COMPUTER NETWORKS AND INTERNET PROTOCOLS

ARP – RARP – BOOTP - DHCP

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

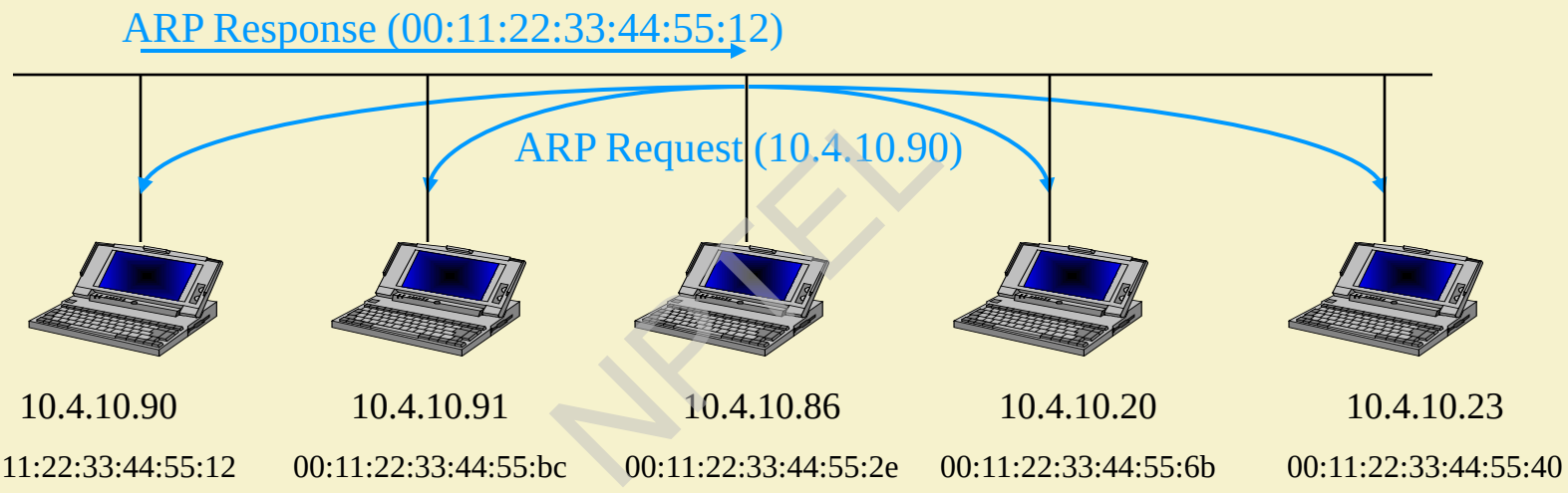
Address Resolution Protocol (ARP)

- Two machines on a given network can communicate only if they know each other's physical network address

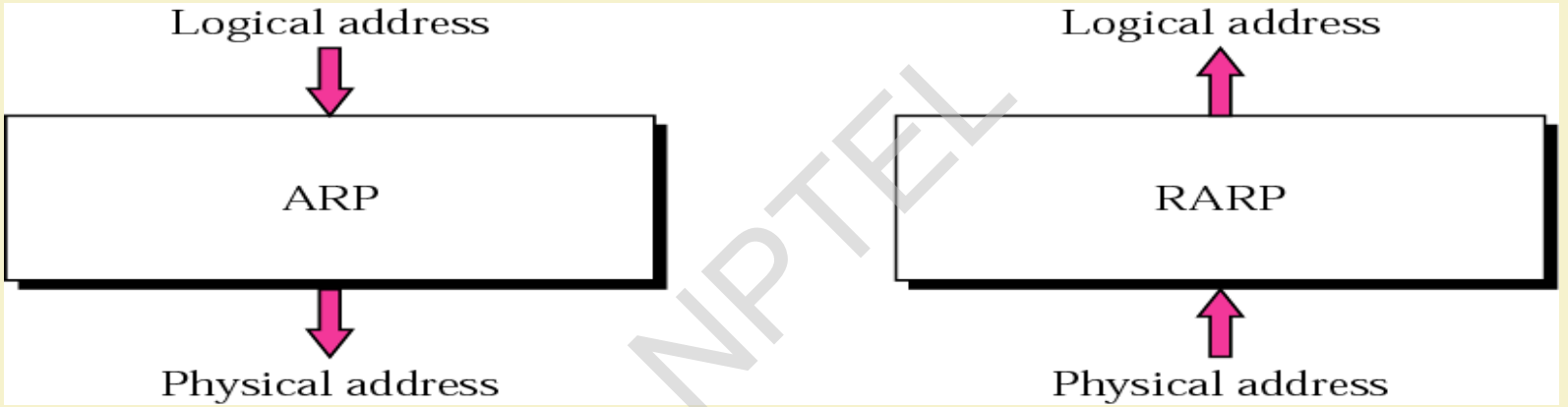
- ARP (Address Resolution Protocol) serves for mapping from high-level IP address into low level MAC address.

Ref: Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; Local & Metropolitan Area Networks, L. Christofi; TCP/IP Tutorials, IBM Redbooks

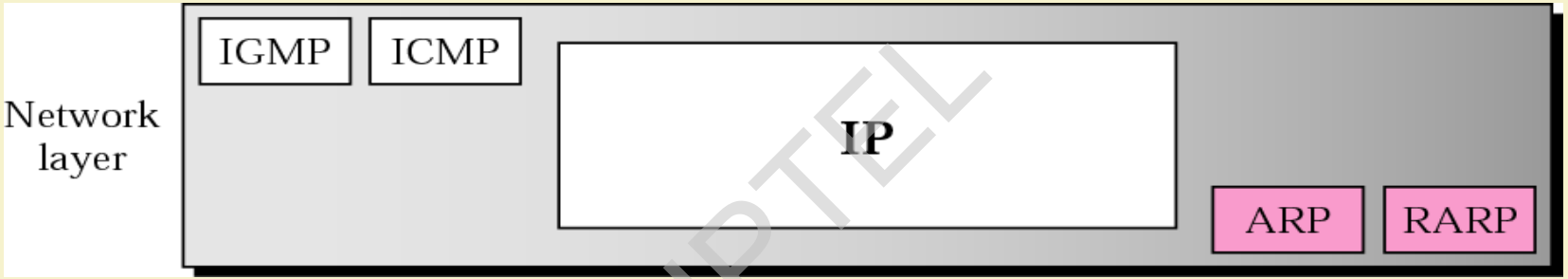
ARP


ARP Response (00:11:22:33:44:55:12)
ARP Request (10.4.10.90)
10.4.10.90
00:11:22:33:44:55:12
10.4.10.91
00:11:22:33:44:55:bc
10.4.10.86
00:11:22:33:44:55:2e
10.4.10.20
00:11:22:33:44:55:6b
10.4.10.23
00:11:22:33:44:55:40

ARP


Logical address
ARP
Physical address
Logical address
RARP
Physical address

ARP and RARP positions in TCP/IP protocol suite?

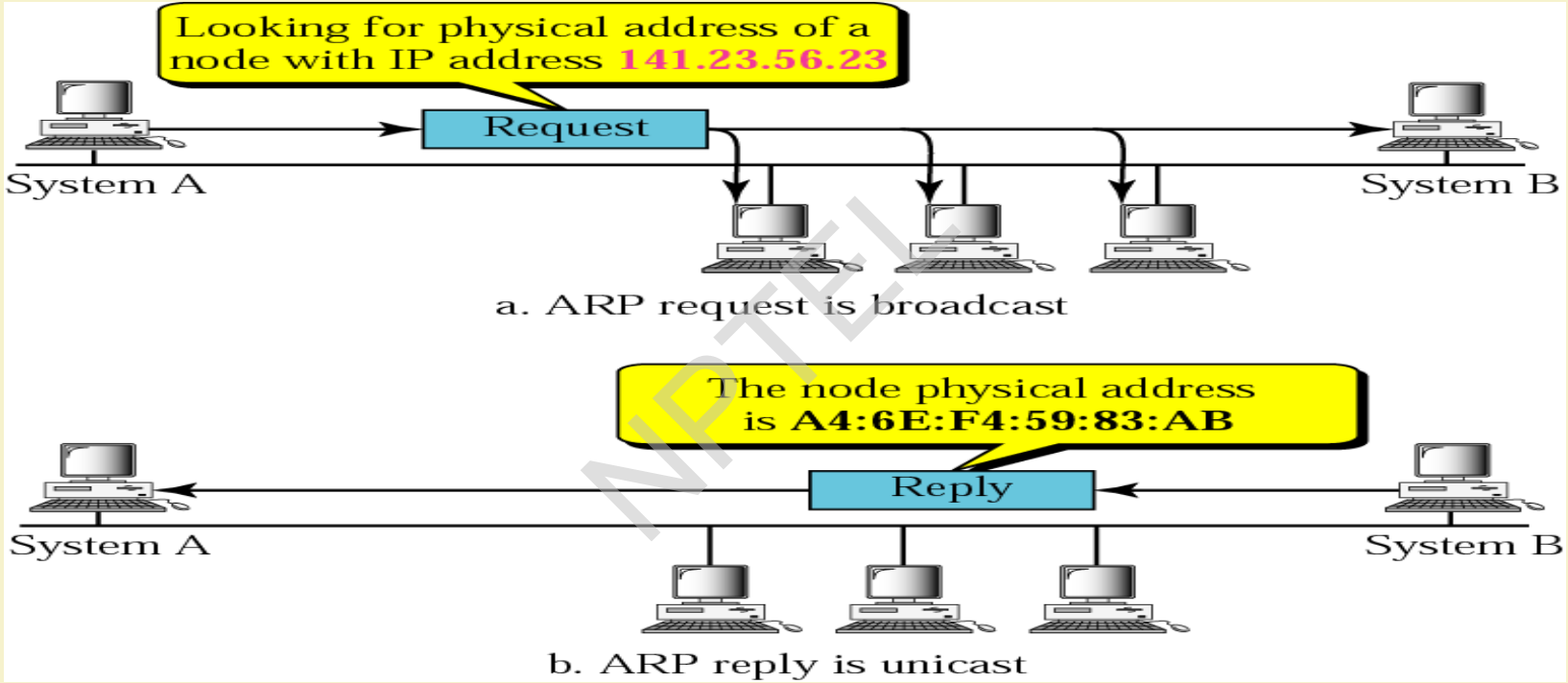


ARP

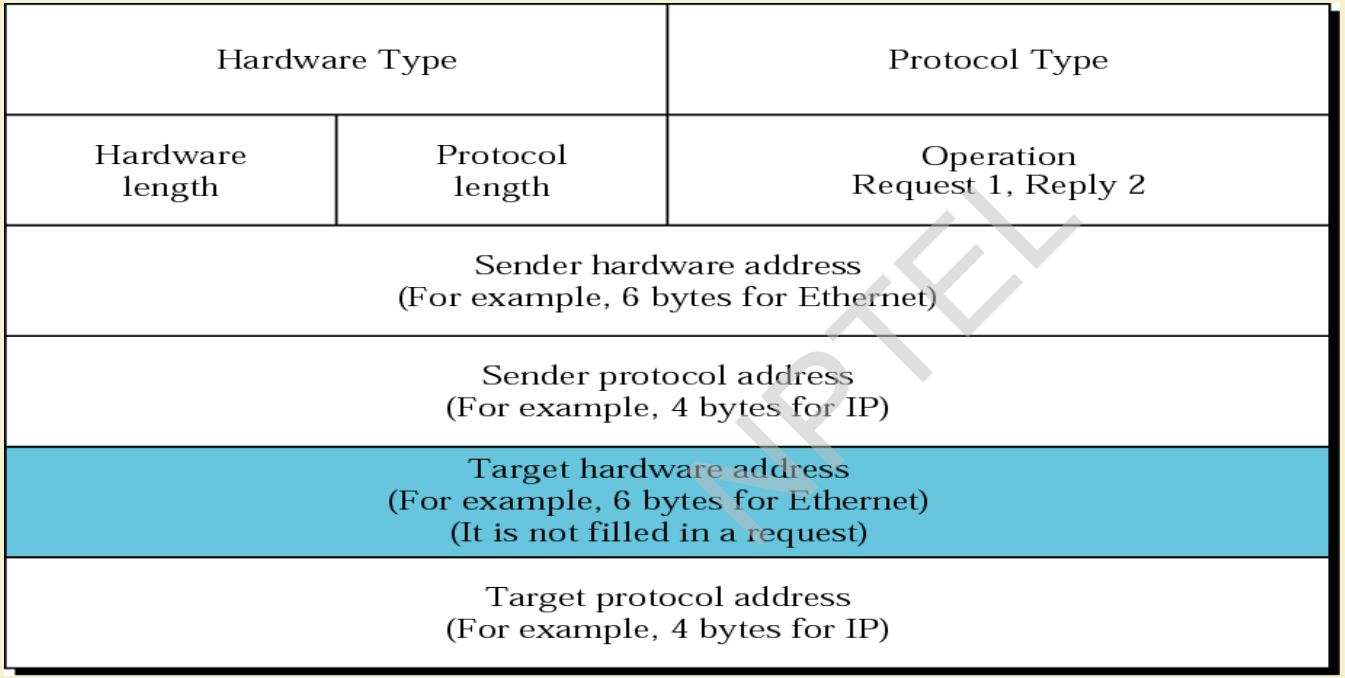
ARP associates an IP address with its Physical Address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC.

Logical address to physical address translation can be done statically (not practical) or dynamically (with ARP).

ARP Operation



ARP Packet



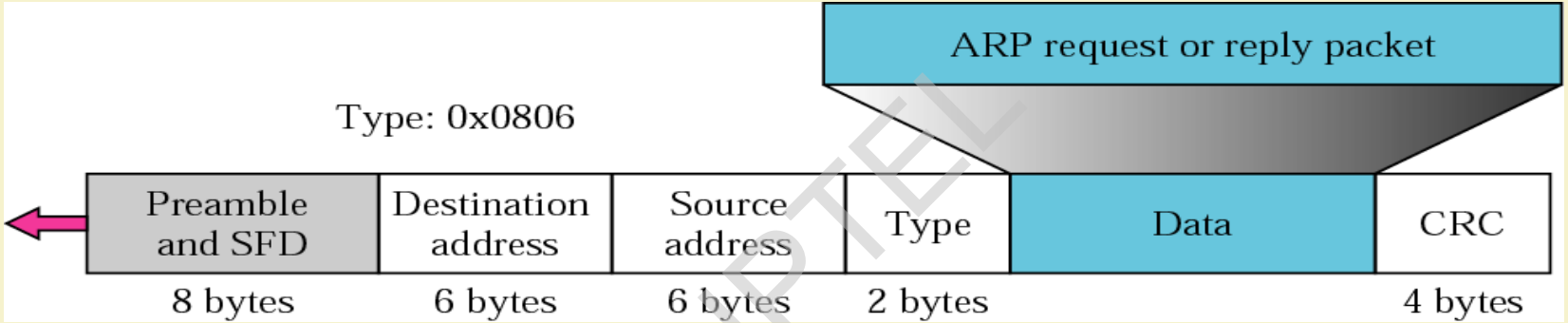
Hardware Type - Ethernet is type 1

Protocol Type- IPv4=x0800

Hardware Length: length of Ethernet Address (6)

Protocol Length: length of IPv4 address (4)

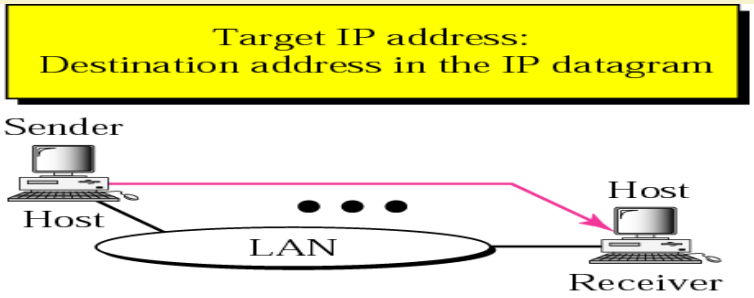
Encapsulation of ARP packet



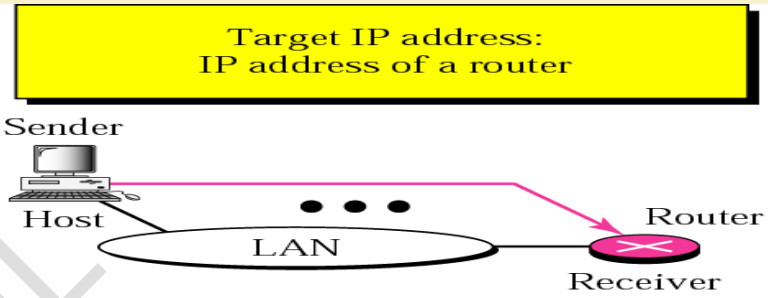
ARP packet is encapsulated within an Ethernet packet.

