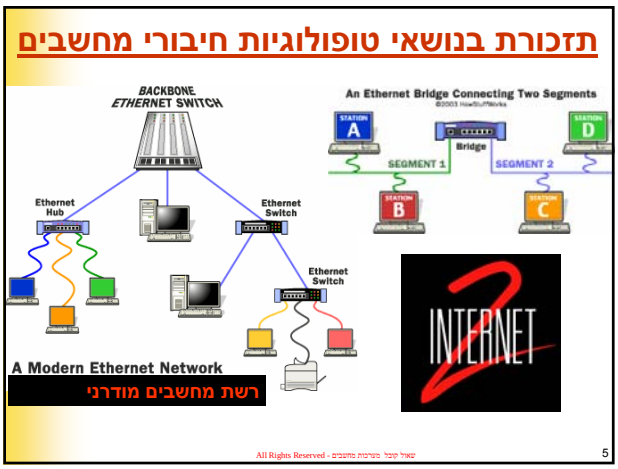
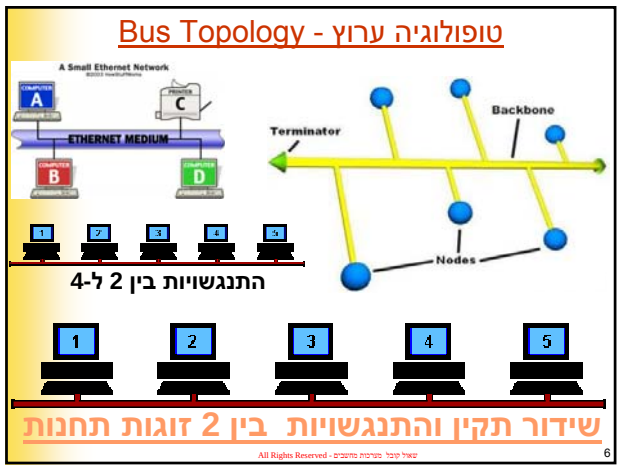

R&D Advisers
Web & Net Design - System Analyst
Computer Engineering Teach Advice
מצגות לימודיות להוראת מיקרו-מעבדים, אסמבלר, תקשורת, מערכות הפעלה.
שאול קובל
IEEE 802.1 -.2-.3
ETHERNET
יום שישי 05 מאי 2006
1
saul@coval.net
http://www.coval.net


ערב טוב !
נא לשמור על
השקט ולכבות
טלפונים!! תודה
תכינו את דפי העזר וכלי כתיבה
ורשמו הערות על פי הצורך
יום שישי 05 מאי 2006

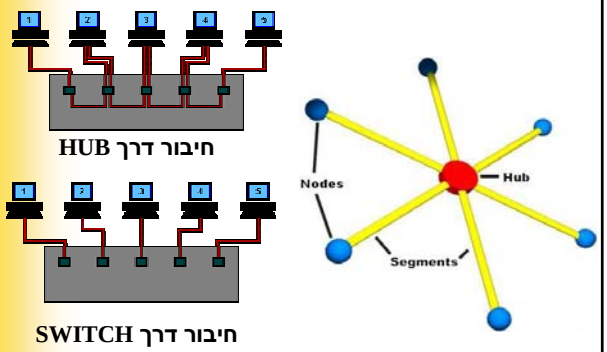

IEEE 802.1 / 802.2 / 802.3
ETHERNET
יום שישי 05 מאי 2006
saul@coval.net
http://www.coval.net


על פי תוכנית לימודים של משרד החינוך:
IEEE 802 10 שעות עיוני
IEEE 802 רקע , היסטוריה
מבוא IEEE 802 ומבנה השכבות
שכבת בקרת גישה לוגית - LLC - LOGICAL LINK CONTROL
שכבת בקרת גישה לתווך - MAC - MEDIA ACCESS CONTROL
MAC ADDRESS כתובת פיסית
הגדרה , מדוע דרושה הכתובת הפיסית , מיקום הכתובת הפיסית
כיצד שכבת ה- MAC משתמשת בכתובת הפיסית
framing- מבנה המסגרת , מבנה כללי של מסגרת
הסבר השדות במסגרת
שדה התחלה, שדה כתובת , שדה אורך/סוג , שדה נתונים שדה גילוי שגיאות , שדה סיום מסגרת
3.2.3 שכבה פיסית - PHYSICAL LAYER
3.3 השוואת IEEE 802 עם מודל OSI
כרטיס הרשת ותפקודו לפי המודלים
4
יום שישי 05 מאי 2006
Append by: שאול קובל מערכות מחשבים - All Rights Reserved
saul@coval.net
http://www.coval.net

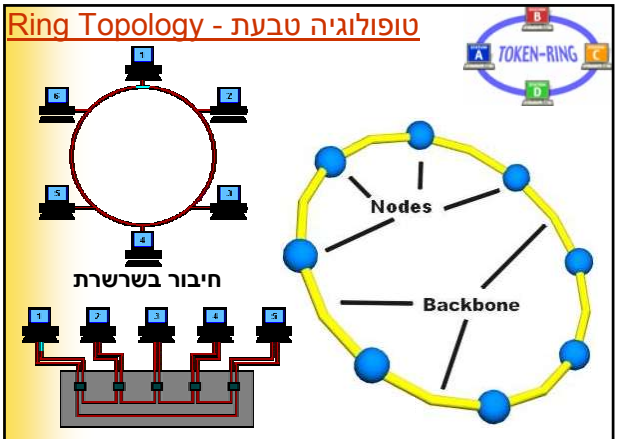

תזכורת בנושאי טופולוגיות חיבורי מחשבים
BACKBONE ETHERNET SWITCH
Ethernet Hub
Ethernet Switch
Ethernet Switch
A Modern Ethernet Network
רשת מחשבים מודרני
An Ethernet Bridge Connecting Two Segments
Bridge
SEGMENT 1
SEGMENT 2
INTERNET 2
All Rights Reserved - שאול קובל מערכות מחשבים
5


טופולוגיה ערוץ - Bus Topology
A Small Ethernet Network
ETHERNET MEDIUM
Terminator
Backbone
Nodes
התנגשויות בין 2 ל-4
שידור תקין והתנגשויות בין 2 זוגות תחנות
All Rights Reserved - שאול קובל מערכות מחשבים
6

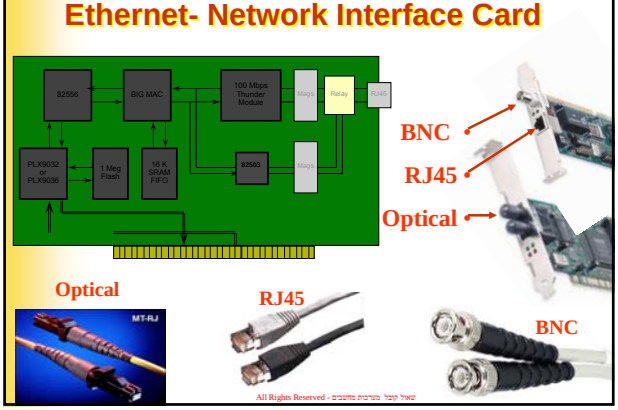
Star Topology - טופולוגיה כוכב



Ring Topology - טופולוגיה טבעת



שיטות חיבור לכרטיס תקשורת מסוג "אטרנט"
Ethernet- Network Interface Card



A brief detour… Matching Ethernet to the OSI Model

- The ***International Organization for Standardization*** (***ISO***) released the Open System Interconnection (***OSI***) *reference model* in 1984, was the descriptive scheme they created.
- ***"ISO. A network of national standards institutes from 140 countries working in partnership with international organizations, governments, industry, business and consumer representatives. A bridge between public and private sectors."*** www.iso.ch

ISO and the OSI Model

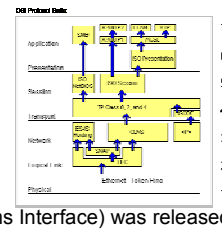
- "According to ISO, "ISO" is not an abbreviation. It is a word, derived from the Greek ***isos***, meaning "**equal**", which is the root for the prefix "iso-" that occurs in a host of terms, such as "isometric" (of equal measure or dimensions) and "isonomy" (equality of laws, or of people before the law).
- The name ISO is used around the world to denote the organization, thus avoiding the assortment of abbreviations that would result from the translation of "International Organization for Standardization" into the different national languages of members.
- Whatever the country, the short form of the organization's name is always ISO." www.whatis.com

OSI Model – Make more sense later

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

OSI Model



7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

- **OSI** (Open Systems Interface) was released as a **suite of protocols** to be used as the Internet standard.
- However, **TCP/IP** became the de facto standard.
- The OSI reference model is the primary model for network communications.
- Although there are other models in existence, most network vendors, today, relate their products to the OSI reference model, especially when they want to educate users on the use of their products.

OSI Model

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

The use of this model can be confusing and will become clearer later!

The **OSI reference model** allows you to

- view the network functions that occur at each layer
- a framework that you can use to understand how information travels throughout a network.
- understand, visualize, and troubleshoot the sending and receiving data on a network
- visualize how information, or data packets, travels from application programs, through a network medium (e.g. wires, etc.), to another application program that is located in another computer on a network, even if the sender and receiver have different types of network media

Note: The Application Layer of the OSI model refers to networking applications, and not user applications.

ISO's OSI Reference Model - תזכורת

A Layered Model:

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

A mnemonic:

All People Seem To Need Data Processing

ISO's OSI Reference Model

Why a Layered Network Model?

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

- Reduces complexity
- Standardizes interfaces
- Facilitates modular engineering
- Ensures interoperable technology
- Accelerates evolution
- Simplifies teaching and learning

Open System Interconnection (OSI)

Layer Functions

7	Application	Network processes to applications
6	Presentation	Data representation
5	Session	Interhost communication
4	Transport	End-to-end connections
3	Network	Addresses and best path
2	Data Link	Access to media
1	Physical	Binary transmition

7 - Application Layer

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Network processes to applications

- Provides network services to application processes (such as electronic mail, file transfer, and terminal emulation)

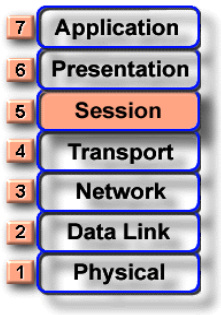
6 - Presentation Layer

Network processes to applications

Data representation

- Insure data is readable by receiving system
- Format of data
- Data structures
- Negotiates data transfer syntax for application layer

5 - Session Layer



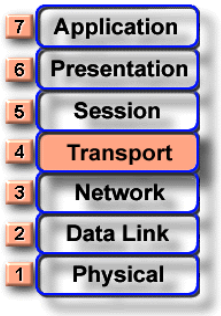
Network processes to applications

Data representation

Interhost communication

- Establishes, manages, & terminates sessions between applications

4 - Transport Layer



Network processes to applications

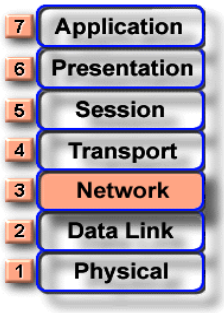
Data representation

Interhost communication

End-to-end connections

- Concerned with data transport issues between hosts
- Data transport reliability
- Establish, maintain, terminate virtual circuits
- Fault detection and recovery
- Information flow control

3 - Network Layer



Network processes to applications

Data representation

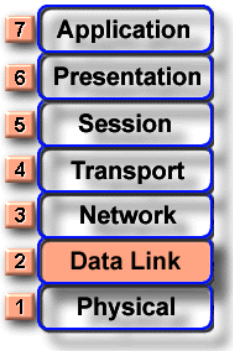
Interhost communication

End-to-end connections

Addresses and best path

- Provides connectivity and path selection between two end systems
- Domain of routing

2 - Data Link



Network processes to applications

Data representation

Interhost communication

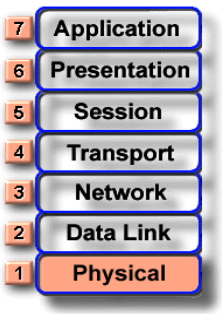
End-to-end connections

Addresses and best path

Access to media

- Provides reliable transfer of data across media
- Physical addressing, network topology, error notification, flow control

1 - Physical Layer



Network processes to applications

Data representation

Interhost communication

End-to-end connections

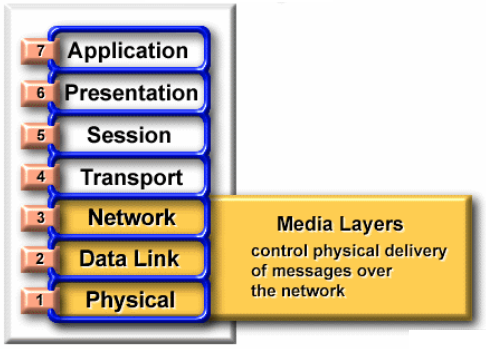
Addresses and best path

Access to media

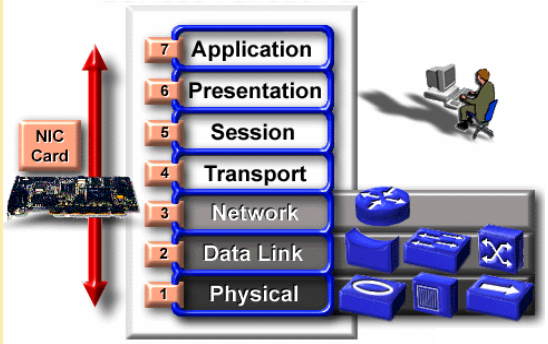
Binary transmition

* Wires, connectors, voltages data rates

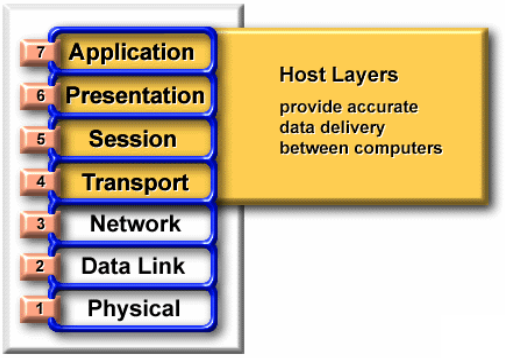
Media Layers



Devices at Layers



Host Layers



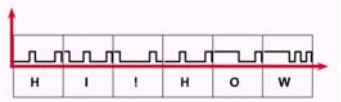
Layer 1 Limitations

- No addressing
- No logical grouping or organization (framing)
- No method to provide media access

Layer 2

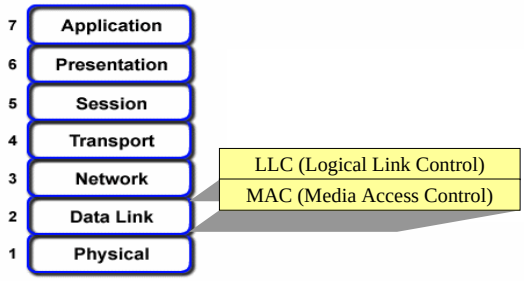
Layer 2 solves these problems.

