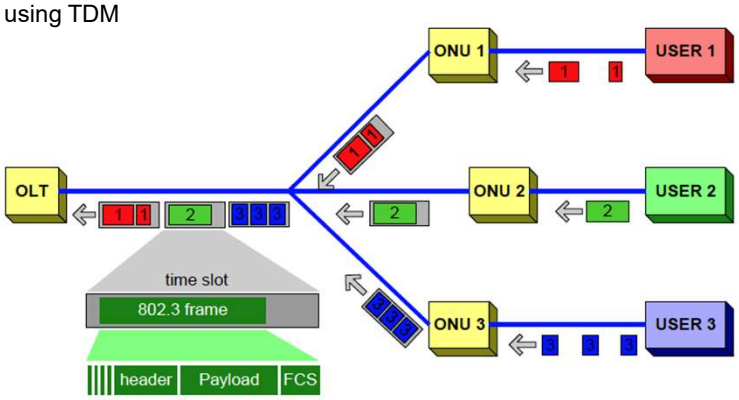


Figure 8-7. Upstream traffic in EPON.

138

GPON: Gigabit Capable PON

- GPON may be used to carry different data: Ethernet, ATM, voice …
- Data from OLT to users share common channel between OLT or RN
  - Downstream broadcast
  - Upstream TDM
  - Data are encapsulated in GPON frames with ID of the receiver (downstream direction), sender (upstream direction)

SOICT TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
School of Information and Communication Technology

139

139

WPON (WDM PON)

- Developed by companies and has not been standardized
- Each ONT use a wavelength to transmit data
- Remote note is AWG (arrayed waveguide grating). The AWG is capable to MUX/DEMUX wavelengths from up and down streams.