[*Type field for Ethernet is x0806*]

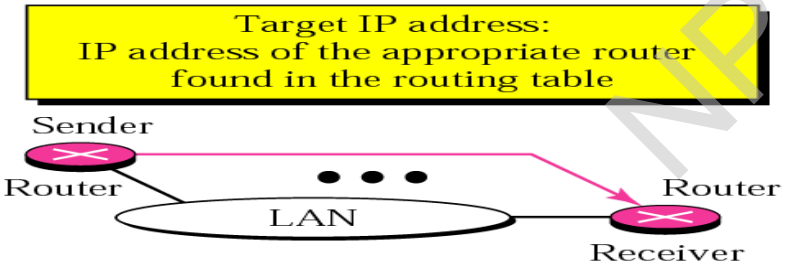
Four Cases using ARP



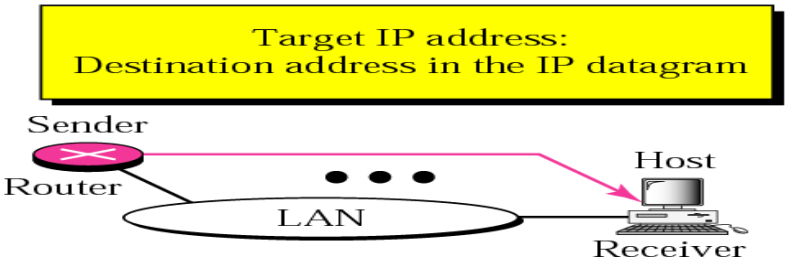
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.

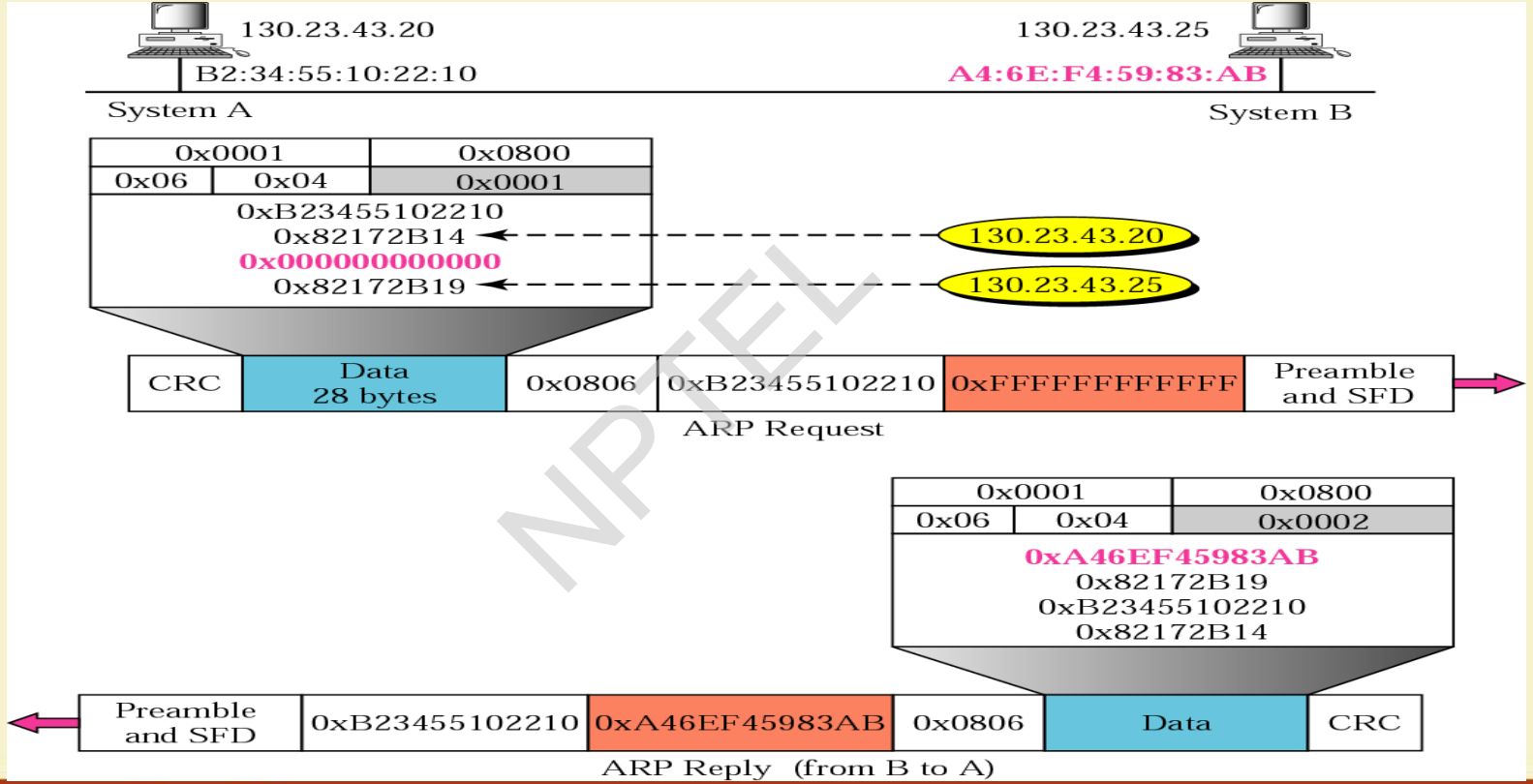


Case 4. A router receives a packet to be sent to a host on the same network.

Example:

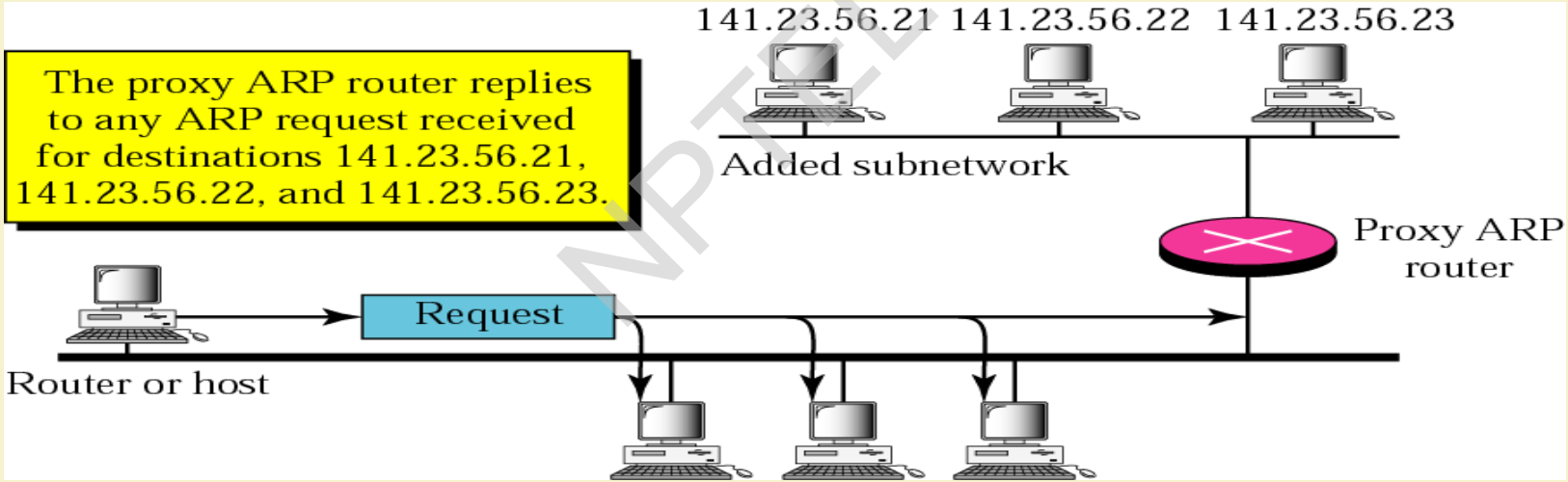
A host with IP address 130.23.43.20 and physical address B2:34:55:10:22:10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Example:



Proxy ARP

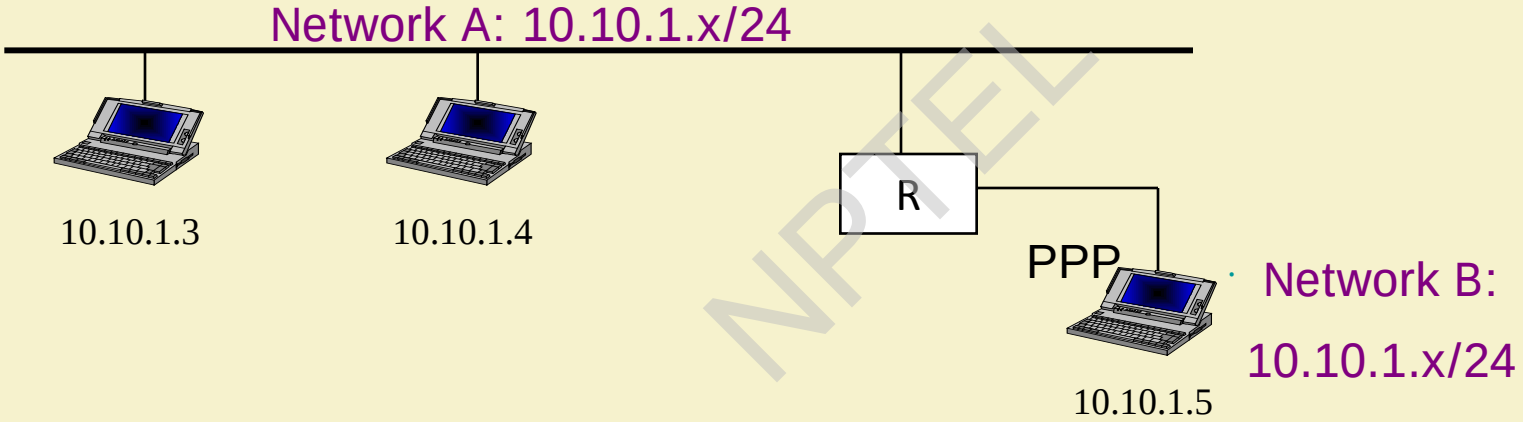
A proxy ARP, running in a router, can respond to an ARP request for any of its proteges. The proxy ARP replies with its own MAC address. When the packet arrives, the router delivers it to the appropriate host.



Proxy ARP

- **Proxy ARP** (also called promiscuous ARP or ARP hack) is a technique used to map a single IP network prefix into two or more physical addresses.
  - Using the same network address space for more than one physical address
- Assume that there are two networks *A* and *B* connected by router *R* that runs *Proxy ARP*
- Using Proxy ARP, R can use the same net-id for both networks.

Proxy ARP



Proxy ARP

- Router R replies to ARP requests that are generated by hosts on the PPP connection (Network B), in which the target IP is on network A, namely it sends its MAC address.
  - R knows which hosts are connected through the PPP.
- These hosts assume that the destination hosts are on the same physical network.
- In their ARP tables the router MAC address is associated with the destination IP address.
- Advantage of Proxy ARP over other networking schemes is “simplicity” !

Typical uses of Proxy ARP

- Joining a broadcast LAN with serial links (e.g., dialup or VPN connections).
- Taking multiple addresses from a LAN
- On a firewall
- Mobile-IP

ARP Software Modules

ARP software modules

- Cache Table
- Queues
- Output Module
- Input Module
- Cache-Control Module

ARP : Cache Table

- If ARP just resolved an IP address, chances are a few moments later there is a request to resolve the same IP address
- When ARP returns a MAC address, it is placed in a cache. When the next request comes in for the same IP address, look first in the cache

Cache Table content:

- Queue number: which queue the ARP request is sitting in
- Attempts: how many times have you tried to resolve this address?
- Time-out: how long until this address is tossed out (need the room in cache)
- Hardware address: destination hardware address
- Protocol address: destination IP address

Working of the Cache

- The **output module** waits for an IP packet with a request
- Checks the cache for an existing entry
- If entry found and state RESOLVED, we already have this MAC address
- If entry found and state PENDING, packet waits until destination hard address found

Original cache table used for examples

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Example 2

The ARP output module receives an IP datagram (from the IP layer) with the destination address 114.5.7.89. It checks the cache table and finds that an entry exists for this destination with the RESOLVED state (R in the table). It extracts the hardware address, which is 457342ACAE32, and sends the packet and the address to the data link layer for transmission. The cache table remains the same.

Example 3

Twenty seconds later, the ARP output module receives an IP datagram (from the IP layer) with the destination address 116.1.7.22. It checks the cache table and does not find this destination in the table. The module adds an entry to the table with the state PENDING and the Attempt value 1. It creates a new queue for this destination and enqueues the packet. It then sends an ARP request to the data link layer for this destination. The new cache table is shown in the Table.

Updated cache table for Example 3

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Example 4

Fifteen seconds later, the ARP input module receives an ARP packet with target protocol (IP) address 188.11.8.71. The module checks the table and finds this address. It changes the state of the entry to RESOLVED and sets the time-out value to 900. The module then adds the target hardware address (E34573242ACA) to the entry. Now it accesses queue 18 and sends all the packets in this queue, one by one, to the data link layer. The new cache table is shown in Table.

Updated cache table for Example 4

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
P	23	1		116.1.7.22	
R	9		60	19.1.7.82	4573E3242ACA
R	18		900	188.11.8.71	E34573242ACA

Example 5

Twenty-five seconds later, the cache-control module updates every entry. The time-out values for the first three resolved entries are decremented by 60. The time-out value for the last resolved entry is decremented by 25. The state of the next-to-the last entry is changed to FREE because the time-out is zero. For each of the three pending entries, the value of the attempts field is incremented by 1. One entry (IP addr 201.1.56.7 is over max, so change to FREE.

Updated cache table for Example 5

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		840	180.3.6.1	ACAE32457342
P	2	3		129.34.4.8	
F					
R	8		390	114.5.7.89	457342ACAE32
P	12	2		220.55.5.7	
P	23	2		116.1.7.22	
F					
R	18		875	188.11.8.71	E34573242ACA

COMPUTER NETWORKS AND INTERNET PROTOCOLS

ARP – RARP – BOOTP – DHCP (contd.)

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

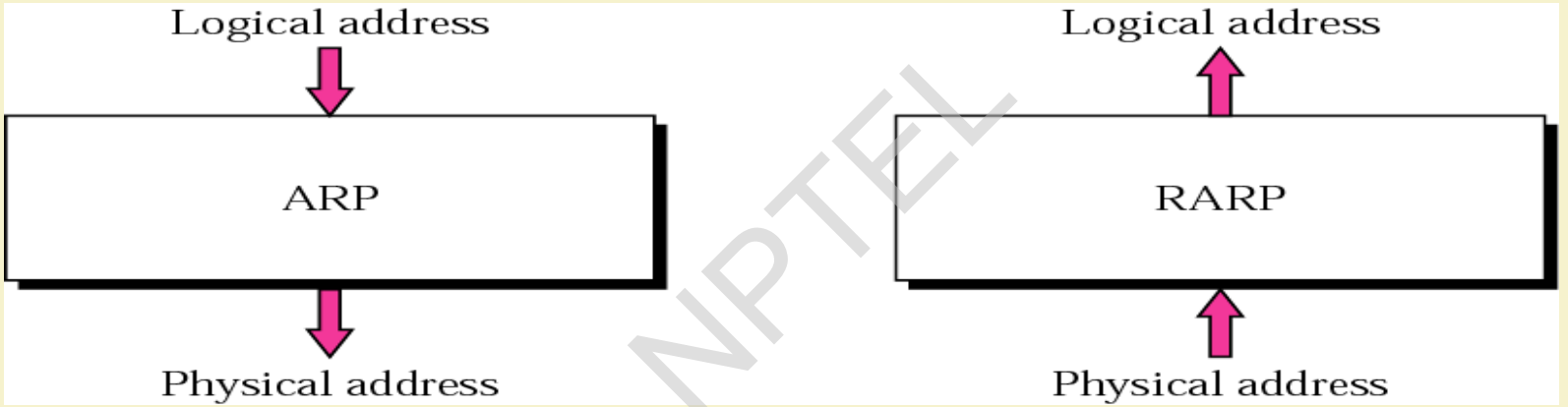
Address Resolution Protocol (ARP)

- Two machines on a given network can communicate only if they know each other's physical network address

- ARP (Address Resolution Protocol) serves for mapping from high-level IP address into low level MAC address.