Layer 1 Limitations



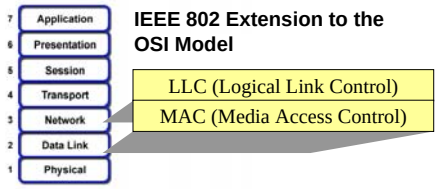
- Layer 1 involves media, signals, bit streams that travel on media, components that put signals on media, and various topologies.
- Layer 1 cannot communicate with the upper-level layers; Layer 2 does that with ***Logical Link Control (LLC).***
- Layer 1 cannot name or identify computers; Layer 2 uses an ***addressing*** (or naming) process.
- Layer 1 can only describe streams of bits; Layer 2 uses ***framing*** to organize or group the bits.
- Layer 1 cannot decide which computer will transmit binary data from a group that are all trying to transmit at the same time. Layer 2 uses a system called ***Media Access Control (MAC).***

Data Link Sublayers



IEEE 802 Extension to the OSI Model

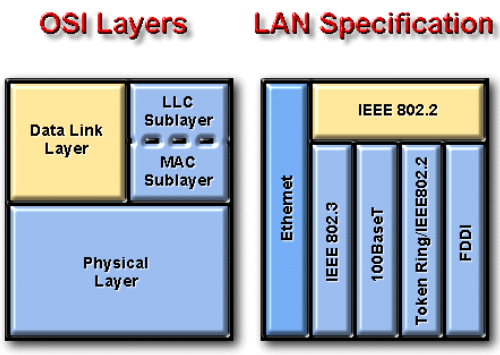
Data Link Sublayers



IEEE 802 Extension to the OSI Model

- The Institute of Electrical and Electronic Engineers (IEEE) is a professional organization that defines network standards.
- IEEE 802.3 and IEEE 802.5 are the predominant and best known LAN standards.
- The *IEEE* divides the OSI data link layer into two separate sublayers. Recognized IEEE sublayers are:
  - Media Access Control (MAC) (transitions down to media)
  - Logical Link Control (LLC) (transitions up to the network layer)

OSI v IEEE

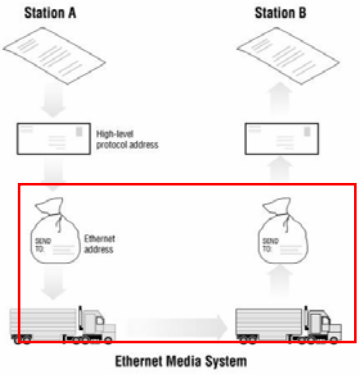


Evolution of the Ethernet Standard

- **1979** Bob Metcalfe developed Ethernet at XEROX PARC
- **1980** DEC-Intel-Xerox (DIX) publish first original 10 Mbps Ethernet Standard over thick coaxial cable
- **1985** IEEE 802.3 used DIX standard and published standard with the title *IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- **Supplements**
  - 1985 10BASE2 Thin Ethernet
  - 1990 10BASE-T Twisted-pair
  - 1995 100BASE-T Fast Ethernet and Autonegotiation
  - 1997 Full Duplex Standard
  - 1998 1000BASE-X Gigabit Ethernet

Ethernet is Best Effort Delivery

- **Ethernet is best-effort delivery, no guarantee.**
- **Like a trucking service, it doesn't really know or care about the what it is carrying.**



IEEE Identifiers

Early Standards	Older Fiber Standards	100 Mbps Media	1000 Mbps Media
10BASE5	10BASE-F	100BASE-T	1000BASE-X
10BASE2	10BASE-FB	100BASE-X	1000BASE-SX
FOIRL	10BASE-FP	100BASE-TX	1000BASE-LX
10BROAD36	10BASE-FL	100BASE-FX	1000BASE-CX
1BASE5		100BASE-T4	1000BASE-T
10BASE-T		100BASE-T2	
Many of these standards were short lived or never implemented			

3 part identifier

- Speed in Mbps
- Type of signaling used (Baseband or Broadband)
- Distance or Medium
  - Early days: Cable Distance in meters, rounded to the nearest 100 meters
  - Later days: Physical medium used

IEEE Identifiers

- **10BASE5 (Thick Ethernet)**
  - 10 refers to 10 Mbps
  - **Baseband**: Dedicated to carrying one type of service
  - **Broadband**: (Cable television) Designed to deliver multiple channels
  - 5 refers to 500 meter maximum distance
- **100BASE-TX (Most widely used variety of Fast Ethernet)**
  - 100 refers to 100 Mbps
  - TX Two pairs of Category 5 Twisted-pair cable

The IEEE Working Groups

802.1	Networking Overview and Architecture
802.2	Logical Link Control
802.3	Ethernet
802.4	Token Bus
802.5	Token Ring
802.6	MANs
802.7	Broadband
802.8	Fiber Optic
802.9	Isochronous LAN

...and more!

BTW: Ethernet vs IEEE 802.3

- Most of the time, the term “Ethernet” is used to mean IEEE 802.3
- For the most part, **Ethernet** and **IEEE 802.3** are used interchangeably, even though they are not really the same thing.
- We will discuss this more later.

Logical Link Control (LLC)

- Defined by a committee named 802.2
- Is technology independent
- Is not used by all networks

What is it?

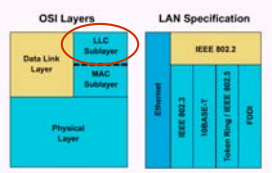
- Provides independence to the protocols running in the upper and lower layers.
- The LLC acts as a managing buffer between the “executive” upper layers and the “shipping department” lower layers.

Logical Link Control

- The LLC sublayer uses:
  - *Source Service Access Points (SSAPs)*
  - *Destination Service Access Points (DSAPs)*

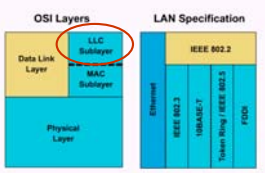
  to help the lower layers communicate to the Network layer protocols.

LLC – Logical Link Sublayer



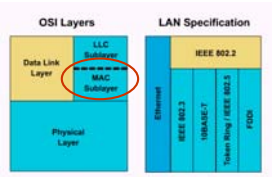
- Logical link sublayer allows part of the data link layer to function independently from existing technologies.
- Provides versatility in services to network layer protocols that are above it, while communicating effectively with the variety of technologies below it.
- The LLC, as a sublayer, participates in the encapsulation process.
- It adds two addressing components of the 802.2 specification - the Destination Service Access Point (DSAP) and the Source Service Access Point (SSAP). (Later)

LLC – Logical Link Control Sublayer



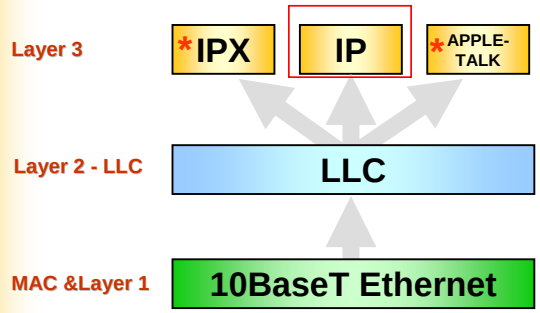
- Defined in the IEEE 802.2 specification
- Defines a number of fields in the data link layer frames that enable multiple higher-layer protocols to share a single physical data link.
- The LLC acts as a managing buffer between the “executive” upper layers and the “shipping department” lower layers.

MAC – Media Access Control Sublayer



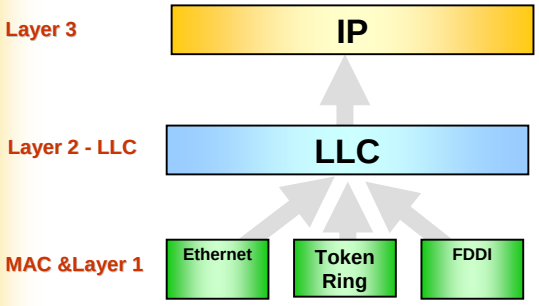
- The Media Access Control (MAC) sublayer deals with the protocols that a host follows in order to access the physical media.
- Responsible for the actual framing
  - builds the 1s and 0s to hand off to the physical layer.
- Responsible for media access: (later)
  - Contention
  - Token Passing
  - Polling

802.2 LLC



* Legacy technologies

802.2 LLC



Media Access Control

- Responsible for the actual framing
  - builds the 1s and 0s to hand off to the physical layer.
- Responsible for media access:
  - Contention
  - Token Passing
  - Polling

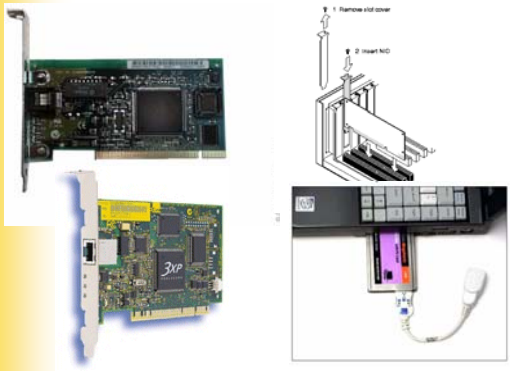
Data Link Layer - Up Close

- Responsible for accessing the media
- Provides a unique hardware address or Media Access Control (MAC) address.
- The Network Interface Card (NIC) lives here

The NIC (Card)

MAC address 00-C0-4F-6C-35-73
"Burned In" to the card

Network Interface Card (NIC)

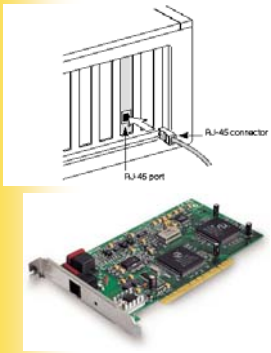


Network Interface Card (NIC)

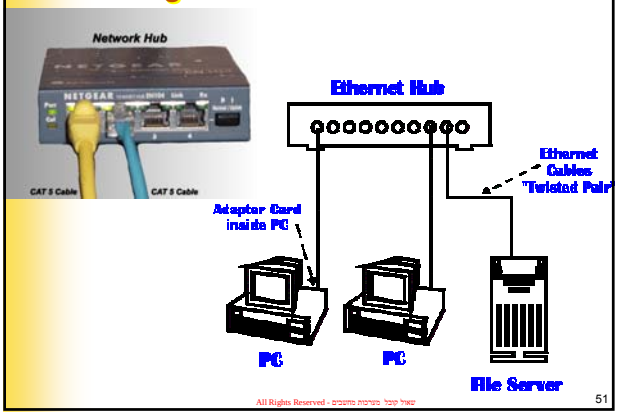
Network Interface Card (NIC)

- Layer 2, Data Link Layer, device
- Connects the device (computer) to the LAN
- Responsible for the local Layer 2 address (later)
- Common Layer 2 NICs:
  - Ethernet
  - Token Ring
- Common Bandwidth
  - 10 Mbps, 10/100 Mbps, 10/100/1000 Mbps

Tracing the Physical Connection NIC (Network Interface Card)

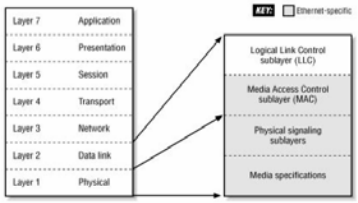


Connecting the NIC to a Hub or Switch…



From PC to Ethernet Port…

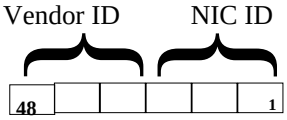
Media Access Control Protocol



- Original Ethernet standard based on CSMA/CD media access control (MAC)
- Also known as Half-duplex mode
- No need for CSMA/CD in Full-duplex mode (later)
- Compete for a shared Ethernet channel in a fair and equitable manner

Ethernet

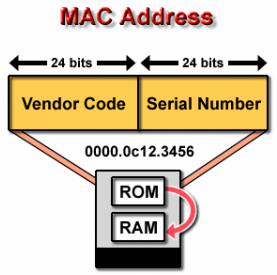
- Every station on a network has a unique address, known as a MAC (Media Access Control) address.
- The MAC address is a world-wide unique 6-byte address assigned by the IEEE.