Ref: Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks

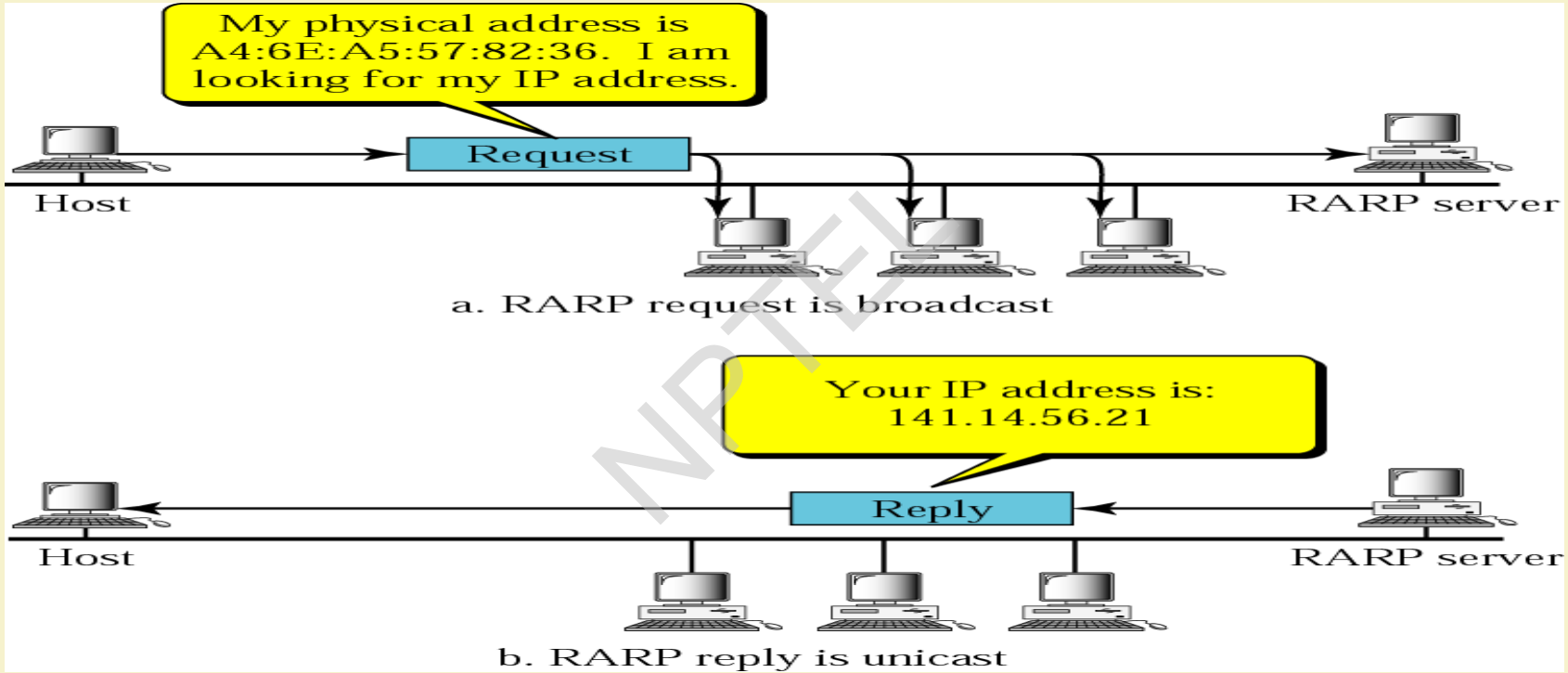
ARP


Logical address
ARP
Physical address
Logical address
RARP
Physical address

RARP

- RARP finds the logical address for a machine that only knows its physical address.
- This if often encountered on thin-client workstations. No disk, so when machine is booted, it needs to know its IP address
- RARP requests are broadcast, RARP replies are unicast.
- If a thin-client workstation needs to know its IP address, it probably also needs to know its subnet mask, router address, DNS address, etc.
- So we need something more than RARP. BOOTP, and now DHCP have replaced RARP.

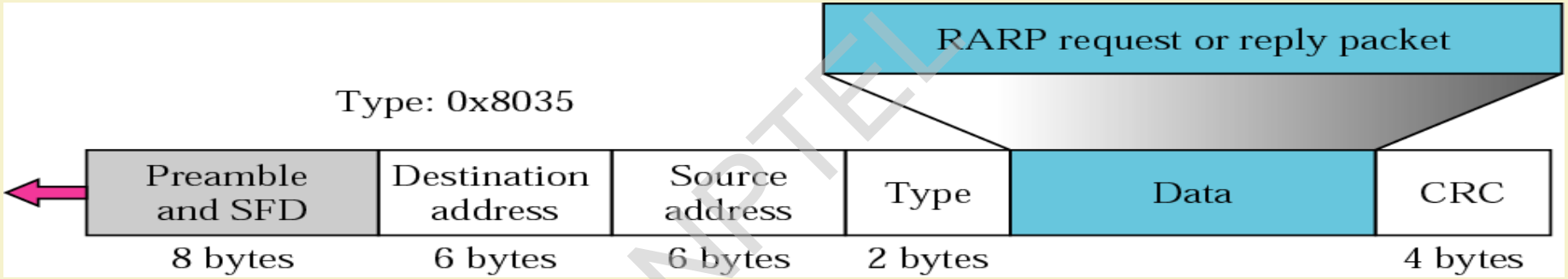
RARP Operation



RARP packet format

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

Encapsulation of RARP packet



BOOTP

BOOTP - Basics

- Bootstrap Protocol allows a host to configure itself dynamically at boot time.
- This protocol provides three services:
  - IP address assignment.
  - Detection of the IP address of a serving machine.
  - The name of a file to be loaded and executed by the client machine.
- *BOOTP packet is assumed to never fragment.*

BOOTP

- BOOTP uses two well-defined port numbers.
  - UDP port number 67 is used for the server.
  - UDP port number 68 is used for the BOOTP client.
- Process:
  - The BOOTP client broadcasts a single packet. called a BOOTREQUEST packet containing the client's MAC address.
  - The client waits for a response from the server. If not received within a specified time interval, the client retransmits the request.
  - The server responds with a BOOTREPLY packet.

BOOTP - Basics

- BOOTP is an alternative to RARP, which operates at the data link layer for LAN only.
- BOOTP, a UDP/IP based configuration protocol, provide much more configuration information.
  - Allows dynamic configuration of the entire IP network.
- BOOTP and its extensions became the basis for the DHCP protocol.

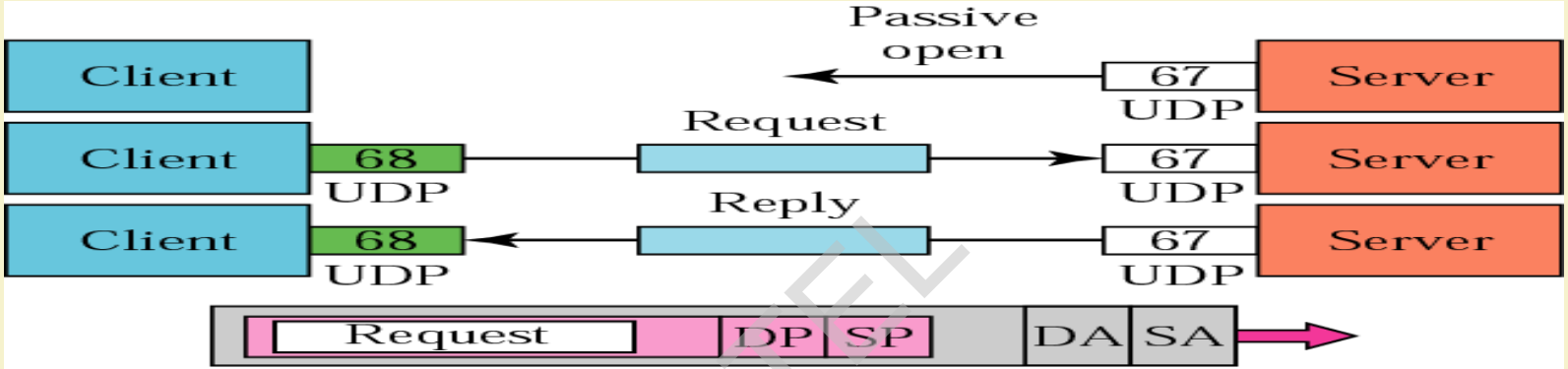
BOOTP Packet Format

Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds		Unused	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot file name (128 bytes)			
Options			

BOOTP

- Operation code (8 bits)
  - Value = 1 ➔ Boot request
  - Value = 2 ➔ Boot reply
- Hardware type (8 bits)
  - Value = 1 ➔ Ethernet
  - Value = 2 ➔ Experimental Ethernet
  - Value = 15 ➔ Frame relay
  - Value = 19 ➔ ATM

BOOTP Operation



SP: Source port (68)
DP: Destination port (67)
SA: Source address (All 0s)
DA: Destination address (All 1s)

SP: Source port (67)
DP: Destination port (68)
SA: Source address (Server unicast address)
DA: Destination address (All 1s or client unicast address)

DHCP

Dynamic Host Control Protocol

DHCP

- Dynamic Host Control Protocol
  - Used to centrally allocate and manage TCP/IP configurations of client nodes.
  - Allows us to define pools of IP addresses, which are then allocated to client computers by the server.
    - These pools of addresses are called “scopes”.
    - Not only are the addresses handed out, so also are the related configuration settings like the subnet mask, default router, DNS server, etc.

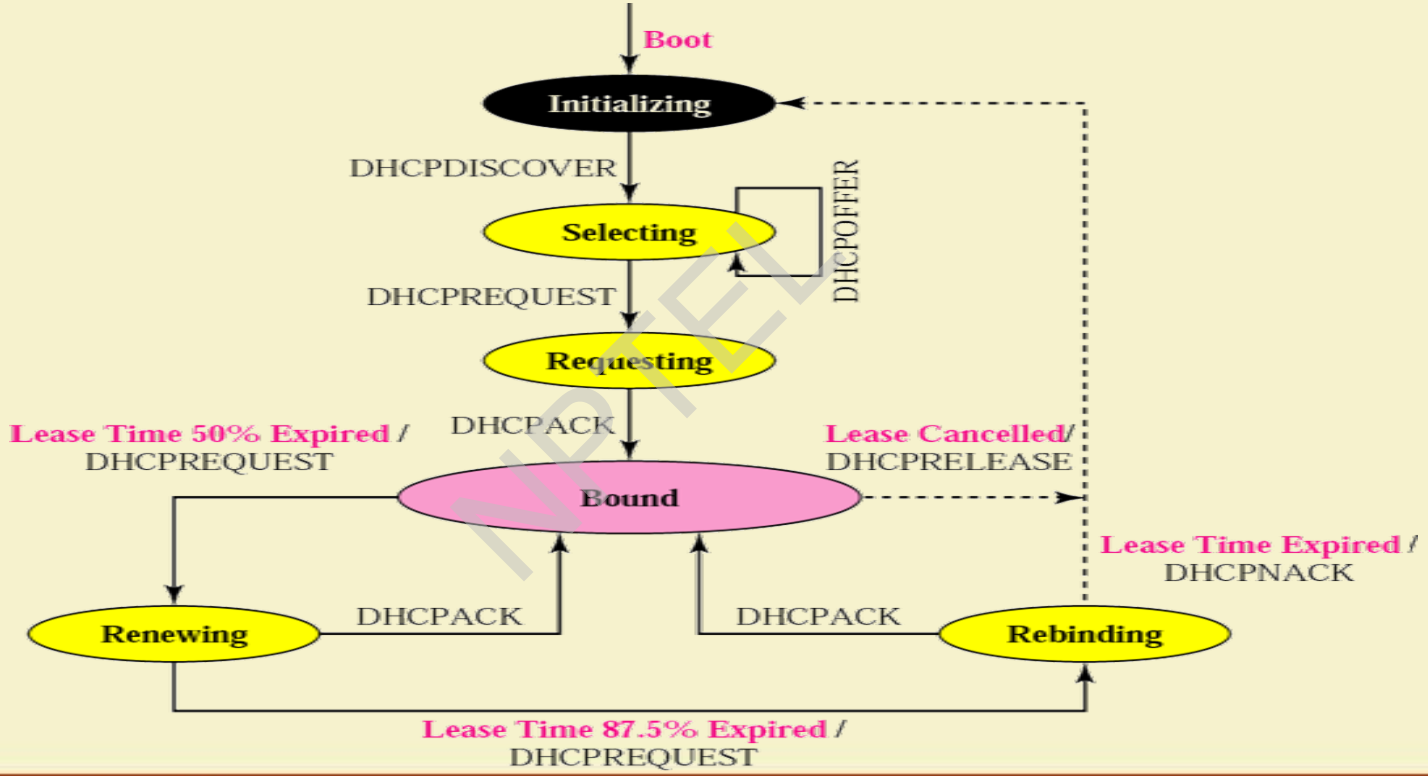
DHCP Working

- DHCP works across most IP routers, and allocates addresses depending on the subnet the request came from.
  - No need to reconfigure a PC that is moved from one subnet to another.
- When a DHCP client is first switched on:
  - It sends a broadcast packet on the network with a DHCP request.
  - This is picked up by the DHCP server.
  - Server allocates an IP address to the PC, from one of the scopes it has.
- DHCP does not allocate addresses permanently:
  - It "leases" the address for a particular time period.
  - Controlled by the administrator.

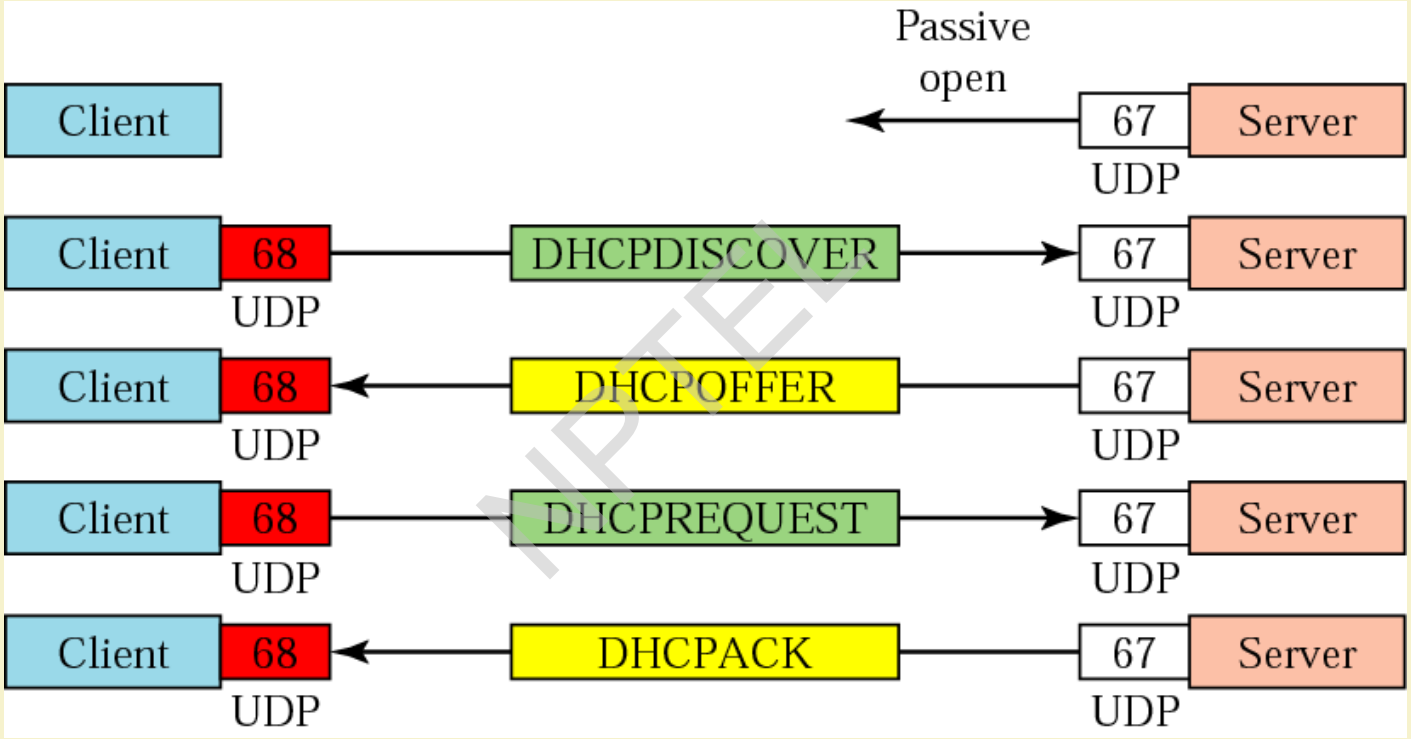
DHCP Packet Format

Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds	F	Unused	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot file name (128 bytes)			
Options (Variable length)			

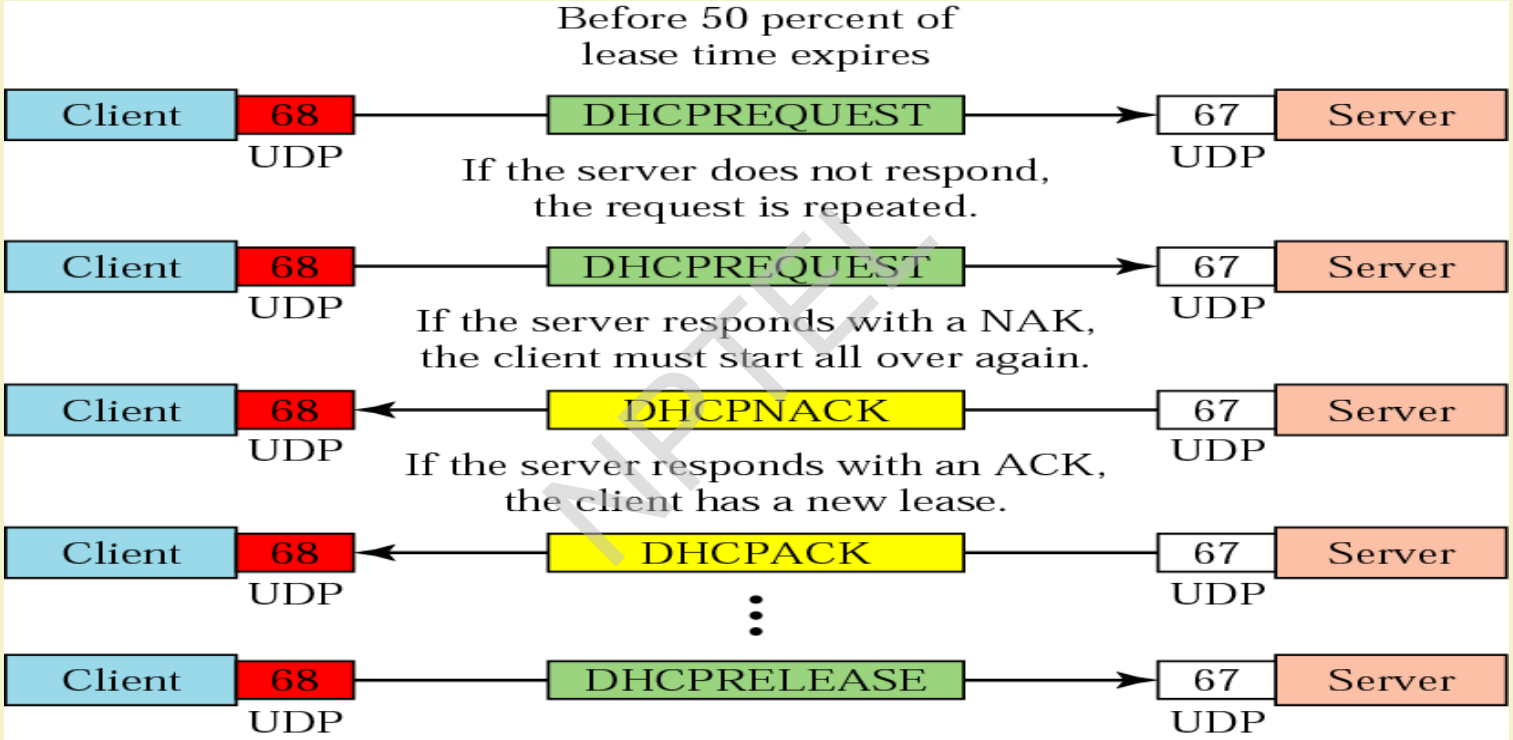
DHCP Operation



DHCP: Exchanging Messages



Exchanging Messages (contd.)



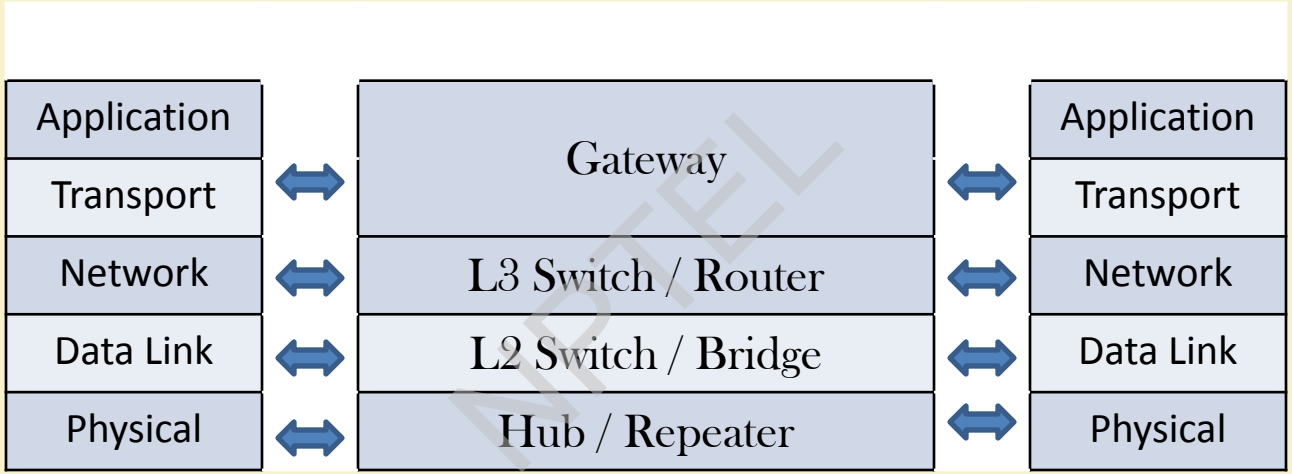
COMPUTER NETWORKS AND INTERNET PROTOCOLS

Connecting LANs, VLAN

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

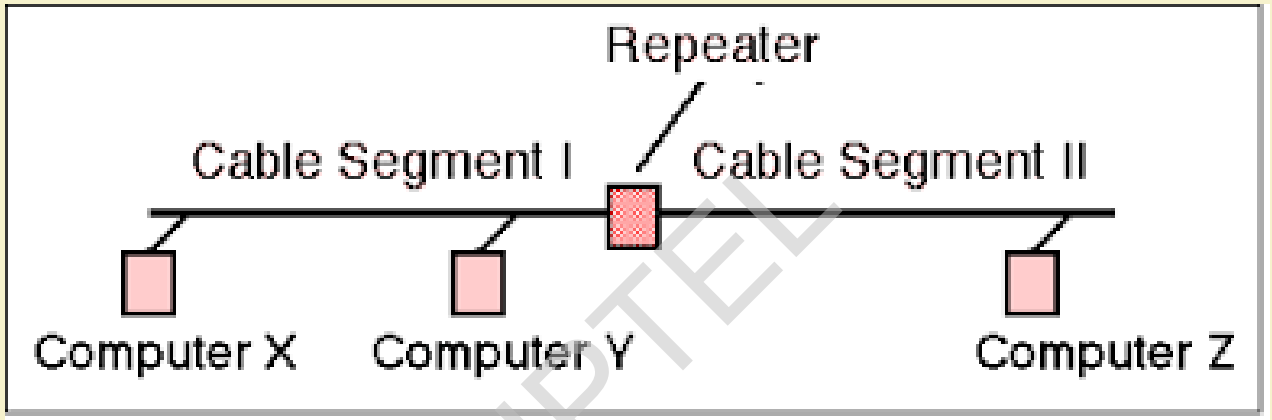
SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

Layer-wise connectivity



Ref: Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com

Repeater / Hub: Connecting two segments of a LAN at Physical level



- Acts as signal regenerator
- No filtering
- Hub is a multi-port Repeater
- Hierarchy of hubs

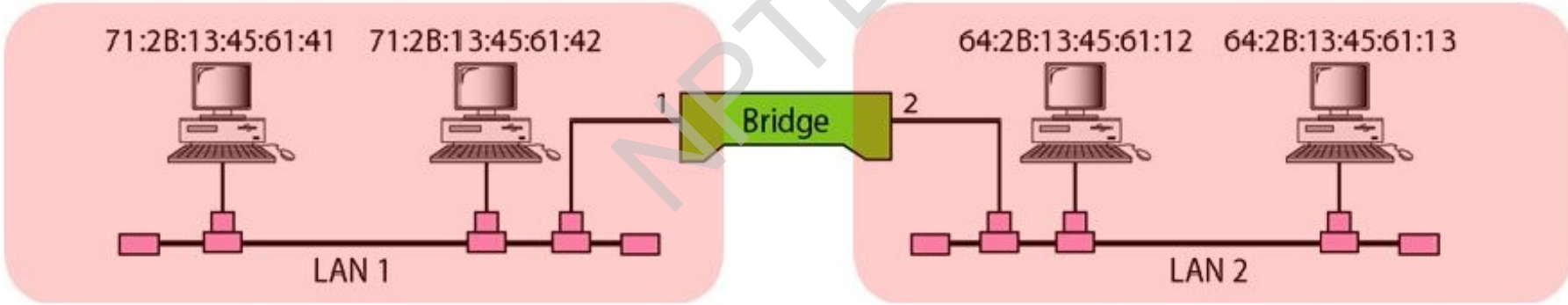
Bridges: Connecting LANs

- Separating collision domains
- MAC address are used for filtering traffic
- Connected segments form a single network – Same broadcast domain

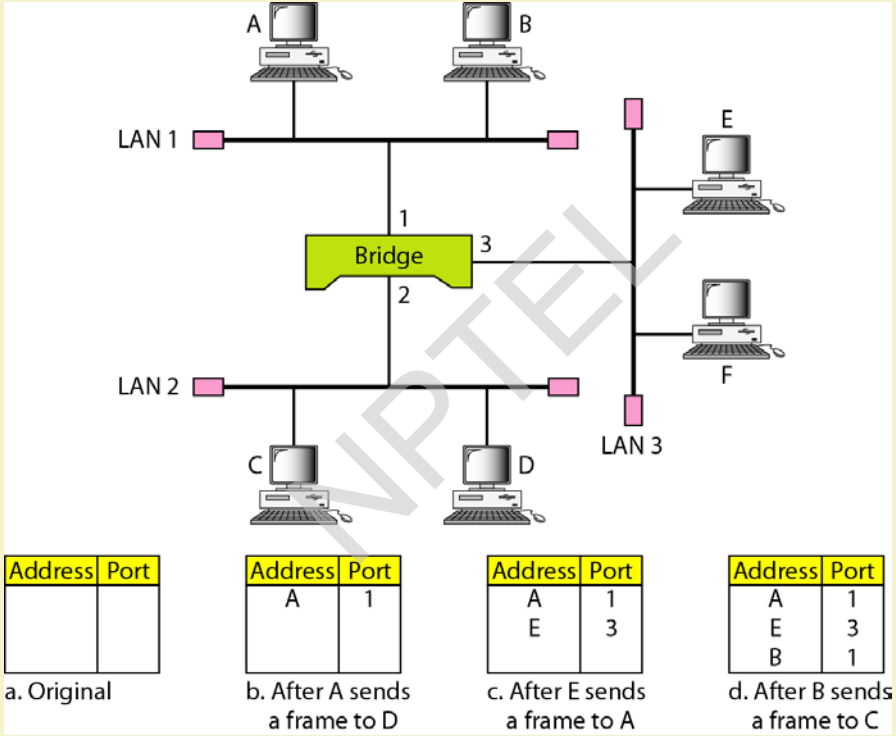
Bridge: Connecting LANs

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table



Bridge Learning / Bridge Table



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

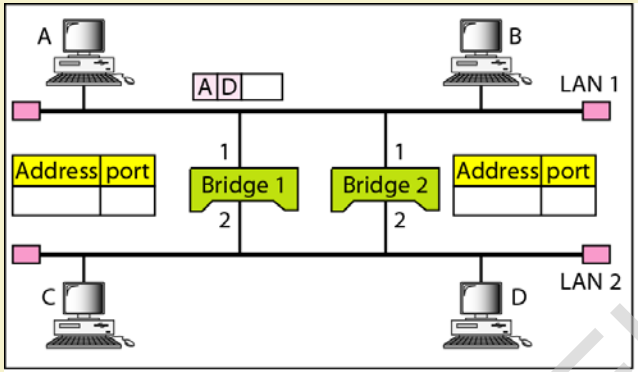
Address	Port
A	1
E	3

c. After E sends a frame to A

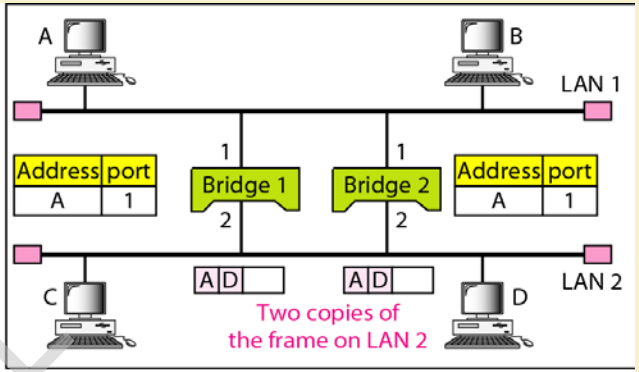
Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