MAC address

The MAC address is also called the:

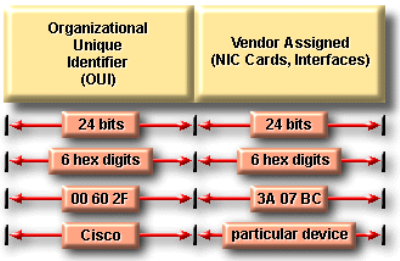
- Hardware address
- Physical address
- Ethernet address
- Adapter address



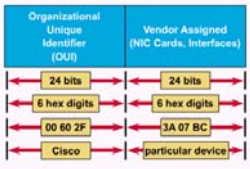
- Mac address is burned into ROM on a network interface card

The MAC Address

MAC Address Format

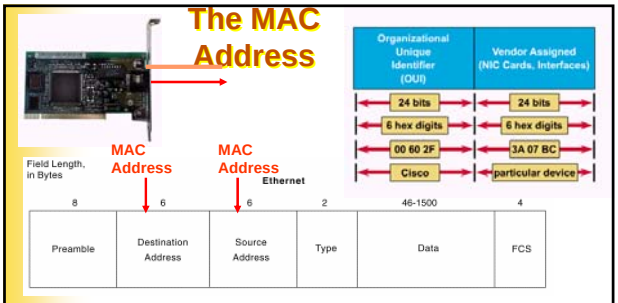


The MAC Address



- MAC addresses are:
  - 48 bits in length
  - Expressed as twelve hexadecimal digits.
  - The first six hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and thus comprise the ***Organizational Unique Identifier (OUI).***
  - The remaining six hexadecimal digits comprise the *interface serial number*, or another value administered by the specific vendor.
- MAC addresses are sometimes referred to as *burned-in addresses (BIAs)* because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the NIC initializes

The MAC Address



- The Ethernet protocol uses MAC addresses to identify the **source** of the Ethernet frame and the **destination** of the Ethernet frame.
- Whenever is computer sends an Ethernet frame, it includes the MAC address on its NIC as the Source "MAC" Address.
- We will learn later how it learns the Destination "MAC" Address.
- We will see how all of this works in a moment.

Hexadecimal

Base 16 (Hexadecimal) Number System

Place Value- 1024's 256's 16's 1's

Base Exponent - $16^3 = 1024$
$16^2 = 256$
$16^1 = 16$
$16^0 = 1$

Number of Symbols- 16

Symbols- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(=10), B(=11), C(=12), D(=13), E(=14), F(=15)

Why? Useful for computer engineering and programming purposes.

Method 1: Converting Decimal to Hex

Method 1: Convert the decimal number 24,032 to hex

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(14)

	4096's	256's	16's	1's
24,032 / 4096 = 5 r 3,352	5			
3,552 / 256 = 13 r 224		D(13)		
224 / 16 = 14 r 0			E(14)	
0 / 1 = 0				0

5DE0

Method 2: Converting Decimal to Hex

Method 2: Convert the decimal number 24,032 to hex

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(14)

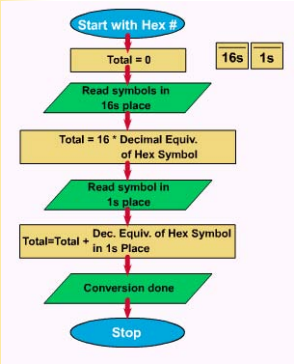
24,032/16= 1502, with a remainder of 0
1,502/16=93, with a remainder of 14 or E
93/16=5, with a remainder of 13 or D
5/16=0, with a remainder of 5

By collecting all the remainders backward, you have the hex number
5DE0

Method 3: Converting Decimal to Hex

- View -> Scientific
- Nice tool, but be sure you know how to calculate it by hand!

Hex to Decimal



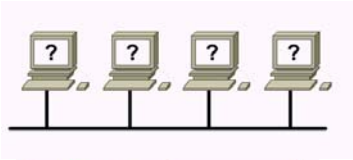
Convert the hex number **3F4B** to a decimal number. (Work from right to left.)

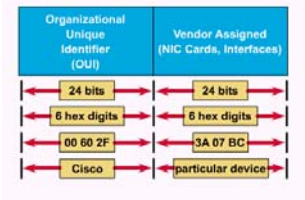
```
3 x 16³ (4,096)  = 12,288
F(15) x 16² (256)=  3,840
4 x 16¹ (16)     =     64
B(11) x 16⁰ (1)  =     11
-------------------------
                   16,203
```


Decimal, Binary, Hex

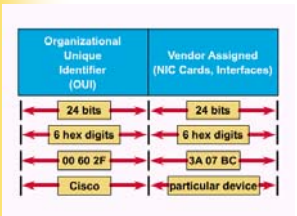
0 = 0000 = 0	8 = 1000 = 8
1 = 0001 = 1	9 = 1001 = 9
2 = 0010 = 2	10 = 1010 = A
3 = 0011 = 3	11 = 1011 = B
4 = 0100 = 4	12 = 1100 = C
5 = 0101 = 5	13 = 1101 = D
6 = 0110 = 6	14 = 1110 = E
7 = 0111 = 7	15 = 1111 = F

Nameless Computers





MAC Address Format

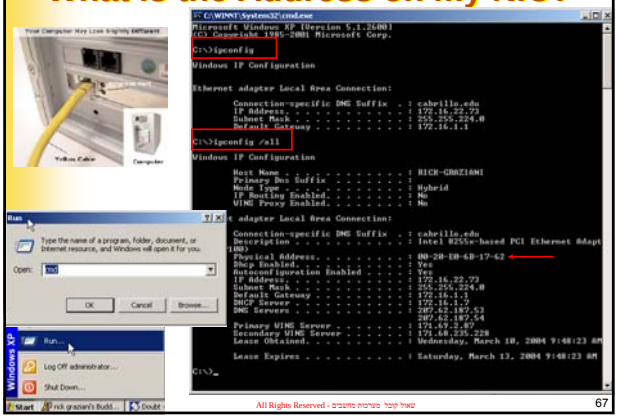


0 = 0000 = 0 | 8 = 1000 = 8
1 = 0001 = 1 | 9 = 1001 = 9
2 = 0010 = 2 | 10 = 1010 = A
3 = 0011 = 3 | 11 = 1011 = B
4 = 0100 = 4 | 12 = 1100 = C
5 = 0101 = 5 | 13 = 1101 = D
6 = 0110 = 6 | 14 = 1110 = E
7 = 0111 = 7 | 15 = 1111 = F

OUI unique

- An Intel MAC address: **00-20-E0-6B-17-62**
- 0000 0000 - 0010 0000 – 1110 0000 - 0110 1011 – 0001 0111 – 0110 0010
- IEEE OUI FAQs: http://standards.ieee.org/faqs/OUI.html

What is the Address on my NIC?

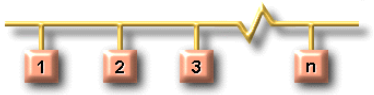


67

MAC Addresses Are Flat

Mac Addresses: A Flat Addressing Scheme

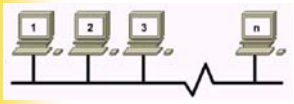
Flat (Non-Hierarchical) Addressing

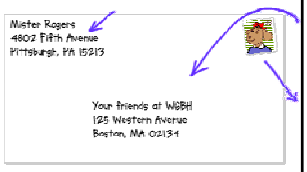


As n increases, communication becomes difficult

68

MAC Addresses Are Flat

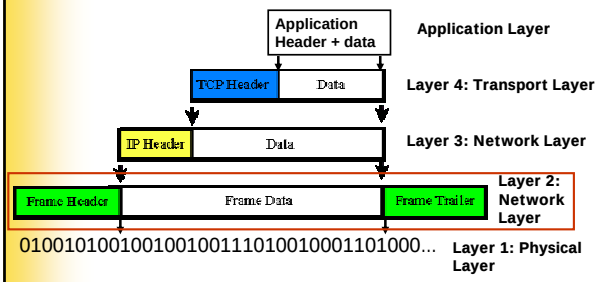




- MAC addresses provide a way for computers to identify themselves.
- They give hosts a permanent, unique name.
- The number of possible MAC addresses is 16^12 (or over 2 trillion!).
- MAC addresses do have one major **disadvantage**:
  - They have no structure, and are considered flat address spaces.
  - Like using just a name when sending a letter instead of a structured address.

69

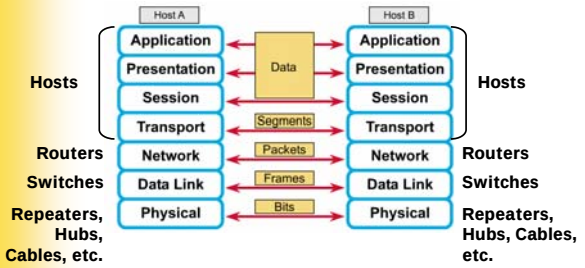
Data Encapsulation Example



Let us focus on the Layer 2, Data Link, Ethernet Frame for now.

70

Peer-to-Peer Communications



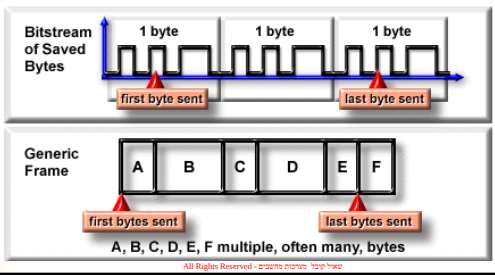
- Again, we are dealing with just the Data Link (and Physical) layers.

71

Generic Data Link Frame

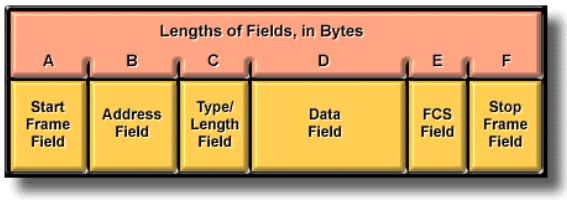
- A message is “framed” at layer two.
- Framing provides order, or structure, to the bitstream.

Frames Provide Structure



72

Frame Format



Ethernet / IEEE 802.3 frame format:

Ethernet

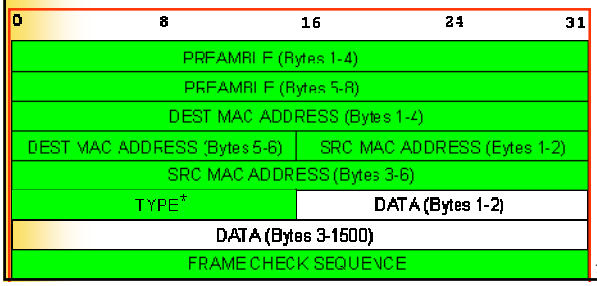
Preamble	Destination Address	Source Address	Type	Data	CRC
1010101010.....11					
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

IEEE 802.3

Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header	Data	CRC
101010...	*10101011*						
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		46-1500 bytes	4 bytes

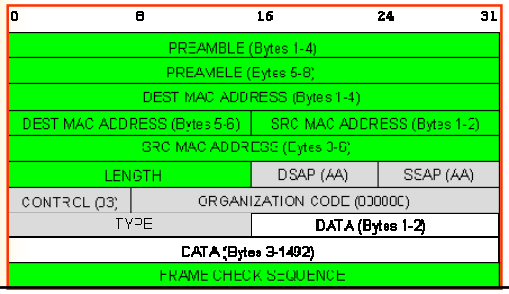
Ethernet

Preamble	Destination Address	Source Address	Type	Data	CRC
1010101010.....11					
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes



IEEE 802.3

Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header	Data	CRC
101010...	*10101011*						
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		46-1500 bytes	4 bytes



FCS – Frame Checksum

- Used to insure that the data has arrived without corruption.
- More efficient than sending the data twice and comparing the results.
- Necessary to prevent errors.

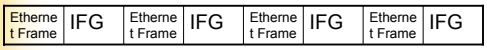
Three Kinds of FCS

- cyclic redundancy check (CRC)
  - performs polynomial calculations on the data
- two-dimensional parity
  - adds an 8th bit that makes an 8-bit sequence have an odd or even number of binary 1s
- Internet checksum
  - adds the numbers to determine a number

Bringing it all together…

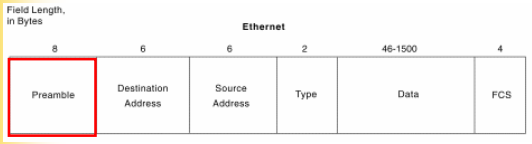
- Let's pause here for a moment and figure all of this out!
- Let's bring the following together:
  - Ethernet Frames and MAC Addresses
  - Sending and receiving Ethernet frames on a bus
  - CSMA/CD
  - Sending and receiving Ethernet frames via a hub
  - Sending and receiving Ethernet frames via a switch

IFG – Interframe Gap



- Ethernet devices must allow a minimum idle period between transmission of frames known as the **interframe gap (IFG)** or interpacket gap (IPG).
- Note: Both half and full-duplex
- It provides a brief recovery time between frames to allow devices to prepare for reception of the next frame.
- The minimum interframe gap is:
  - **10 Mbps Ethernet**: 96 bit times, which is 9.6 microseconds (millionths of a second)
  - **100 Mbps, Fast Ethernet**: 960 nanoseconds (billionths of a second)
  - **1000 Mbps**, **Gigabit Ethernet**: 96 nanoseconds
- Note: 802.11 (WLAN) uses similar

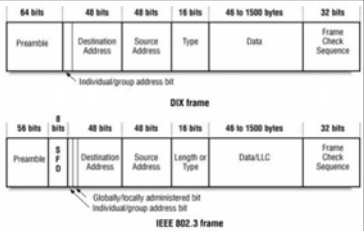
Generic Data Link Frame Format



Preamble or Start Field

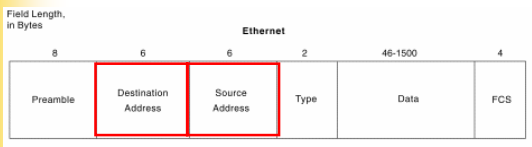
- When computers are connected to a physical medium, there must be a way they can grab the attention of other computers to broadcast the message, "Here comes a frame!"
- Various technologies have different ways of doing this process, but all frames, regardless of technology, have a beginning signaling sequence of bytes.
- Depending up frame format: Preamble = 7 bytes, Start or Start of Frame Delimiter (SFD) = 1 byte

A closer look at the frames



- **Preamble**
  - Allows NIC to synchronize themselves with incoming data stream
  - Allows beginning of the frame to lose a few bits due to start-up delays
  - Like a heat shield of a spacecraft
  - Fast Ethernet and Gigabit Ethernet do not need preamble, but is preserved for backwards compatibility.
- No practical difference between DIX and 802.3
  - 802.3 divides preamble into two parts including SFD (Start Frame Delimeter)

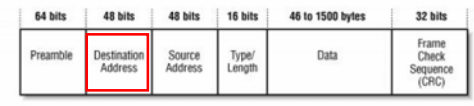
Generic Data Link Frame Format



Address Field

- We saw how IEEE 802.3 uses Destination and Source Addresses.
- By the way: Any idea how a serial data link frame is addressed?
  - **Unicast** address – Single device
  - **Broadcast** address – All devices
  - **Multicast** address – Specific group of devices

Unicast, Multicast, Broadcast Destination Addresses



- **Unicast address**: A single Ethernet frame to be received by a single station.
  - **Unknown Unicast**: This is from the perspective of a switch, when the unicast address is not in its MAC Address Table
- **Multicast address**: A single Ethernet frame to be received by a group of stations.
- **Broadcast address**: Special case of a multicast address, which is all 1's. This is an Ethernet frame to be received by all stations.