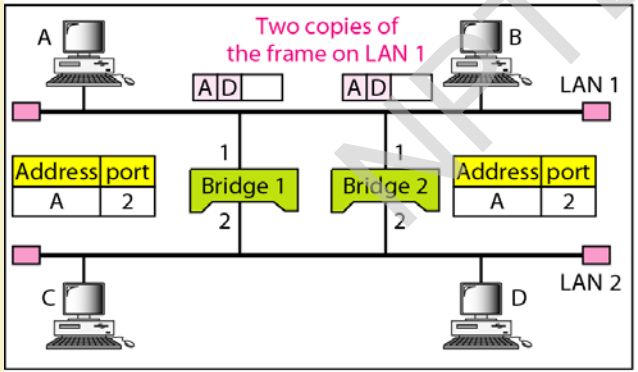
Bridge:
Loop problem



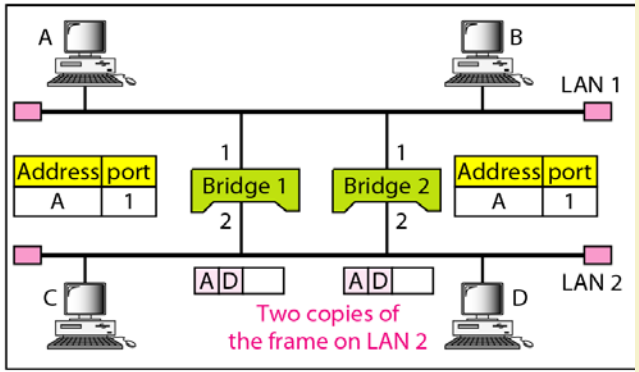
a. Station A sends a frame to station D



b. Both bridges forward the frame

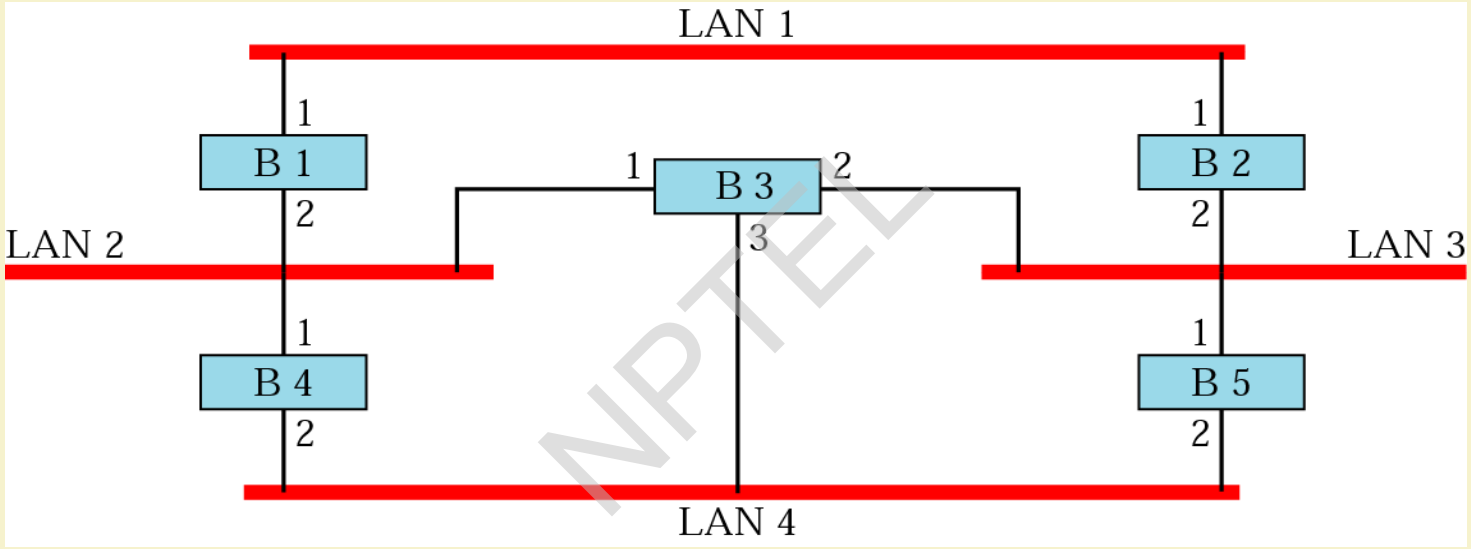


c. Both bridges forward the frame



d. Both bridges forward the frame

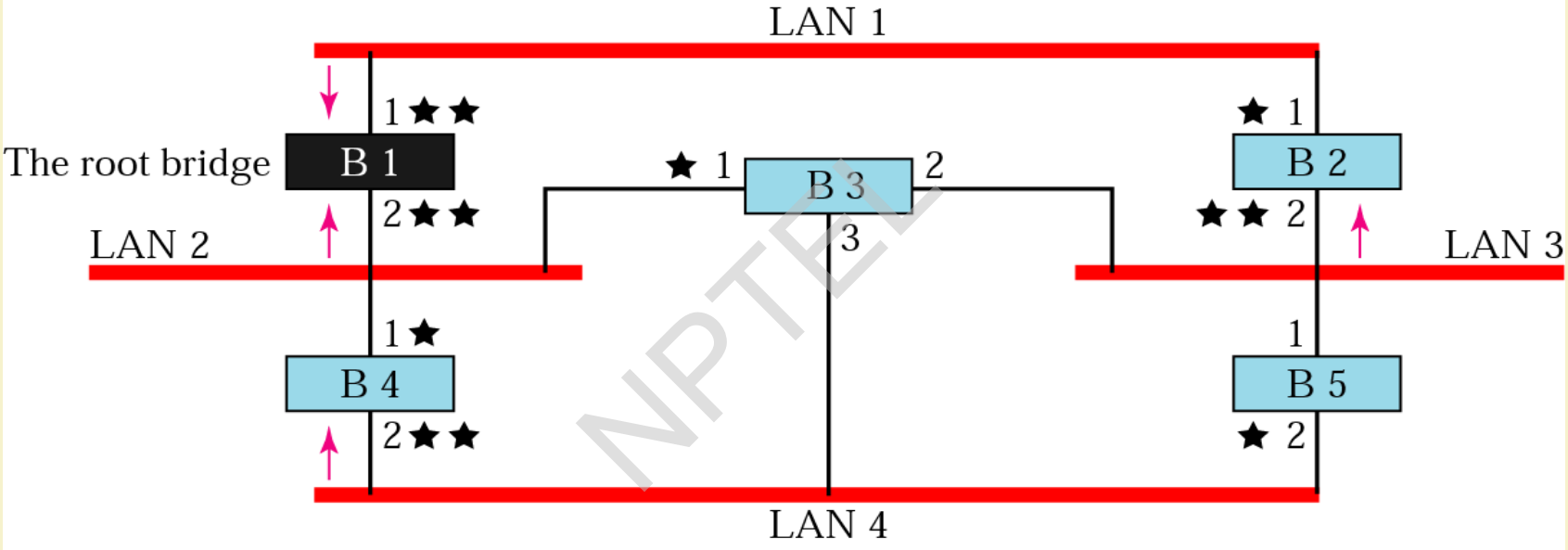
Handling Loop problem in Transparent Bridge: Spanning Tree Protocol (STP)



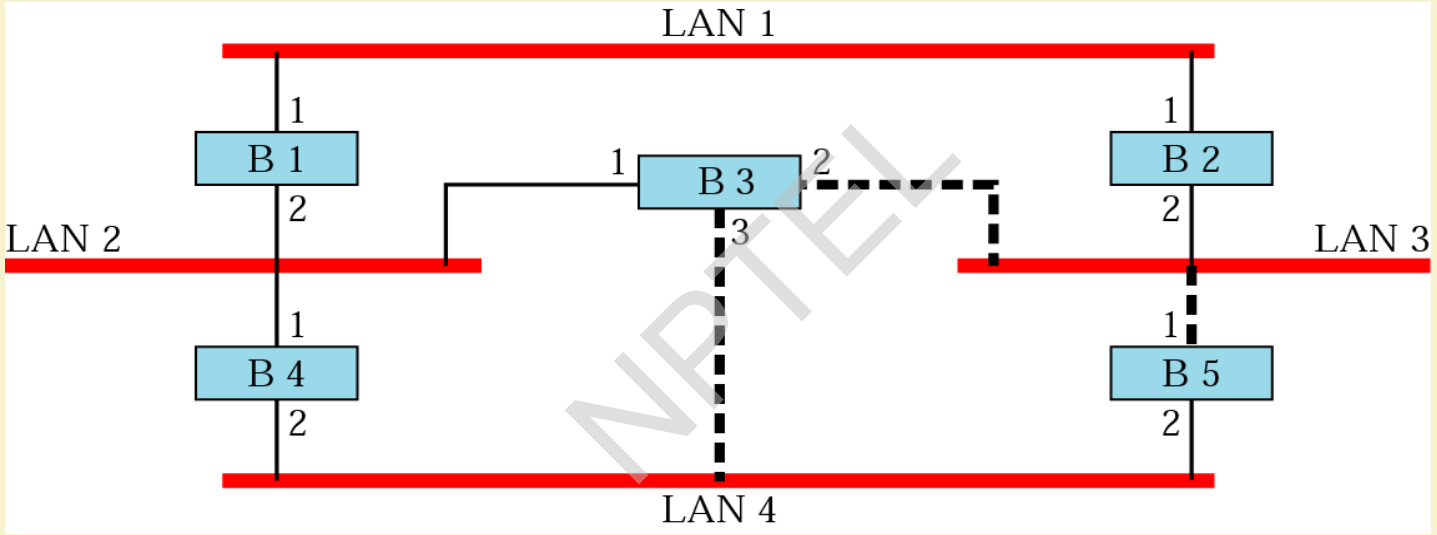
Applying STP for Loop avoidance

1. Every bridge has an *unique ID*. Select the bridge with smallest ID. This is the ***root bridge***.
2. Mark one port of each bridge (except root bridge) as the ***root port***. Root port is the port with least-cost path from the bridge to the root bridge (marked with 1 star).
3. For each LAN, choose a ***designated bridge***. A designated bridge has the least-cost path between the LAN and root bridge (the arrows). Mark the corresponding port that connects the LAN to its designated bridge the *designated port* (two stars).
4. Mark the root port and designated port as ***forwarding ports***, the others as ***blocking ports*** (every port with 1 or 2 stars keep, ports with no stars drop).
5. *There is only one path between any two bridges*.

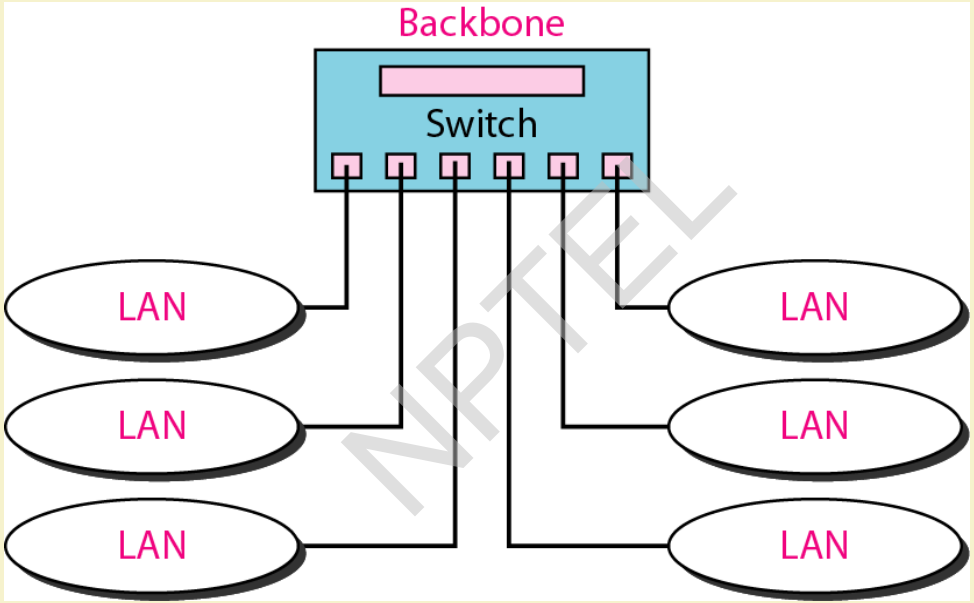
Applying STP



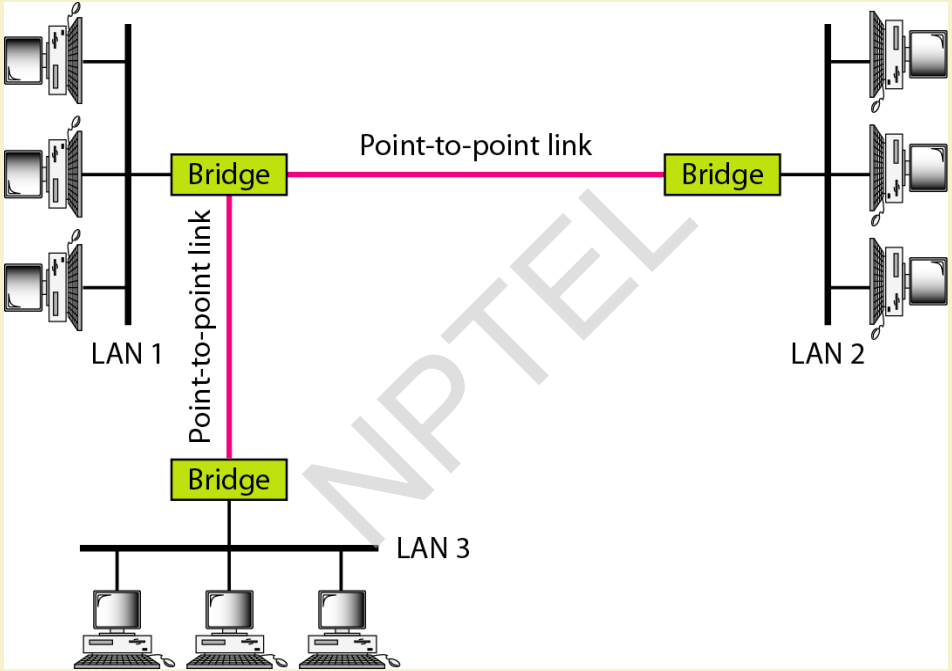
Bridged Network: Forwarding ports and Blocking ports



Backbone Network : *Star backbone*

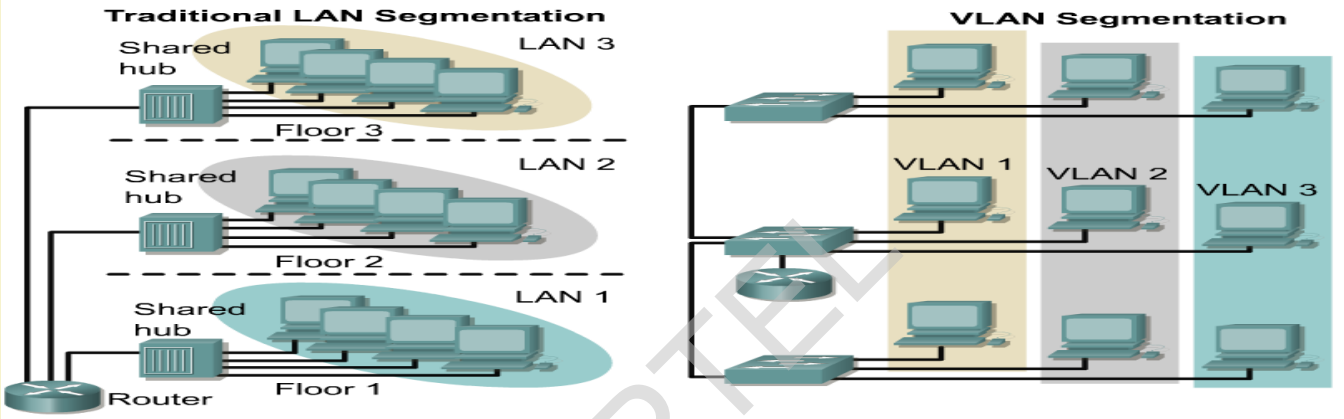


Connecting LANs with bridges



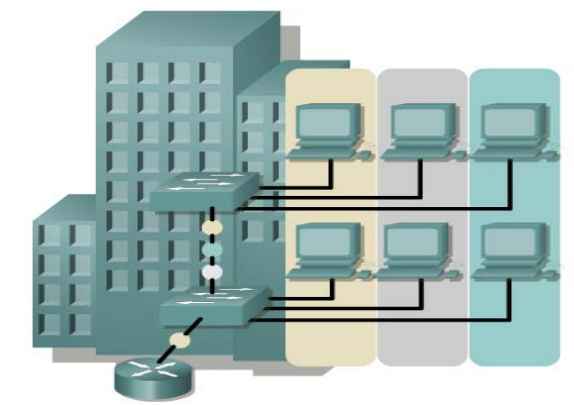
VIRTUAL LANs (VLAN)

VLAN basics



- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

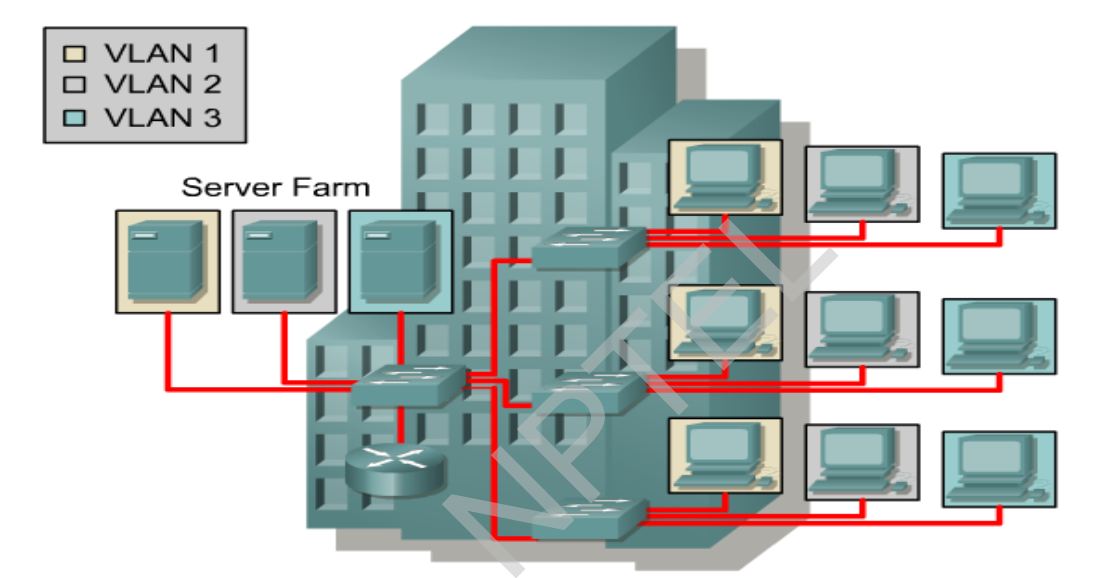
VLAN basics



- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

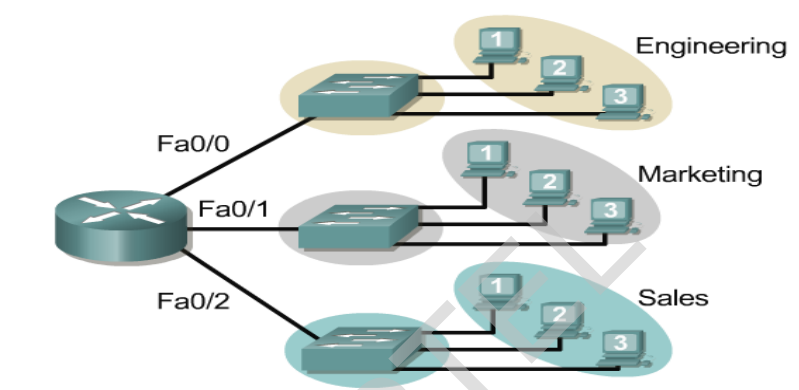
Broadcast domains with VLANs and Routers



- A VLAN is a broadcast domain created by one or more switches.
- The network design above creates three separate broadcast domains.