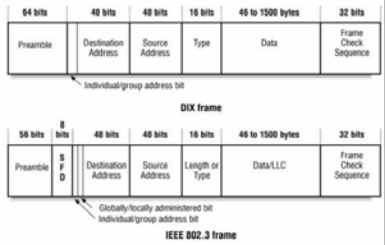
Destination Address

- First bit of Destination Address:
  - 0 = Unicast Address
  - 1 = Multicast or Broadcast Address
- 802.3 adds significance to the 2nd bit of Destination Address
  - 0 = Globally Administered, assigned by manufacturer
  - 1 = Locally Administered, assigned by administrator (very rare!)
- 48 bit address can be written as 12 hexadecimal digits
  - Leftmost octet of bits written as rightmost hexadecimal octet
  - Actual transmission order of the octet, is least significant bit to most significant bit. [2E = 0010 1110 would be transmitted as 0111 0100]

F0-2E-15-6C-77-9B

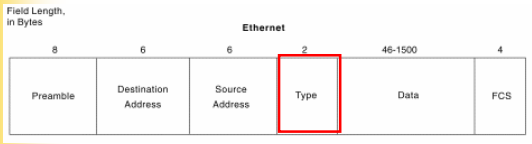
0000 1111 0111 0100 1010 1000 0011 0110 1110 1110 1101 1001

Type or Length Field



- DIX
  - Type field: refers to high-level protocol being carried
  - 0x800 = IP
- 802.3
  - < 1500 (decimal) = length field
    - Number of bits carried in the data field, less any padding
  - >= 1536 (0x600 hex) = type field, same as DIX

Generic Data Link Frame Format



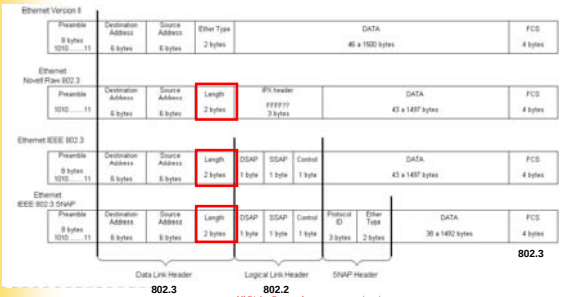
Type Field

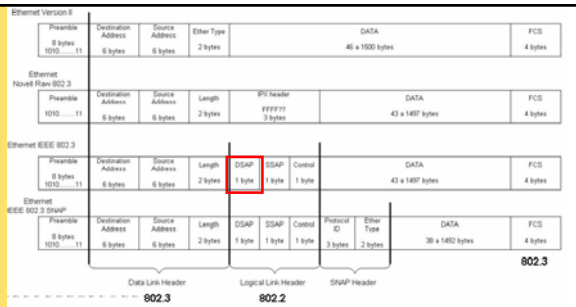
- Usually information indicating the layer 3 protocols in the data field, I.e. IP Packet.
- Type field values of particular note for IEEE 802.3 frames include:
  - 0x0600 XNS (Xerox)
  - **0x0800 IP** (the Internet protocol)
  - 0x8137 Novell NetWare packet formatted for Ethernet II
  - 0x6003 DECNET

"Ethernet" Frame Formats

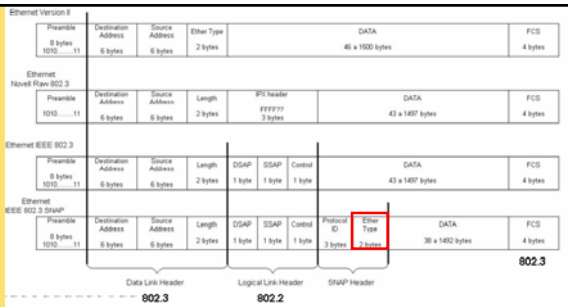
Length Field

- In some frame formats such as 802.3, there is a length field which specifies the exact length of a frame.

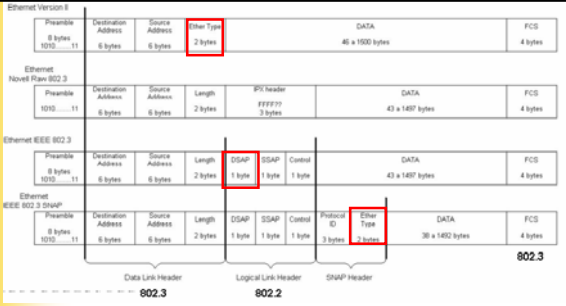




- IEEE 802.3 specification limits the data portion to a maximum of 1500 bytes.
- Designed to hold a Layer 3 IP packet.
- When IEEE created 802.2, it saw the need for a protocol TYPE field that identified what was inside the "data" field.
- IEEE called its 1 byte type field DSAP (Destination Service Access Point).
- Turned out that 1 byte was not long enough to handle all the different number of protocols.

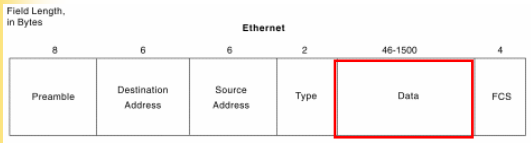


- To accommodate more protocols IEEE added the SNAP (Subnetwork Access Protocol) header.



- The fields of various Ethernet framing that are used for identifying the type of data contained in a frame:
  - **Ethernet II or DIX (DEC, Intel, Xerox) – Most common**
  - IEEE Ethernet (802.3)
  - IEEE 802.3 with SNAP header

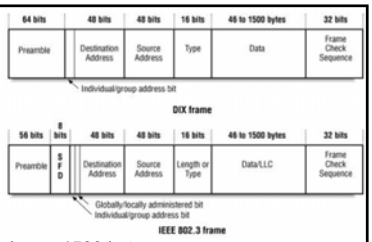
Generic Data Link Frame Format



Data Field

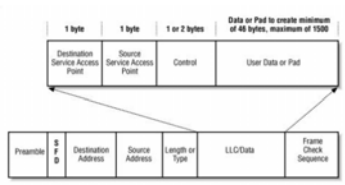
- Included along with this data, you must also send a few other bytes.
- They are called *padding bytes*, and are sometimes added so that the frames have a minimum length for timing purposes.
- LLC bytes are also included with the data field in the IEEE standard frames. (later)

Data Field



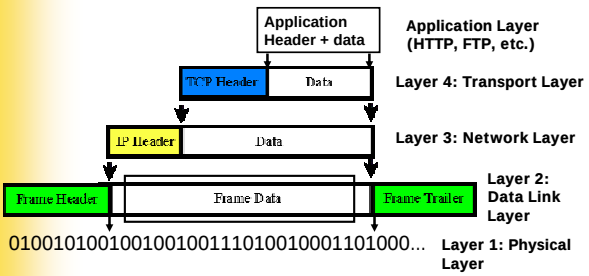
- DIX
  - Minimum 46 bytes, maximum 1500 bytes
  - Layer 3, network protocol, software expected to proved at least 46 bytes of data
- 802.3
  - Minimum 46 bytes, maximum 1500 bytes
  - May include LLC protocol for control information to identify type of data being carried, similar to DIX type field

802.3 Data Field

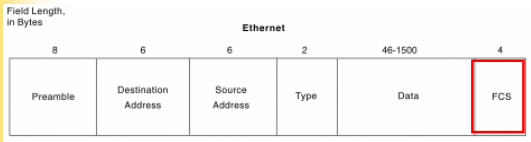


- Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) are similar to DIX type field.
- ***To sum all of this up…***

Data Encapsulation Example



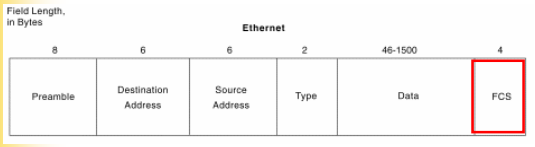
Generic Data Link Frame Format



FCS

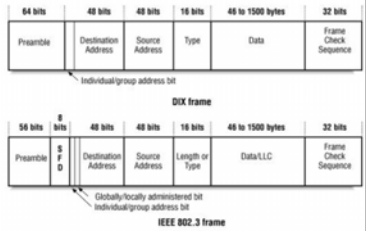
- Used to insure that the data has arrived without corruption.
- More efficient than sending the data twice and comparing the results.
- Necessary to prevent errors.

Three Kinds of FCS



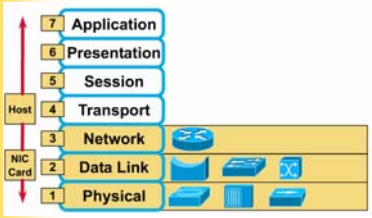
- **Cyclic redundancy check (CRC)**
  - performs polynomial calculations on the data
- **Two-dimensional parity**
  - adds an 8th bit that makes an 8-bit sequence have an odd or even number of binary 1s
- **Internet checksum**
  - adds the numbers to determine a number

FCS



- Frame Check Sequence (FCS)
  - Uses CRC (Cyclic Redundancy Check)
  - Checks integrity of all fields except preamble/SFD
  - Calculation using contents of destination, source, type or length and data fields.
  - CRC calculated again by received NIC
  - If calculations differ, frame is dropped

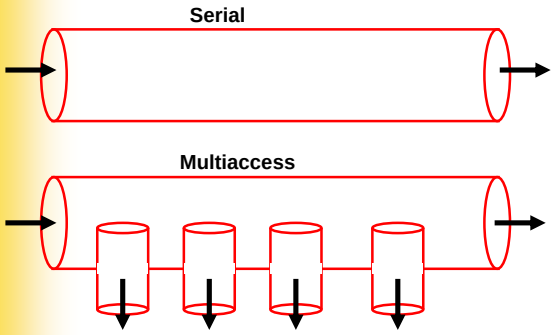
Devices and their layers

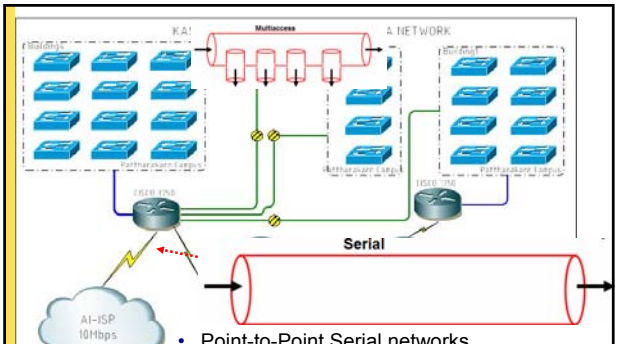


Transceiver

- Hosts and servers operate at Layers 2-7; they perform the encapsulation process.
- **Routers**: Layers 1 through 3, make decisions at layer 3
- **Switches and NICs**: Layers 1 and 2, make decisions at layer 2
- **Hubs and transceivers**: Layer 1, no decisions to make

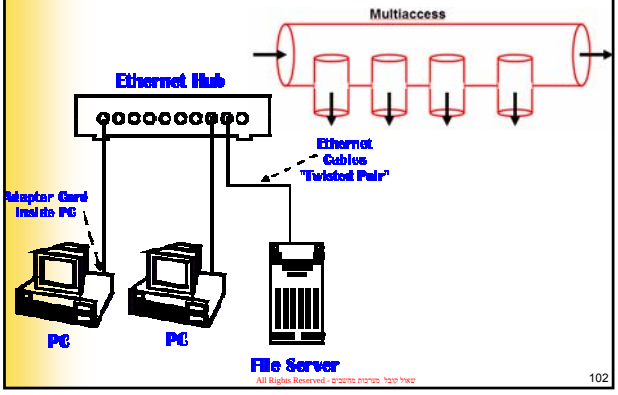
Serial vs Multiaccess Network



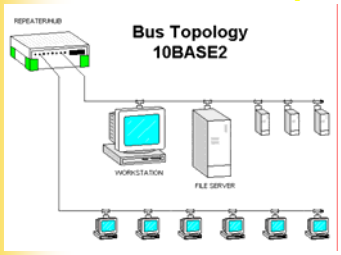


- Point-to-Point Serial networks
  - Usually connection between only two devices, such as two routers.
  - Point-to-Point Serial protocols include ISDN, PPP, HDLC, T1, T3, etc.