Broadcast domains with VLANs and routers

1) Without VLANs



10.1.0.0/16

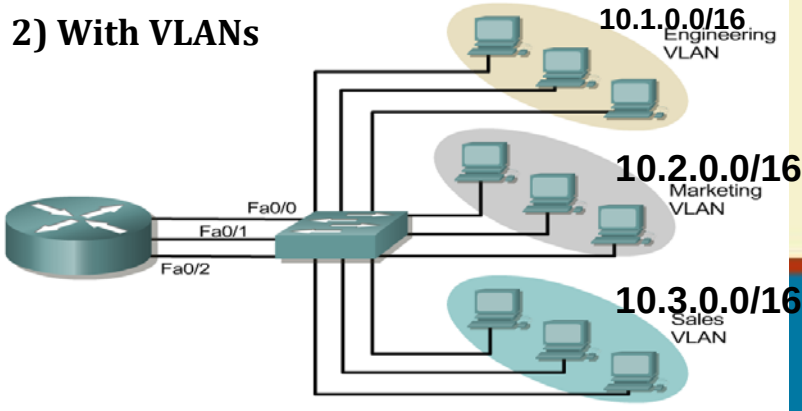
10.2.0.0/16

10.3.0.0/16

- Without VLANs, each group is on a different IP network and on a different switch.
- Using VLANs, Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch.
- What are the broadcast domains in each?

One link per VLAN or a single VLAN Trunk

2) With VLANs

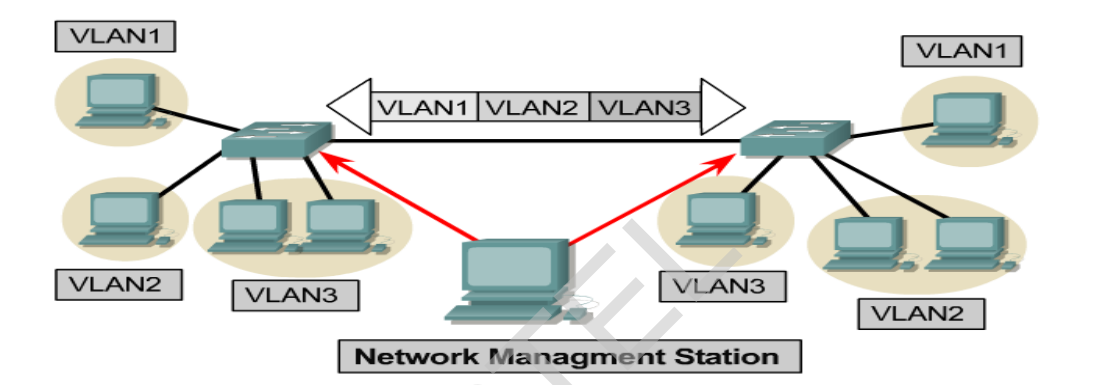


VLAN operation

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

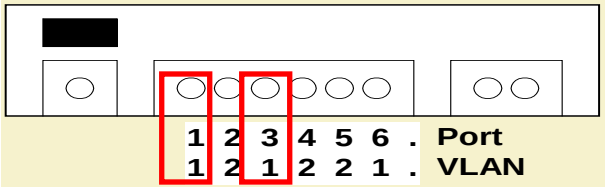
- Each switch port can be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

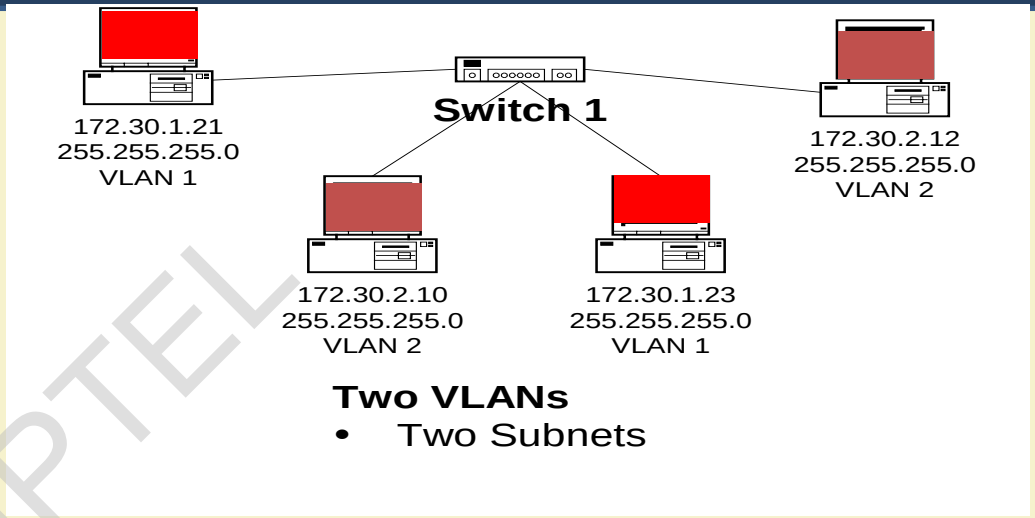
VLAN operation



- **Static membership VLANs are called port-based and port-centric membership VLANs.**
- As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached.
- "The ***default VLAN*** for every port in the switch is the management VLAN. The management VLAN is always VLAN 1 *and may not be deleted."*
- All other ports on the switch may be reassigned to alternate VLANs.
- More on VLAN 1 later.

VLAN operation

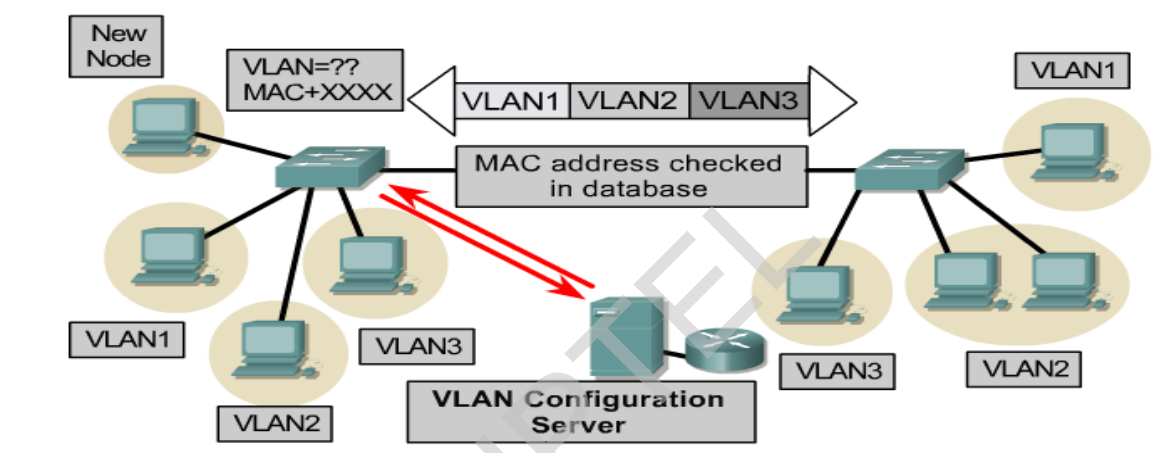




Important points on VLANs:

- VLANs are assigned on the switch port. There is no "VLAN" assignment done on the host (usually).
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
  - VLAN => Subnet
- Assigning a host to the correct VLAN is a 2-step process:
  - Connect the host to the correct port on the switch.
  - Assign to the host the correct IP address depending on the VLAN membership

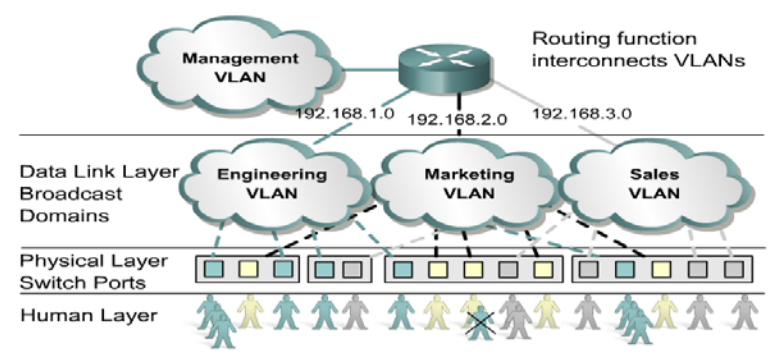
VLAN operation



- *Dynamic membership VLANs are created through network management software.*
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network, it queries a database within the switch for a VLAN membership.

Benefits of VLANs

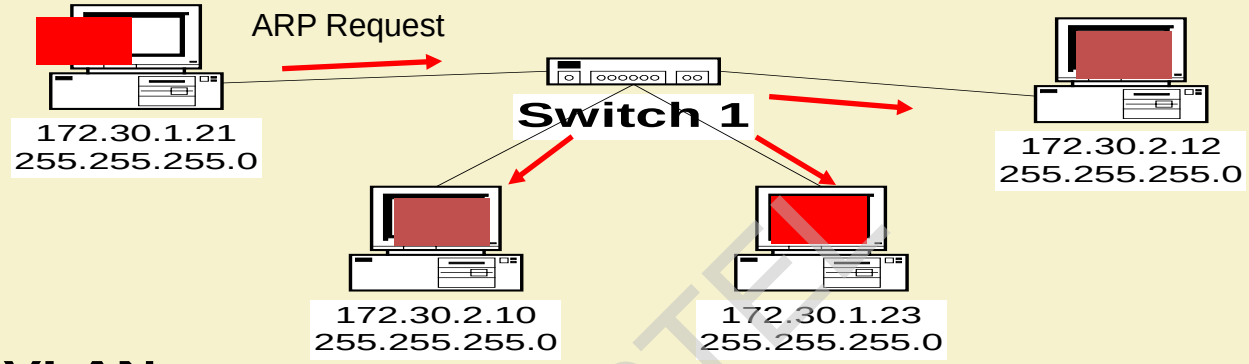
All systems attached to the same port must be in the same VLAN



If a hub is connected to VLAN port on a switch, all devices on that hub must belong to the same VLAN.

- Key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.
- Helps an administrator:
  - Easily move workstations on the LAN.
  - Easily add workstations to the LAN.
  - Easily change the LAN configuration.
  - Easily control network traffic.
  - Improve security.

Without VLANs – *No Broadcast Control*

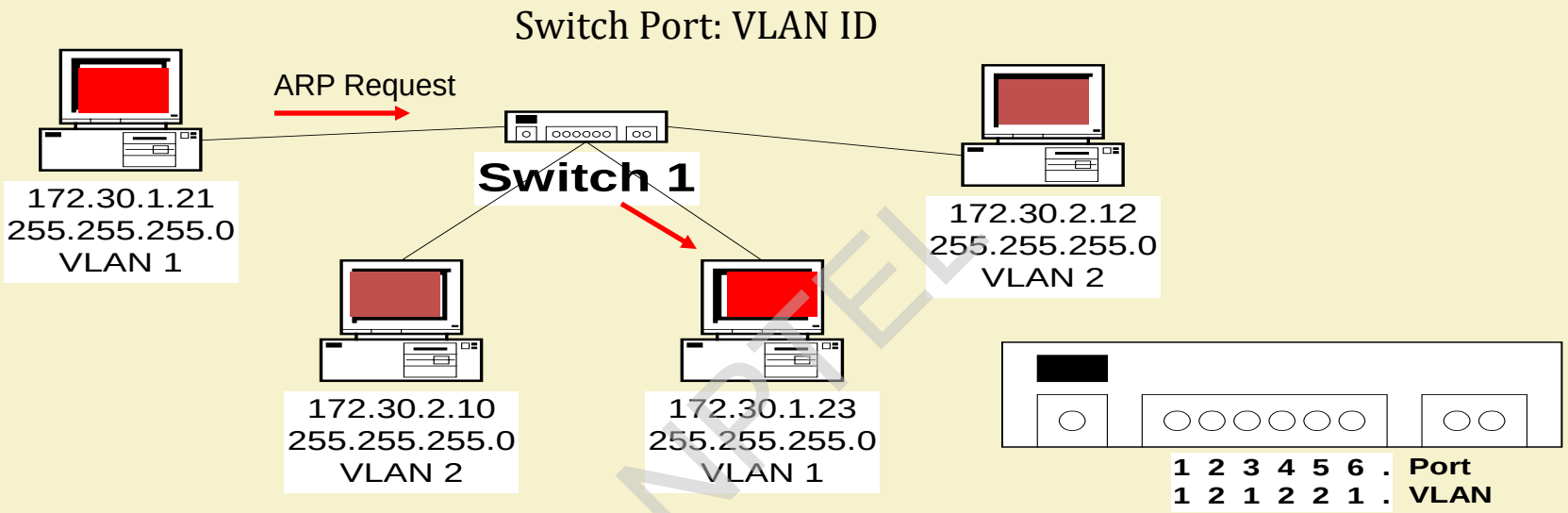


No VLANs

- Same as a single VLAN
- Two Subnets

- Without VLANs, the ARP Request would be seen by all hosts.
- Again, consuming unnecessary network bandwidth and host processing cycles.

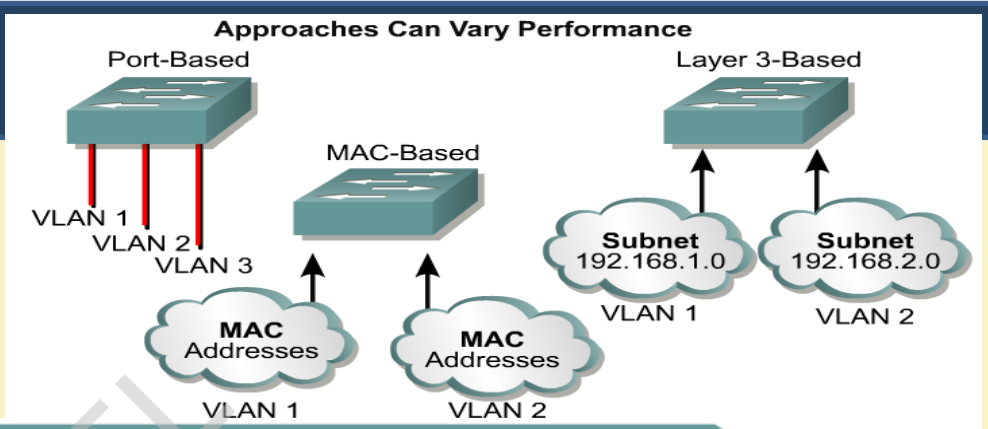
With VLANs – Broadcast Control



Two VLANs

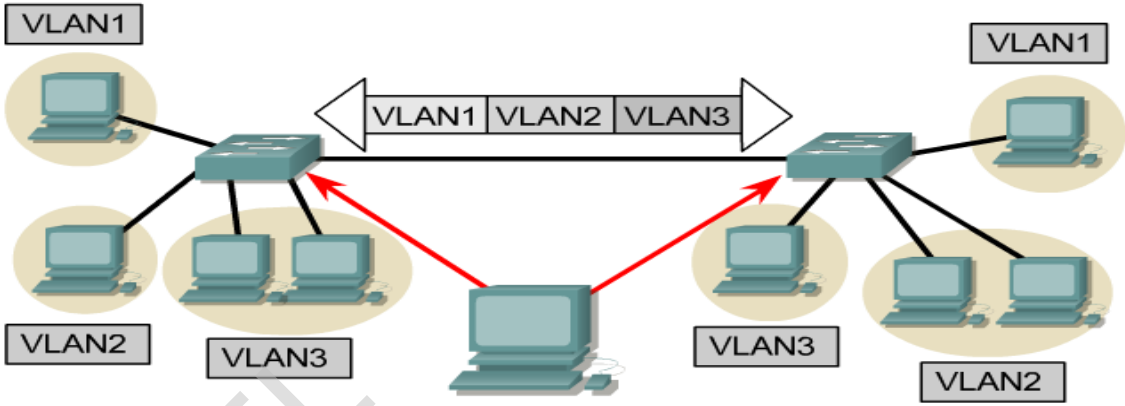
- Two Subnets

VLAN Types



VLAN Types	Description
Port-based	• Most common configuration method. • Ports assigned individually, in groups, in rows, or across 2 or more switches. • Simple to use. • Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts.
MAC address	• Rarely implemented today. • Each address must be entered into the switch and configured individually. • Users find it useful. • Difficult to administer, troubleshoot and manage.
Protocol Based	• Configured like MAC addresses, but instead uses a logical or IP address. • No longer common because of DHCP.