Ethernet: Multiaccess Network



Bus Topology

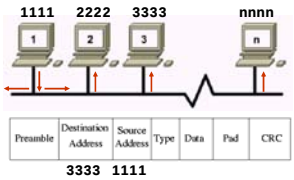


A bus topology uses a single backbone segment (length of cable) that all the hosts connect to directly.

Original Ethernet used a bus topology.

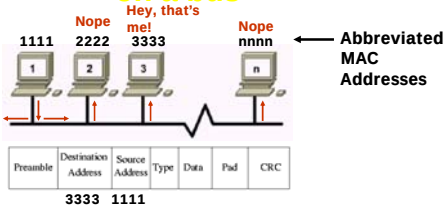
By the way, Ethernet hubs work the same as a "bus".

Sending and receiving Ethernet frames on a bus



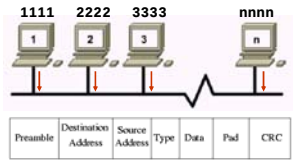
- When an Ethernet frame is sent out on the "bus" all devices on the bus receive it.
- What do they do with it?

Sending and receiving Ethernet frames on a bus



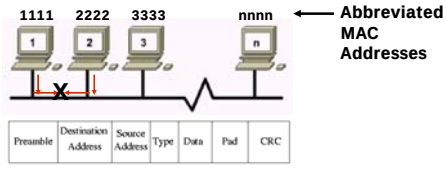
- Each NIC card compares its own MAC address with the Destination MAC Address.
- If it matches, it copies in the rest of the frame.
- If it does NOT match, it ignores the rest of the frame.
  - Unless you are running a Sniffer program

Sending and receiving Ethernet frames on a bus



- So, what happens when multiple computers try to transmit at the same time?

Sending and receiving Ethernet frames on a bus



Collision!

Media Access Methods

Two common types of access methods for LANs include

- **Non-Deterministic**: Contention methods (Ethernet, IEEE 802.3)
  - Only one signal can be on a network segment at one time.
  - Collisions are a normal occurrence on an Ethernet/802.3 LAN

- **Deterministic**: Token Passing (Token Ring)
  - aka "Taking Turns"
  - example: Token Passing used in Token Ring
  - No collisions

Non-Deterministic

- aka “First Come, First Served”
  - Example: CSMA/CD used in Ethernet
  - Started with ALOHA project at University of Hawaii
  - collisions

Network Architectures

Network Architectures combine Layer 1 and Layer 2 “rules.” Four of the most popular network architectures are:

- Ethernet
- Token Ring
- FDDI
- ARCnet

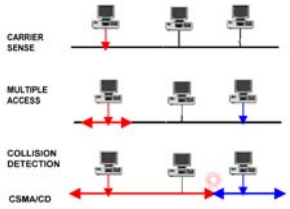
CSMA/CD

CSMA/CD

(Carrier Sense Multiple Access with Collision Detection)

Common contention method used with Ethernet and IEEE 802.3

“Let everyone have access whenever they want and we will work it out somehow.”



CSMA/CD and Collisions

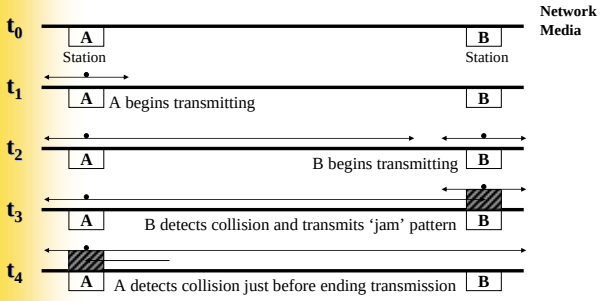
CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- Listens to the network’s shared media to see if any other users on “on the line” by trying to sense a neutral electrical signal or carrier.
- If no transmission is sensed, then *multiple access* allows anyone onto the media without any further permission required.
- If two PCs detect a neutral signal and access the shared media at the exact same time, a *collision* occurs and is *detected*.
- The PCs sense the collision by being unable to deliver the entire frame (coming soon) onto the network. *(This is why there are minimum frame lengths along with cable distance and speed limitations. This includes the 5-4-3 rule.)*
- When a collision occurs, a jamming signal is sent out by the first PC to detect the collision.
- Using either a priority or random backoff scheme, the PCs wait certain amount of time before retransmitting.
- If collisions continue to occur, the PCs random interval is doubled, lessening the chances of a collision.

CSMA/CD and Collisions

- The ‘jam’ pattern consists of from 32 to 48 bits of any pattern except the 32-bit CRC value corresponding to the partial frame transmitted prior to the ‘jam’.
- The ‘jam’ pattern guarantees that the collision lasts long enough to be detected by all transmitting stations.
- A transmitting station that detects the collision then waits (back-off process) for a random period before trying again.

CSMA/CD and Collisions

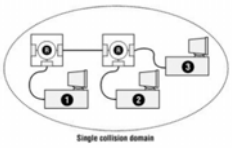


CSMA/CD and Collisions

And as we said,

- When information (frame) is transmitted, every PC/NIC on the shared media copies part of the transmitted frame to see if the destination address matches the address of the NIC.
- If there is a match, the rest of the frame is copied
- If there is NOT a match the rest of the frame is ignored.

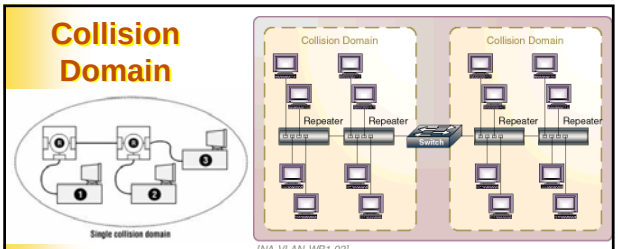
Collisions, Slot time and Minimum Frame Size



Notes

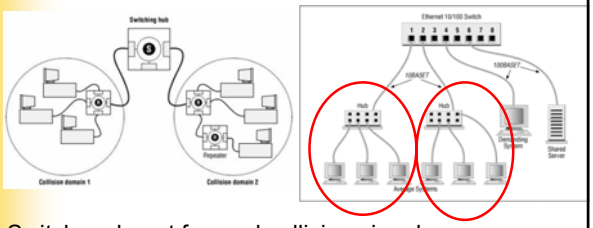
- Original Ethernet (802.3) designed as Half-duplex
- CSMA/CD is based on half-duplex and is NOT part of full-duplex
- Collisions are part of CSMA/CD and half-duplex Ethernet
- Collisions are a normal part of operation and are NOT errors
- Collisions are NOT part of full-duplex Ethernet

Collision Domain



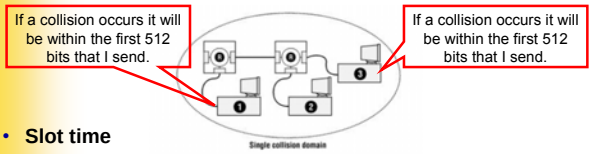
- **Collision Domain**: Refers to a single half-duplex Ethernet system whose elements (cables, repeaters, hubs, station interfaces and other network hardware) are all part of the same signal timing domain.
- If two or more devices transmit at the same time a collision will occur.
- If a collision is detected, the station will continue to transmit 32 bits called the **collision enforcement jam signal**.

Collision Domain



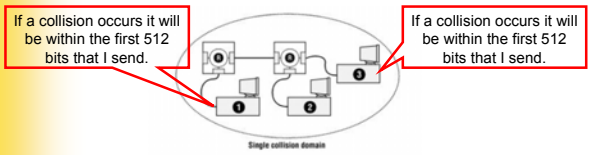
- Switches do not forward collision signals

Slot Time and Maximum Cable Length



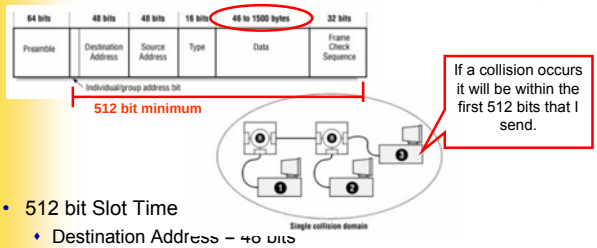
- **Slot time**
  - Time it takes for a signal to travel from one end of the maximum-sized system to the other end and return (round trip propagation time) within a collision domain.
  - Maximum time required by collision enforcement.
  - After this amount of time (or bits), device assumes no collision.
- Ethernet and Fast Ethernet
  - Slot time = 512 bit times (the time it takes to transfer 512 bits)

Slot Time and Maximum Cable Length



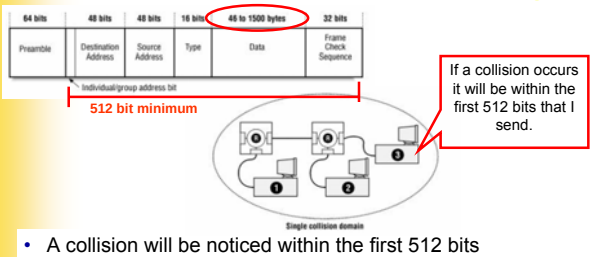
- Slot time and maximum cable length are tightly coupled.
  - Original 10 Mbps Ethernet: On coaxial cable, signals could travel 2,800 meters (9,186 feet) and back in 512 bit times.
  - Maximum distance of collision domain is 2,800 meters.
  - In other words, a station would know about a collision (rise in DC signal level) before it transmitted the 513th bit.
- Fast Ethernet Twisted-pair maximum network diameter is 205 meters or 672 feet, but is limited by cabling standards of 100 meters or 328 feet. (Remember, more bits per second, shorter bits, than Ethernet)

Slot Time and Maximum Cable Length



- 512 bit Slot Time
  - Destination Address = 48 bits
  - Source Address = 48 bits
  - Type = 16 bits
  - Data = 368 bits or (46 bytes * 8 bits per byte)
  - FCS = 32 bits
- ***This is why there is a <u>minimum of 46 bytes of data</u>!***

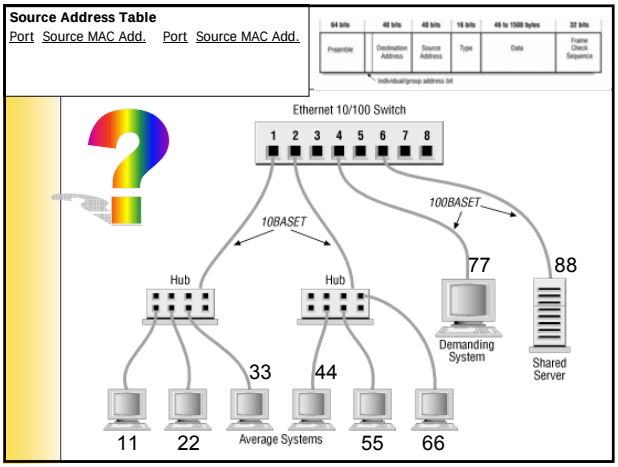
Slot Time and Maximum Cable Length

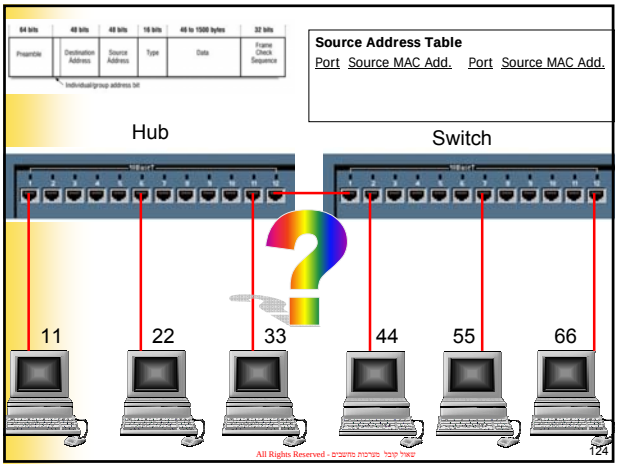


- A collision will be noticed within the first 512 bits transferred, so the minimum frame size must be 512 bits.
- After 512 bits, the sending station assumes no collisions.
- At 513 bits, all stations on the entire Ethernet system, collision domain (cable, repeaters, hubs) should have seen this frame by now before they begin transmitting.
- ~~This is why there is a maximum size to the Ethernet~~

Source Address Table

Port Source MAC Add. Port Source MAC Add.





DL: Random access MAC protocols

- CSMA: Carrier Sense Multiple Access

CSMA: listen before transmit:

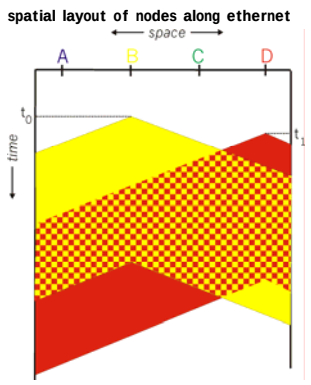
- If channel sensed idle: transmit entire pkt
- If channel sensed busy, defer transmission
  - Persistent CSMA: retry immediately with probability p when channel becomes idle (may cause instability)
  - Non-persistent CSMA: retry after random interval
- human analogy: don't interrupt others!

DL: CSMA collisions

collisions *can* occur:
propagation delay means two nodes may not hear each other's transmission

collision:
entire packet transmission time wasted

note:
role of distance and propagation delay in determining collision prob.



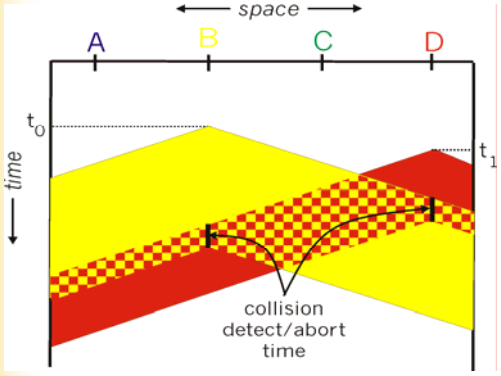
DL: CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- persistent or non-persistent retransmission

- collision detection:
  - For wired LANs: measure signal strengths, compare transmitted, received signals

DL: CSMA/CD collision detection



DL: CSMA/CD problems

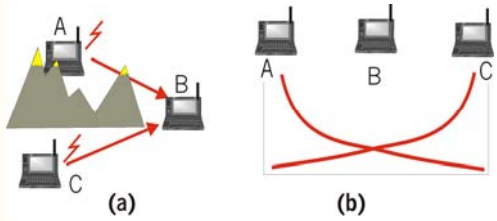
- Can CSMA/CD work over wireless LANs?

– Difficult in wireless LANs: receiver shut off while transmitting

– Hidden terminal problem

DL: Hidden Terminal effect

- A, C cannot hear each other
  - obstacles, signal attenuation
  - collision at B
  - goal: avoid collisions at B



DL: CSMA/CA

- Use base CSMA
- Add acknowledgements
  - Receiver acknowledges receipt of data
  - Avoids hidden terminal problem
- Avoid collisions explicitly
  - Sender explicitly indicates length of time its frame will be transmitted
    - Others hearing frame back off
  - Channel reservation
    - Sender sends “request-to-send” (RTS) messages
    - Receiver sends “clear-to-send” (CTS) messages
- Used in 802.11 wireless LAN networks

DL: “Taking Turns” MAC protocols

channel partitioning MAC protocols:

- share channel efficiently at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols

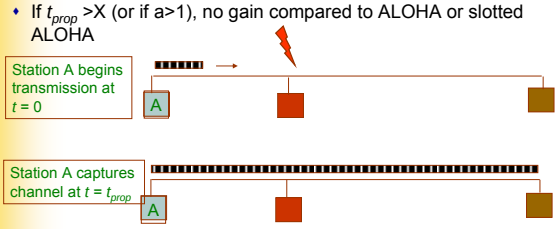
- efficient at low load: single node can fully utilize channel
- high load: collision overhead

“taking turns” protocols

look for best of both worlds!

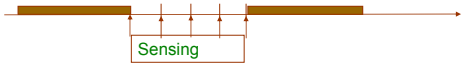
Carrier Sensing Multiple Access (CSMA)

- A station senses the channel before it starts transmission
  - If busy, either wait or schedule backoff (different options)
  - If idle, start transmission
  - Vulnerable period is reduced to t_{prop} (due to *channel capture* effect)
  - When collisions occur they involve entire frame transmission times
  - If t_{prop} >X (or if a>1), no gain compared to ALOHA or slotted ALOHA

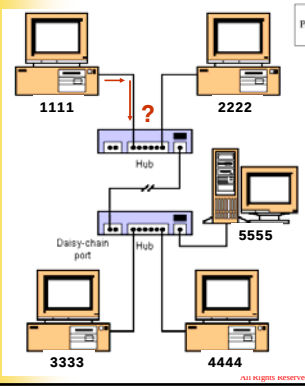


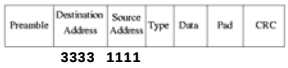
CSMA Options

- Transmitter behavior when busy channel is sensed
  - 1-persistent CSMA (most greedy)
    - Start transmission as soon as the channel becomes idle
    - Low delay and low efficiency
  - Non-persistent CSMA (least greedy)
    - Wait a backoff period, then sense carrier again
    - High delay and high efficiency
  - p-persistent CSMA (adjustable greedy)
    - Wait till channel becomes idle, transmit with prob. p; or wait one mini-slot time & re-sense with probability 1-*p*
    - Delay and efficiency can be balanced



Sending and receiving Ethernet frames via a hub

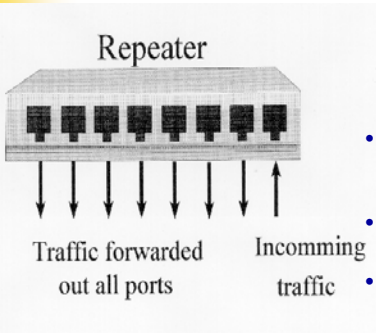




- So, what does a hub do when it receives information?
- Remember, a hub is nothing more than a multiport repeater.

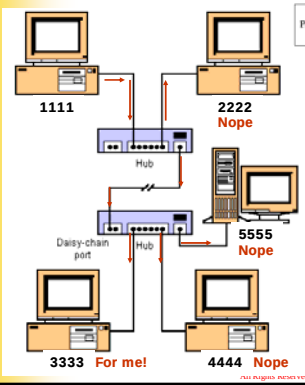
Sending and receiving Ethernet frames via a hub

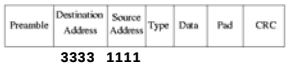
Hub or



- Only one device on the hub can communicate at a time, otherwise collisions occur.
- 10 Mbps ports are the most common.
- 100/1000 Mbps also “available”.
- The hub acts the same as a “bus”.

Sending and receiving Ethernet frames via a hub





- The hub will **flood** it out all ports except for the incoming port.
- Hub is a layer 1 device.
- A hub does NOT look at layer 2 addresses, so it is fast in transmitting data.
- Disadvantage with hubs: A hub or series of hubs is a single **collision domain**.
- A collision will occur if any two or more devices transmit at the same time within the collision domain.
- More on this later.

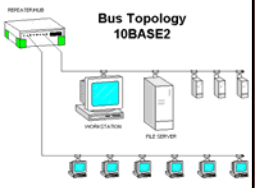
Another detour…
OSI Layer 1 – Physical Layer

- The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.
- Signals, network media (cables, wireless, …), layer 1 devices
- Layer 1 devices include:
  - Repeaters
  - Hubs

Binary Transmission
- Wires, connectors, voltages, data rates

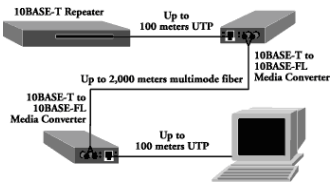
Repeaters

Medium	Max Distance
Twisted Pair	100 meters
Coaxial Cable	185/500 meters
Fiber Optic	2+ kilometers



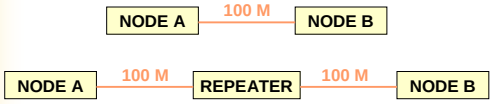
- Signals can only travel so far through media before they weaken, and become garbled.
- This weakening of signals is called **attenuation**.
- Attenuation increases when:
  - Media distances are lengthened
  - Nodes are added to the media

The Repeater



- Repeaters are Layer 1 internetwork devices used to combat attenuation.
- Repeaters:
  - take in weakened signals
  - clean them up
  - regenerate them
  - send them on their way along the network

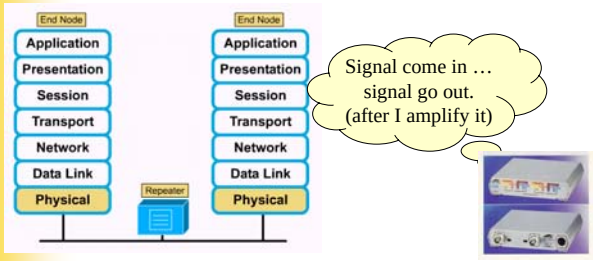
Repeaters Extend Distances



By using repeaters, the distance over which a network can operate is extended.

Example: 10Base-T (a wiring standard) is allowed to run 100 meters. One repeater can double this distance to 200 meters!

Repeater: Layer 1 Device



- **Repeaters** are Layer 1 devices.
- They do **NOT** look at Layer 2, Data Link (MAC, Ethernet) addresses or Layer 3, IP Addresses.

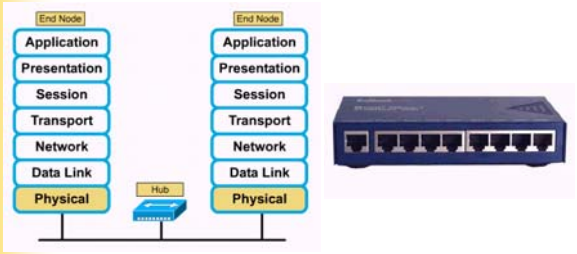
Hub

- **Hub** is nothing but a multiport repeater.
- Hubs are Layer 1 devices.
- Data that comes in one port is sent out all other ports, except for the port it came in on.

Hubs are sometimes called

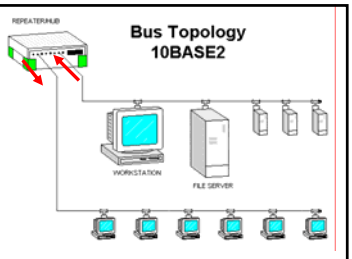
- Ethernet concentrators
- Multiport repeaters
- In Token Ring nets, Multi-station Access Units (MAU or MSAU)

Hub: Layer 1 Device



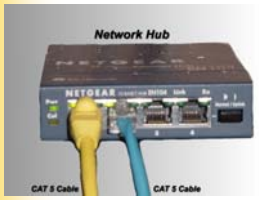
- Hubs are Layer 1 devices.
- They do **NOT** look at Layer 2, Data Link (MAC, Ethernet) addresses or Layer 3, IP Addresses.

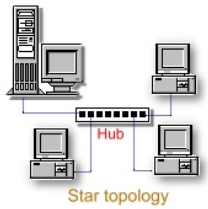
Repeaters



- In the “old days”, repeaters were typically used to extend the size or length of a **bus-topology** network.
- Repeaters take a signal in on one end and regenerate that signal out the other end.
- In most networks (LANs), **repeaters** have been replaced by **hubs**, which have been mostly replaced by **switches**.
- MORE LATER!

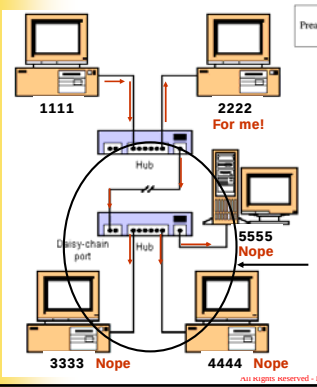
Hubs

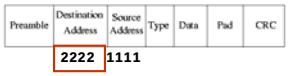




- Hubs allow computers and other network devices to communicate with each other, and use a **star topology**.
- Like a repeater, a hub **regenerates** the signal.
- Hubs have the same disadvantage as a repeater, anything it receives on one port, it **FLOODS** out all other ports.
- Wherever possible, hubs should be replace by **switches**.
- More LATER!

Sending and receiving Ethernet frames via a hub

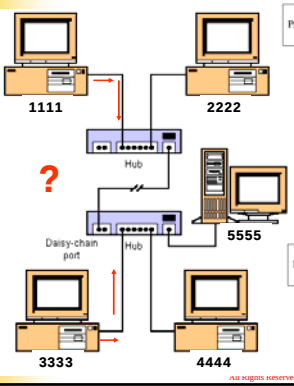


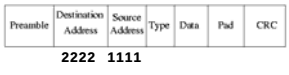


- Another disadvantage with hubs is that is take up unnecessary bandwidth on other links.

Wasted bandwidth

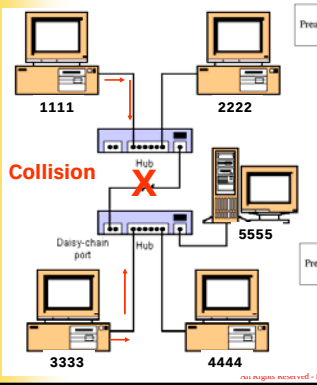
Sending and receiving Ethernet frames via a hub

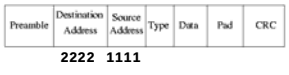




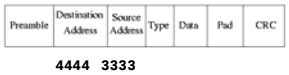
- What happens when two host on the same hub, or when multiple hubs are connected, transmit at the same time?

Sending and receiving Ethernet frames via a hub

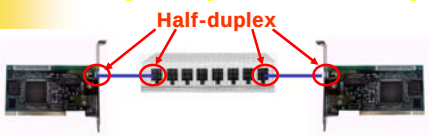




- Collision occurs.
- Although, hubs have little latency, CSMA/CD requires resending of frames and adds latency



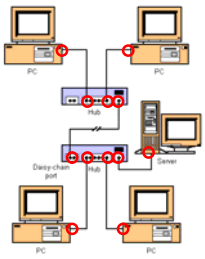
Half-duplex (Introduction)



- Hubs operate only in Half-duplex.
- **Half-duplex** means that only one end can send at a time.
- The other end of the link, Ethernet NIC or another Hub (or switch – later) must also be in Half-duplex mode
- With half-duplex NICs, a host can only transmit or receive, not both at the same time, or a collision will occur.
- When multiple devices are connected to a hub or series of hubs, only one device can transmit.
- Uses CSMA/CD.
- If the a carrier is detected, then the NIC will not transmit.
- Ethernet hubs and repeaters can only operate in half-duplex mode.