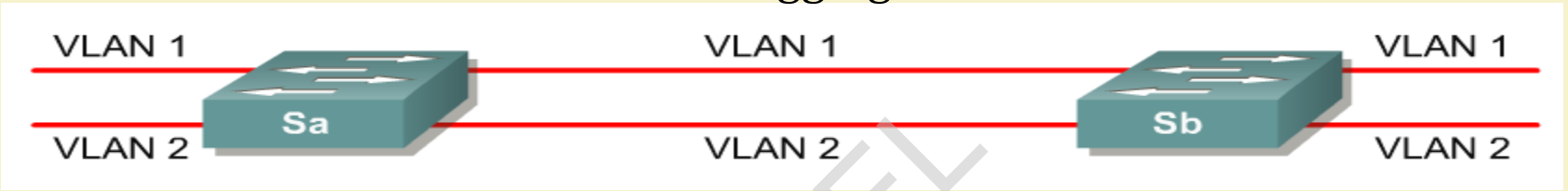
VLAN Tagging



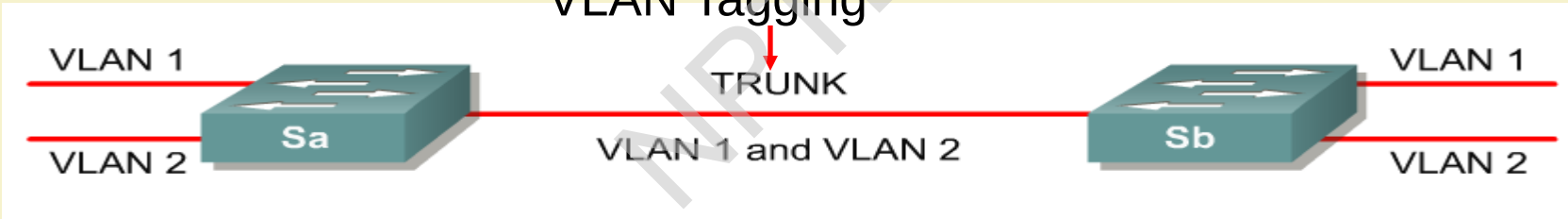
- VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.
  - ***Trunk link*:** As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- *This header information designates the VLAN membership of each packet.*
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the destination node (Switch) the VLAN ID is removed from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a ***trunk link*** or ***VLAN trunking***.

VLAN Tagging

No VLAN Tagging



VLAN Tagging

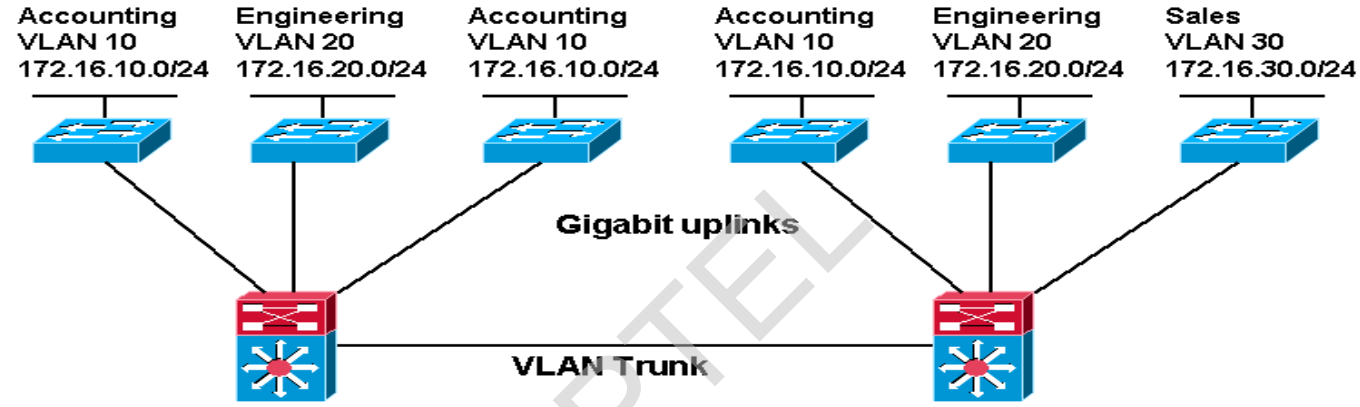


- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN

VLANs Types

- End-to-End or Campus-wide VLANs
- Geographic or Local VLANs

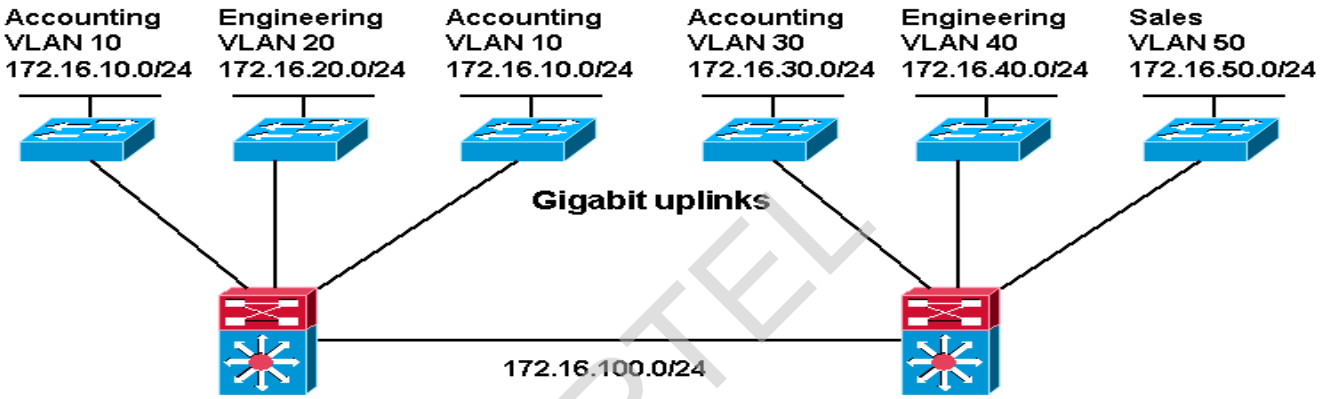
End-to-End or Campus-wide VLANs



Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

Geographic or Local VLANs



Local or Geographic VLAN Model

- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

COMPUTER NETWORKS AND INTERNET PROTOCOLS

Wireless LANs

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

Wireless Local Area Networks (WLANs)

- Proliferation of mobile devices (laptop, PDAs and mobile phones) created an *obvious* application level demand for wireless local area networking.
- Standardization by *IEEE 802 committee*

Ref: Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com; Worcester Polytechnic Institute (WPI), Worcester, MA, USA

IEEE 802 Standards Working Groups

- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence Working Group
- 802.21 Media Independent Handover Services Working Group
- 802.22 Wireless Regional Area Networks
- 802.24 Vertical Applications TAG

IEEE 802.11 Standards

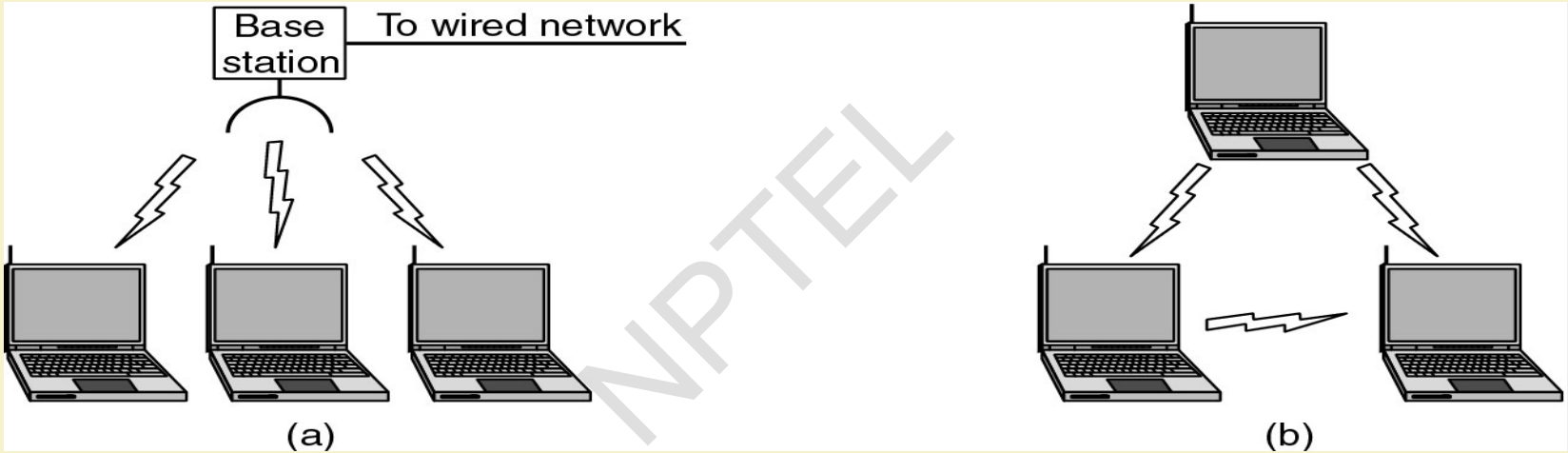
802.11a - Wireless network bearer operating in the 5 GHz ISM band with data rate up to 54 Mbps. ***802.11b*** - Wireless network bearer operating in the 2.4 GHz ISM band with data rates up to 11 Mbps.
802.11e - Quality of service and prioritization
802.11f - Handover
802.11g - Wireless network bearer operating in 2.4 GHz ISM band with data rates up to 54 Mbps.
802.11h - Power control
802.11i - Authentication and encryption
802.11j - Interworking
802.11k - Measurement reporting
802.11n - Wireless network bearer operating in the 2.4 and 5 GHz ISM bands with data rates up to 600 Mbps.
802.11s - Mesh networking
802.11ac - Wireless network bearer operating below 6GHz to provide data rates of at least 1Gbps per second for multi-station operation and 500 Mbps on a single link.
802.11ad - Wireless network bearer providing very high throughput at frequencies up to 60GHz.
802.11af - Wi-Fi in TV spectrum white spaces (often called White-Fi).
802.11ah - Wi-Fi using unlicensed spectrum below 1 GHz to provide long range communications and support for the Internet of Everything.

Of these the standards that are most widely known are the network bearer standards, 802.11a, 802.11b, 802.11g and now 802.11n.

Categories of Wireless Networks

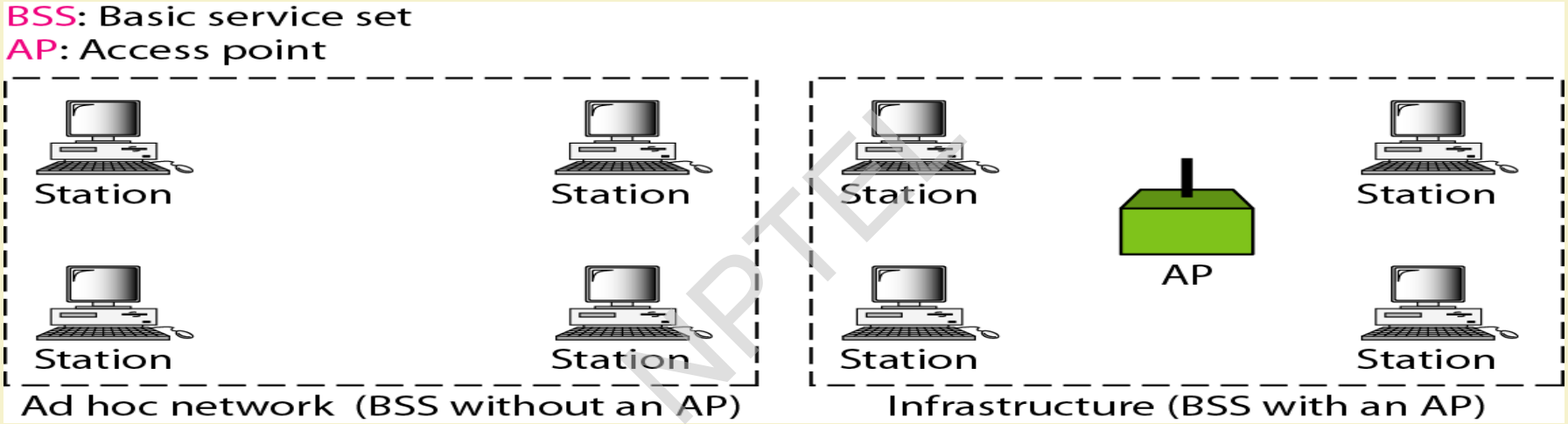
- ***Base Station*** : All communication through an ***access point.*** Other nodes can be fixed or mobile.
- ***Infrastructure Wireless*** : base station network is connected to the wired Internet.
- ***Ad hoc Wireless*** : Wireless nodes communicate directly with one another.
- ***MANETs*** (Mobile Ad Hoc Networks): Ad hoc nodes are mobile.

Wireless LANs

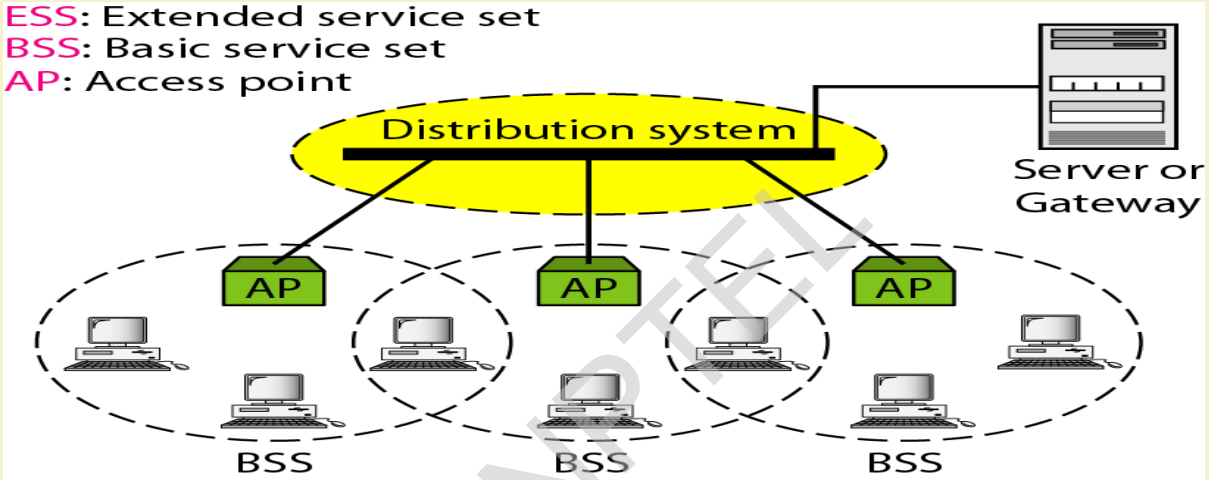


(a) Wireless networking with a base station. (b) Ad hoc networking.

IEEE 802.11



IEEE 802.11



Station Types:

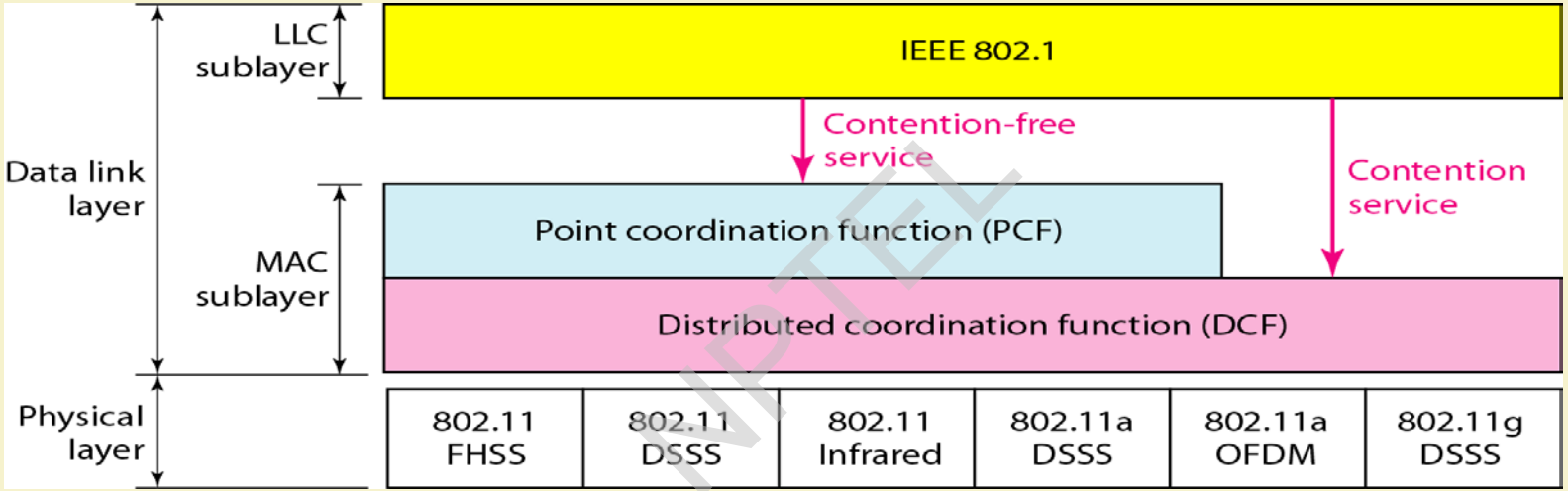
No-Transition : Stationary, moving inside BSS only

BSS-Transition : Movement - one BSS to another BSS inside one ESS

ESS-Transition : Can move from one ESS to another

IEEE 802.11 does not guarantee that communication is continuous during the move

802.11 Stack: DLL and PHY Layers



Wireless Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DHSS
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11 *Infrared***
  - Two capacities 1 Mbps or 2 Mbps.
  - Range is 10 to 20 meters and cannot penetrate walls.
  - Does not work outdoors.
- **802.11 *FHSS* (*Frequency Hopping Spread Spectrum*)**
  - Multipath fading.
  - 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - Same pseudo-random number generator used by all stations.
  - Dwell time: min. time on channel before hopping (400msec).