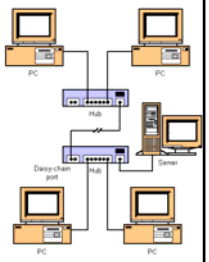
Half-Duplex mode

- All of these Ethernet NICs and ports on the hubs are operating in Half-Duplex mode.
- When multiple devices are connected to a hub or series of hubs, only one device can transmit.

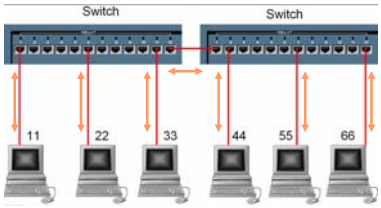


Collision Domain: Shared Access

- **Collision domain (**Wikipedia)**:** A group of Ethernet or Fast Ethernet devices in a CSMA/CD LAN that are connected by repeaters/hubs and compete for access on the network.
  - Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions.
  - A collision domain is sometimes referred to as an Ethernet segment.
- If you connect several computers to a single medium that is only connected by ***repeaters and hubs (Layer 1 devices***), you have a shared-access situation, and you have a single **collision domain**.

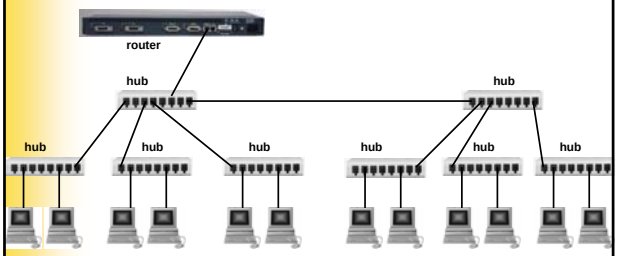


Full-duplex (More in next section)

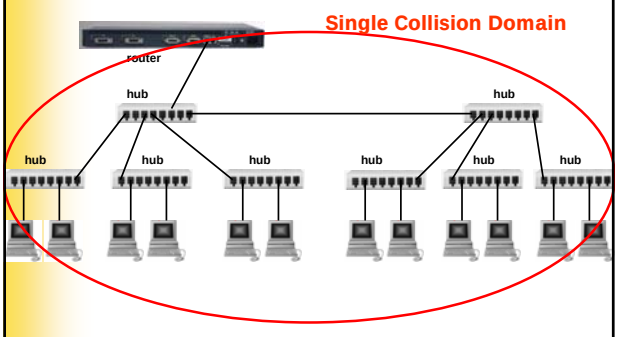


- **Full-duplex** is allows simultaneous communication between a pair of stations or devices.
- Full-duplex allows devices to send and receive at the same time.
- Both ends of the link must be in full-duplex mode.
- Most **switches** operate at either full-duplex but can operate in half-duplex.
- If a hub is connected to a switch, the switch port must be in half-duplex.
- The collision domain will end at the switch port.

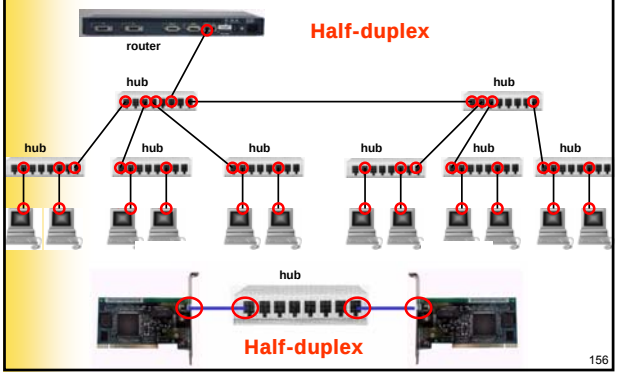
Where are the collision domains? What would be the duplex settings?



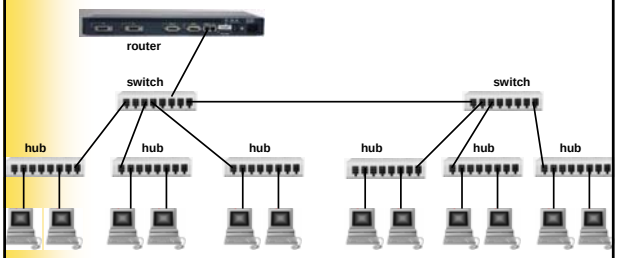
Where are the collision domains?



What would be the duplex settings?

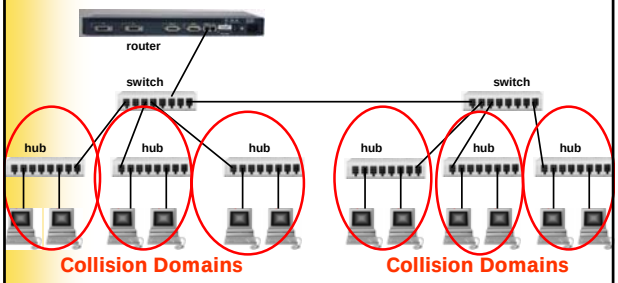


Where are the collision domains?
What would be the duplex settings?



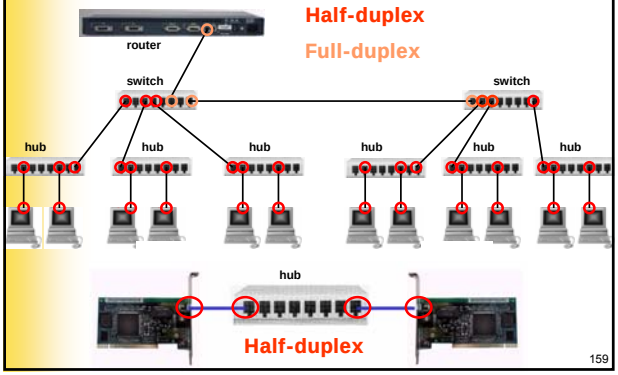
157

Where are the collision domains?
What would be the duplex settings?



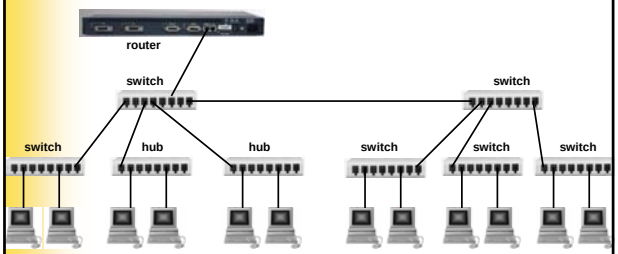
158

What would be the duplex settings?



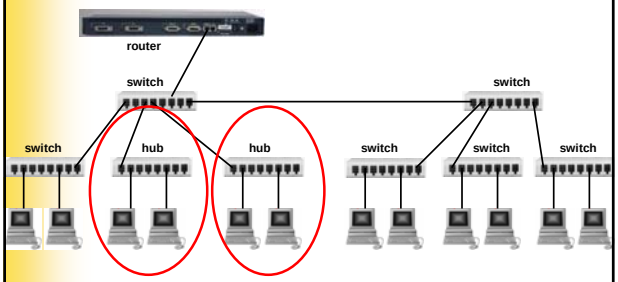
159

Where are the collision domains?
What would be the duplex settings?



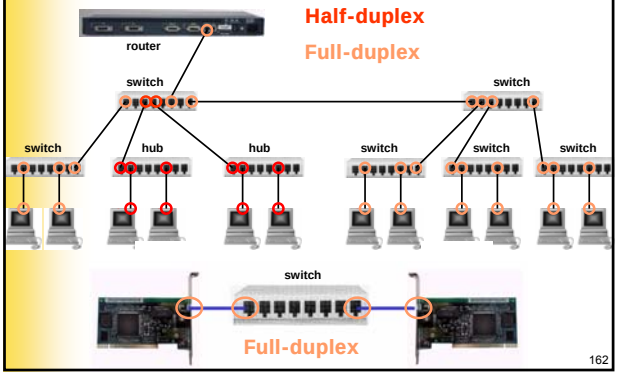
160

Where are the collision domains?



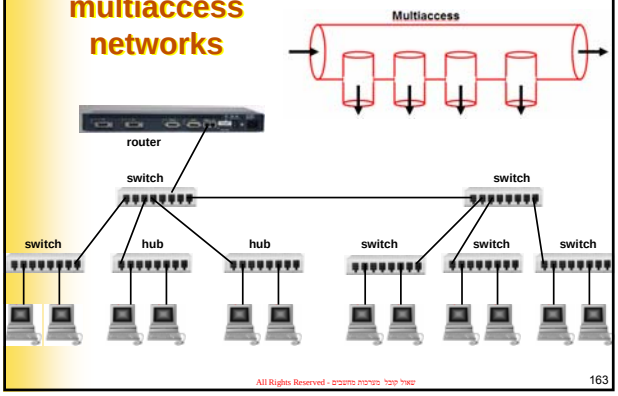
161

What would be the duplex settings?

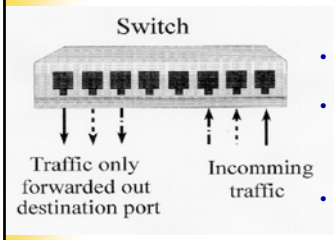


162

All scenarios are multiaccess networks



Sending and receiving Ethernet frames via a switch



- Layer 2 device (also includes layer 1) which examines and bases its decisions on the information in layer 2 frames
- **Switch ports typically operate in full-duplex.**
- Multiple devices on the switch can communicate at a time, otherwise collisions occur.
- 10/100 Mbps ports are the most common.
- 1000 Mbps also are also common, usually connecting to another switch or router.

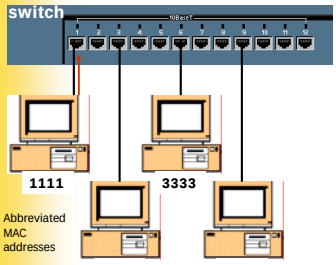
Sending and receiving Ethernet frames via a switch

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111



- Switches are also known as **learning bridges** or **learning switches**.
- A switch has a source address table in cache (RAM) where it stores source MAC address after it learns about them.
- A switch receives an Ethernet frame it searches the source address table for the Destination MAC address.
- If it finds a match, it **filters** the frame by only sending it out that port.
- If there is not a match if **floods** it out all ports.

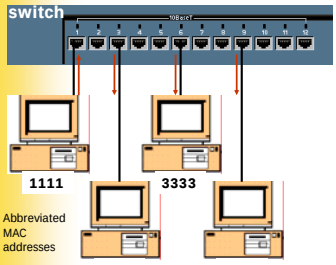
No Destination Address in table, Flood

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111



- How does it learn source MAC addresses?
- First, the switch will see if the SA (1111) is in it's table.
- If it is, it resets the timer (more in a moment).
- If it is NOT in the table it adds it, with the port number.
- Next, in our scenario, the switch will **flood** the frame out all other ports, because the DA is not in the source address table.

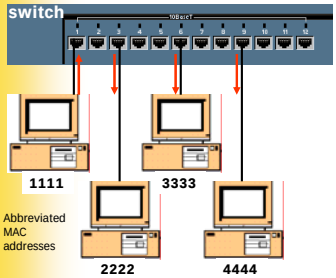
Destination MAC Address: Filter or Flood

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111		

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

3333 1111



- Next, the switch examines the source address table for the **Destination MAC address**.
- If it finds a match, it **filters** the frame by only sending it out that port.
- If there is **not** a match if **floods** it out all ports.
- In this scenario, the switch will **flood** the frame out all other ports, because the **Destination Address** is **not** in the source address table.

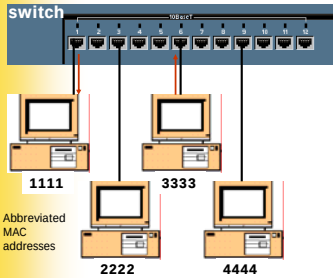
Destination Address in table, Filter

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333

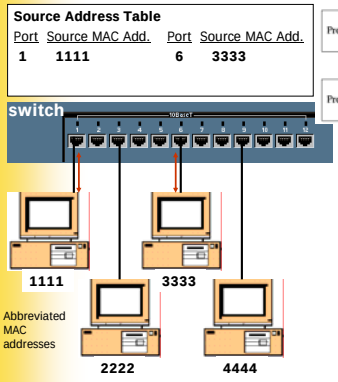
Preamble	Destination Address	Source Address	Type	Data	Pad	CRC

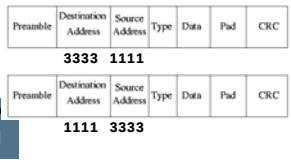
1111 3333



- Most communications involve some sort of client-server relationship or exchange of information. (You will understand this more as you learn about TCP/IP.)
- Now 3333 sends data back to 1111.
- The switch sees if it has the SA stored.
- It does NOT so it adds it. (This will help next time 1111 sends to 3333.)
- Next, it checks the DA and in our case it can **filter** the frame, by sending it only out port 1.

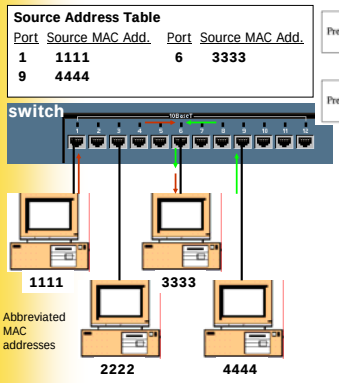
Destination Address in table, Filter

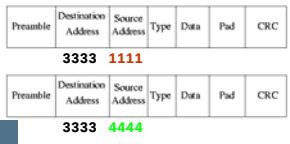




- Now, because both MAC addresses are in the switch's table, any information exchanged between 1111 and 3333 can be sent (filtered) out the appropriate port.
- **What happens when two devices send to same destination?**
- **What if this was a hub?**
- **Where is (are) the collision domain(s) in this example?**

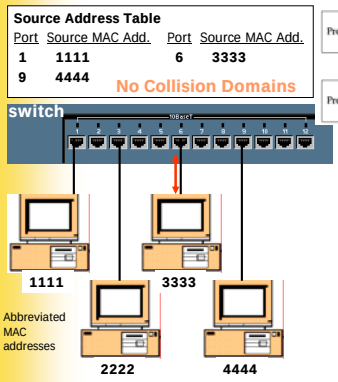
No Collisions in Switch, Buffering

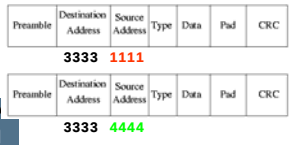




- Unlike a hub, a collision does NOT occur, which would cause the two PCs to have to retransmit the frames.
- Instead the switch buffers the frames and sends them out port #6 one at a time.
- The sending PCs have no idea that their was another PC wanting to send to the same destination.