Wireless Physical Layer

- **802.11 *DSSS* (*Direct Sequence Spread Spectrum*)**
  - Spreads signal over entire spectrum using pseudo-random sequence
  - Each bit transmitted using an 11 chips Barker sequence, PSK at 1Mbaud.
  - 1 or 2 Mbps.
- **802.11a *OFDM* (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - 54Mbps in wider 5.5 GHz band ➔ transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54Mbps 216 data bits encoded into into 288-bit symbols.
  - More difficulty penetrating walls.

Wireless Physical Layer

- **802.11b *HR-DSSS* (*High Rate Direct Sequence Spread Spectrum*)**
  - Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
  - Note in this bandwidth all these protocols have to deal with interference from several home appliances (e.g., microwave ovens, cordless phones etc.)
  - *11b* Range is 7 times greater than *11a.*
  - *11b and 11a are incompatible!!*

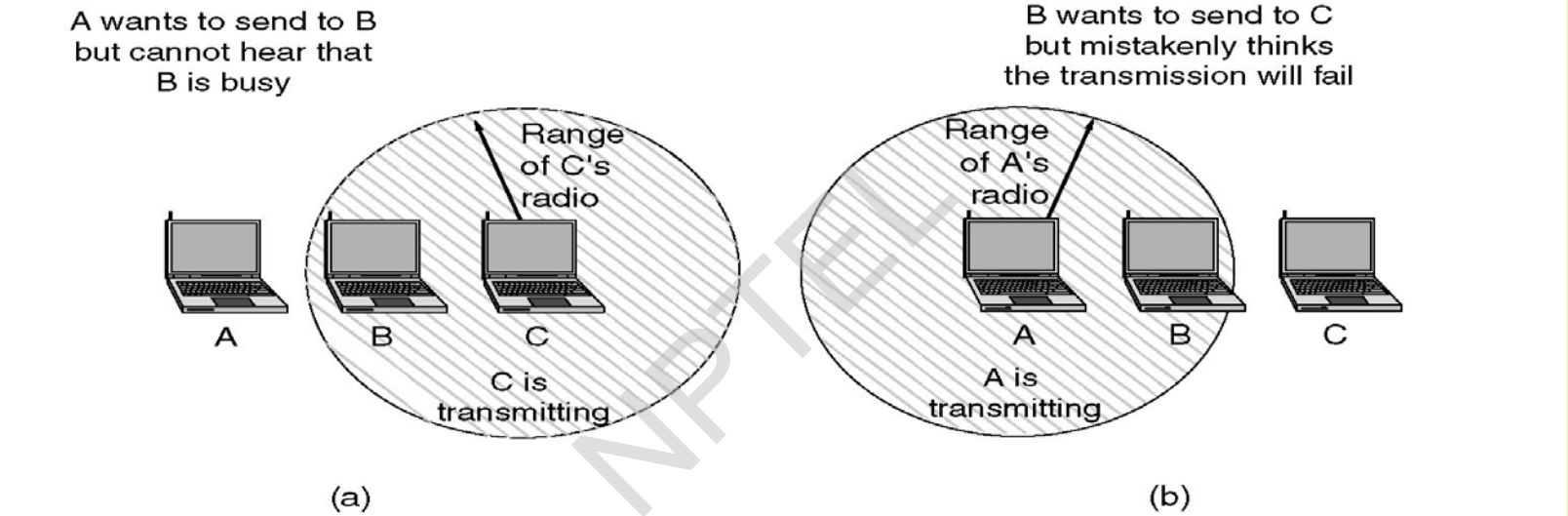
Wireless Physical Layer

- **802.11g *OFDM*(*Orthogonal Frequency Division Multiplexing*)**
  - *An attempt to combine the best of both 802.11a and 802.11b.*
  - Supports bandwidths up to 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.
  - Is backward compatible with 802.11b.

802.11 MAC Sublayer Protocol

- In 802.11 wireless LANs, “seizing channel” does not exist as in 802.3 wired Ethernet.
- Two additional problems:
  - Hidden Terminal Problem
  - Exposed Station Problem
- To deal with these two problems 802.11 supports two modes of operation **DCF (Distributed Coordination Function)** and **PCF (Point Coordination Function).**
- *All implementations must support DCF, but PCF is optional.*

Hidden Station and Exposed Station Problems



(a) Hidden station problem. (b) Exposed station problem.

Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A "*senses*" the channel, it will not hear C's transmission and falsely conclude that A can begin a transmission to B.

Exposed Station Problem

- Inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A's transmission, B falsely assumes that it cannot send to C.

Distribute Coordination Function (DCF)

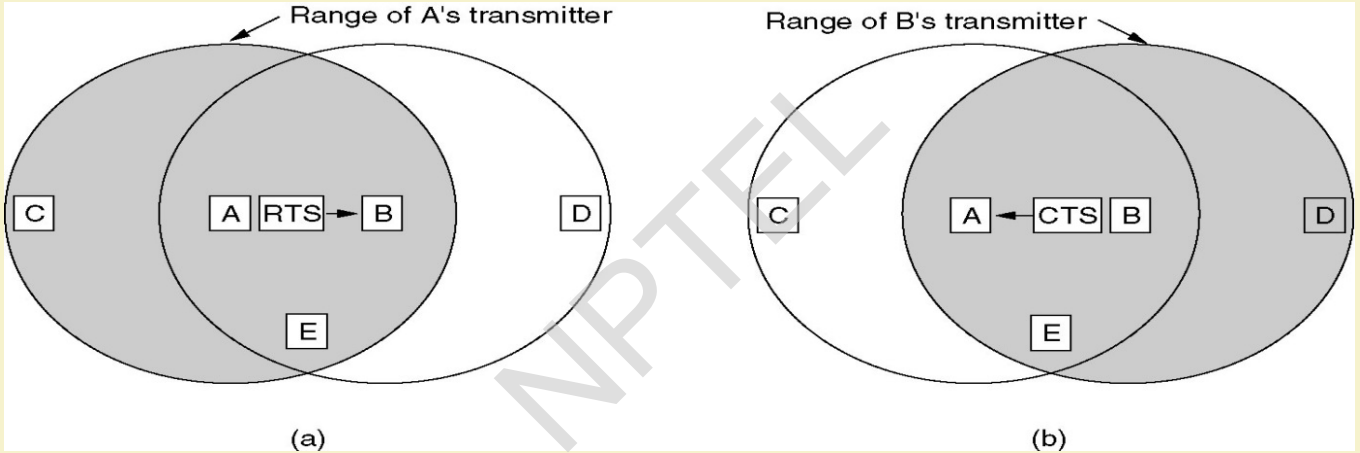
- Uses CSMA/ CA (CSMA with Collision Avoidance).
  - Uses both physical and *virtual* carrier sensing.
  - Two methods are supported:
    1. Based on *MACA*(Multiple Access with Collision Avoidance for Wireless) with virtual carrier sensing.
    2. 1-persistent physical carrier sensing.

Wireless LAN Protocols

- MACA protocol solved hidden, exposed terminal:
  - Send Ready-to-Send (*RTS*) and Clear-to-Send (*CTS*) first
  - RTS, CTS helps determine who else is in range or busy (Collision Avoidance).
  - Can a collision still occur?

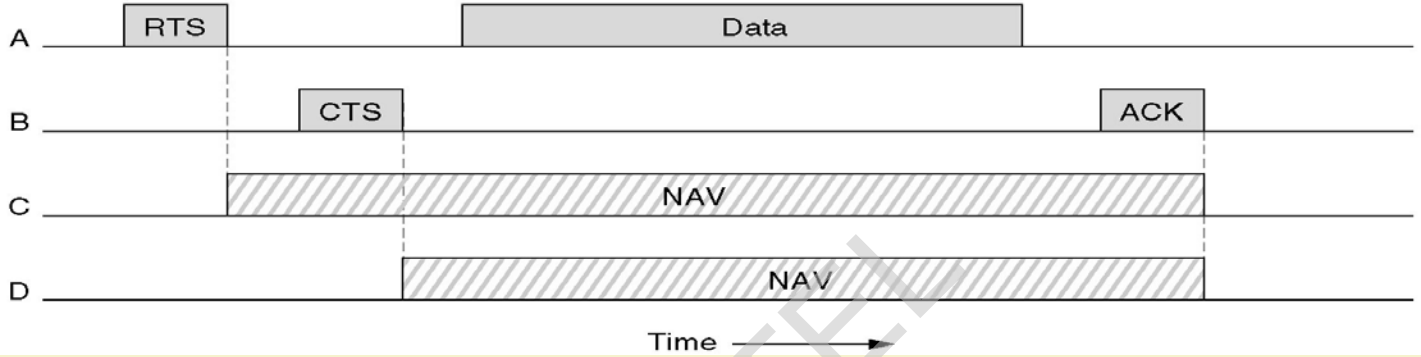
Wireless LAN Protocols

- MACA for WLAN added ACKs and CSMA (no RTS at same time)



(a) A sending an RTS to B (b) B responding with a CTS to A.

(Virtual) **Channel Sensing in CSMA/CA**



Virtual channel sensing using CSMA/CA.

- C (in range of A) *receives the RTS and based on information in RTS creates a virtual channel busy* NAV(Network Allocation Vector).
- Network Allocation Vector (NAV): Time period set by all other waiting stations before sensing the medium for idleness
- D (in range of B) *receives the CTS and creates a shorter* NAV.
- "virtual" implies source station sets *duration field* in data frame or in RTS and CTS frames.
- Stations then adjust their NAV accordingly!

1-Persistent Physical Carrier Sensing

- Station *senses* the channel when it wants to send.
- If idle, station transmits.
  - *Station does not sense channel while transmitting.*
- If the channel is busy, station defers until idle and then transmits.
- Upon collision, wait a *random time* using binary exponential backoff.

Point Coordinated Function (PCF)

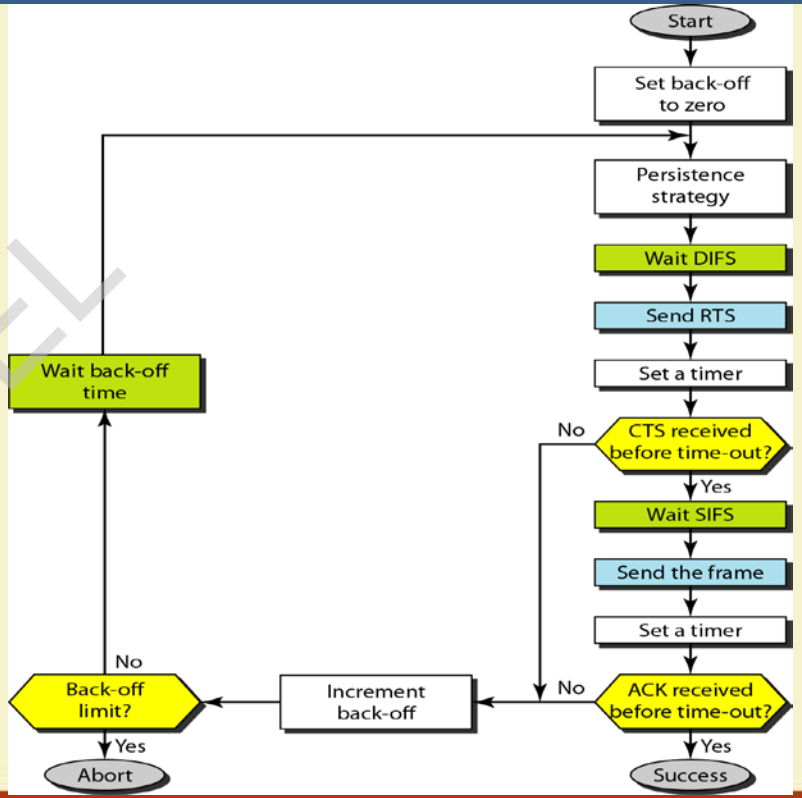
- PCF uses a base station to poll other stations to see if they have frames to send.
- No collisions occur.
- Base station sends ***beacon frame*** periodically.
- Base station can tell another station to ***sleep*** to save on batteries and base stations holds frames for sleeping station.

DCF and PCF Co-Existence

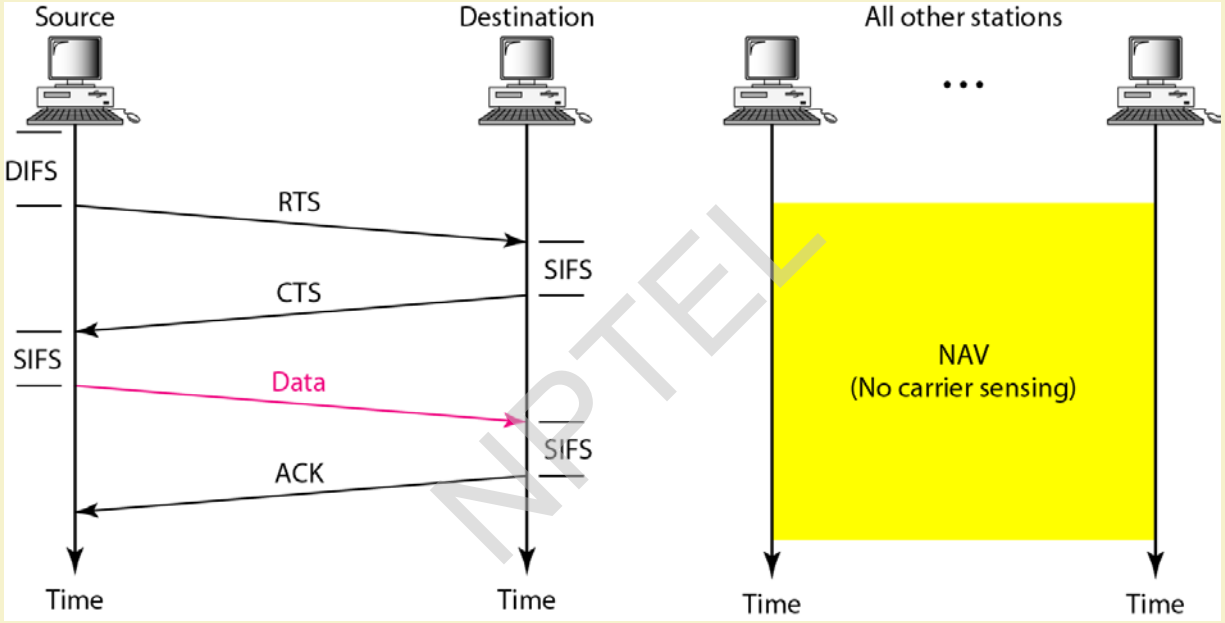
- Distributed and centralized control can co-exist using Inter-Frame Spacing.
- SIFS (Short IFS) : is the time waited between packets in an ongoing dialog (RTS, CTS, data, ACK, next frame)
- PIFS (PCF IFS) : when no SIFS response, base station can issue beacon or poll.
- DIFS (DCF IFS) : when no PIFS, any station can attempt to acquire the channel.
- EIFS (Extended IFS) : lowest priority interval used to report bad or unknown frame.

CSMA/CA

- Uses CSMA/CA as access method, WLANs cannot implement CSMA/CD
  - Collision detection requires send data and receive signals at the same time; requires resourceful stations and higher bandwidth
  - Hidden and Expose station problem
  - Fading problem
- DIFS: Distributed InterFrame Space
- RTS: Request to Send; a control frame
- SIF: Short InterFrame space
- CTS: Clear to Send



CSMA/CA and NAV



Network Allocation Vector (*NAV): Time period set by all other waiting stations before sensing the medium for idleness*