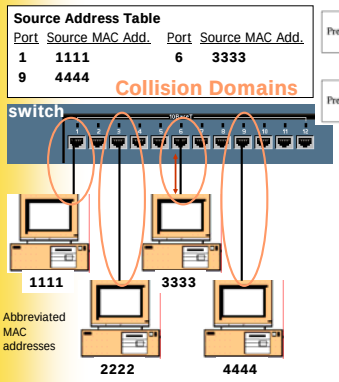
Full Duplex – No collisions

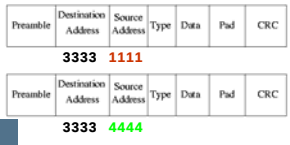




- When there is only one device on a switch port, the collision domain is only between the PC and the switch, which is non-existent with full-duplex.
- With a **full-duplex** PC and switch port, there will be no collision, since the devices and the medium can send and receive at the same time.

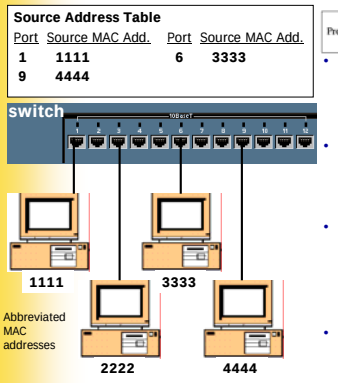
Collision Domains

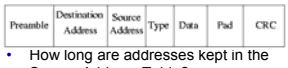




- When there is only one device on a switch port, the collision domain is only between the PC and the switch. (Cisco curriculum is inaccurate on this point.)
- With a **full-duplex** PC and switch port, there will be no collision, since the devices and the medium can send and receive at the same time.

Other Information



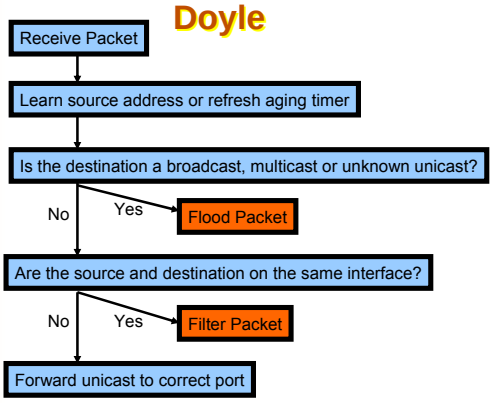


- How long are addresses kept in the Source Address Table?
  - 5 minutes is common on most vendor switches.
- How do computers know the Destination MAC address?
  - ARP Caches and ARP Requests (later)
- How many addresses can be kept in the table?
  - Depends on the size of the cache, but 1,024 addresses is common.
- What about Layer 2 broadcasts?
  - Layer 2 broadcasts (DA = all 1's) is flooded out all ports.

Side Note - Transparent Bridging

- Transparent bridging (normal switching process) is defined in IEEE 802.1d describing the five bridging processes of:
  - learning
  - flooding filtering
  - forwarding
  - aging
- These will be discussed further in STP (Spanning Tree Protocol)

Transparent Bridge Process - Jeff Doyle



Switch Process – Another Look

For every frame that enters a switch…

- Learning Stage (Building/Updating of SAT/MAC table)
  - Examines **Source MAC Address**:
    - If **Source MAC Address** is in the SAT/MAC table, update 5 minute timer
    - If **Source MAC Address** is NOT in the SAT/MAC table, add Source MAC Address and incoming port number to SAT/MAC table
- Forwarding Stage (Flood or Filter)
  - Examines **Destination MAC Address**:
    - If **Destination MAC Address** is in the SAT/MAC table, forward the frame only out that port (**Filter**), unless it is the outgoing port is the same as the incoming port (checks Source MAC Address)

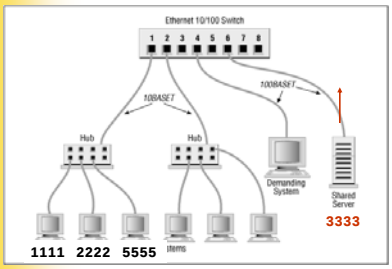
What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
1	2222	1	3333

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	1111	3333				

- Notice the Source Address Table has multiple entries for port #1.

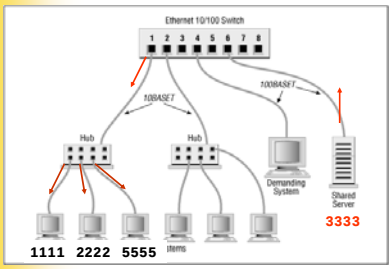


What happens here?

Source Address Table

Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333 Reset timer
1	2222 Filter	1	5555

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	1111	3333				



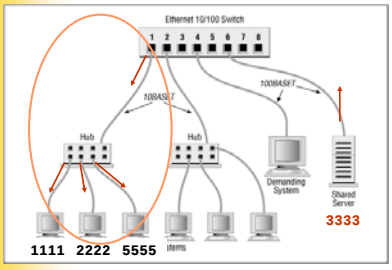
- The switch **resets the 5 minute timer** on the source port entry.
- The **switch filters** the frame out port #1.
- But the hub is only a layer 1 device, so a **hub floods** it out all ports.
- Where is the collision domain?

What happens here?

Source Address Table

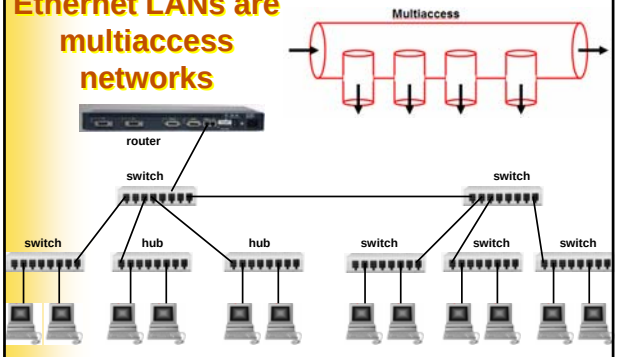
Port	Source MAC Add.	Port	Source MAC Add.
1	1111	6	3333
1	2222	1	5555

Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
	1111	3333				

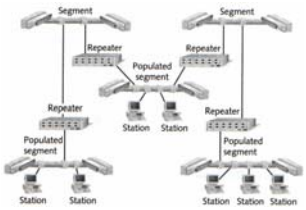


Collision Domain

Ethernet LANs are multiaccess networks



5-4-3 rule



- "The rule mandates that between any two nodes on the network, there can only be a maximum of **five** segments, connected through **four** repeaters, or *concentrators*, and only **three** of the five segments may contain user connections." Webopedia.com
- Note: This is really no longer an issues with switched networks.

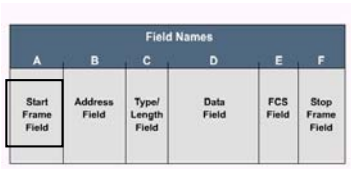
5-4-3 Rule – Webopedia.com

Ethernet and IEEE 802.3 implement a rule, known as the *5-4-3 rule*, for the number of repeaters and segments on shared access Ethernet backbones in a tree topology. The 5-4-3 rule divides the network into two types of physical segments: populated (user) segments, and unpopulated (link) segments. User segments have users' systems connected to them. Link segments are used to connect the network's repeaters together. The rule mandates that between any two nodes on the network, there can only be a maximum of **five** segments, connected through **four** repeaters, or *concentrators*, and only **three** of the five segments may contain user connections.

The Ethernet protocol requires that a signal sent out over the LAN reach every part of the network within a specified length of time. The 5-4-3 rule ensures this. Each repeater that a signal goes through adds a small amount of time to the process, so the rule is designed to minimize transmission times of the signals.

The 5-4-3 rule -- which was created when Ethernet, 10Base5, and 10Base2 were the only types of Ethernet network available -- only applies to shared-access Ethernet backbones. A switched Ethernet network should be exempt from the 5-4-3 rule because each switch has a buffer to temporarily store data and all nodes can access a switched Ethernet LAN simultaneously.

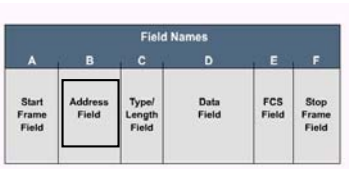
Generic Data Link Frame Format



Start Field

- When computers are connected to a physical medium, there must be a way they can grab the attention of other computers to broadcast the message, "Here comes a frame!"
- Various technologies have different ways of doing this process, but all frames, regardless of technology, have a beginning signaling sequence of bytes.

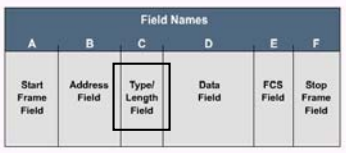
Generic Data Link Frame Format



Address Field

- We saw how IEEE 802.3 uses Destination and Source Addresses.
- BTW: Any idea how a serial data link frame is addressed?
  - Dedicated Links - Broadcast
  - Non-broadcast Multiple Access (NBMA), Frame Relay - DLCIs

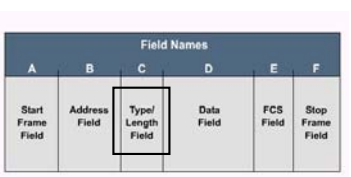
Generic Data Link Frame Format



Type Field

- Usually information indicating the layer 3 protocols in the data field, I.e. IP Packet.
- Type field values of particular note for IEEE 802.3 frames include:
  - 0x0600 XNS (Xerox)
  - 0x0800 IP (the Internet protocol)
  - 0x8137 Novell NetWare packet formatted for Ethernet II
  - 0x6003 DECNET

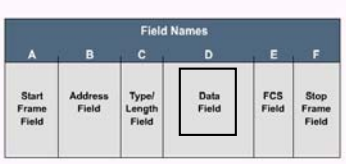
Generic Data Link Frame Format



Length Field

- In some technologies, a length field specifies the exact length of a frame.

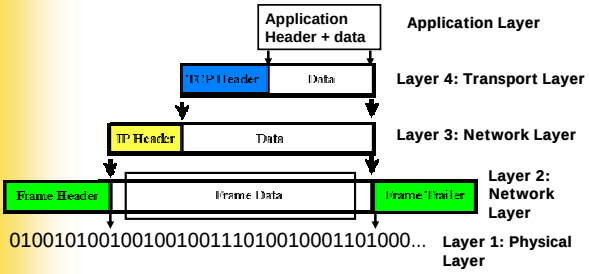
Generic Data Link Frame Format



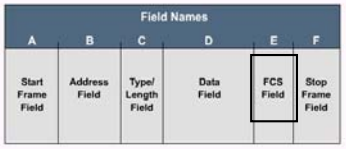
Data Field

- Included along with this data, you must also send a few other bytes.
- They are called *padding bytes*, and are sometimes added so that the frames have a minimum length for timing purposes.
- LLC bytes are also included with the data field in the IEEE standard frames. (later)

Data Encapsulation Example



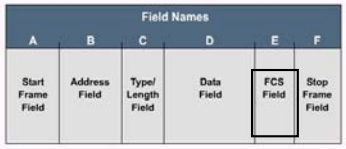
Generic Data Link Frame Format



FCS

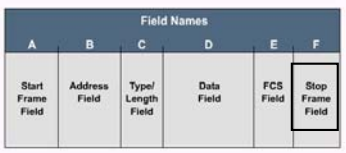
- Used to insure that the data has arrived without corruption.
- More efficient than sending the data twice and comparing the results.
- Necessary to prevent errors.

Three Kinds of FCS



- **Cyclic redundancy check (CRC)**
  - **performs polynomial calculations on the data**
- **Two-dimensional parity**
  - **adds an 8th bit that makes an 8-bit sequence have an odd or even number of binary 1s**
- **Internet checksum**
  - **adds the numbers to determine a number**

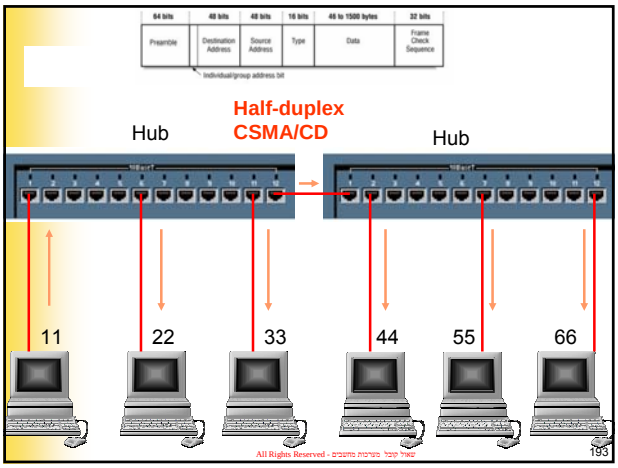
Generic Data Link Frame Format



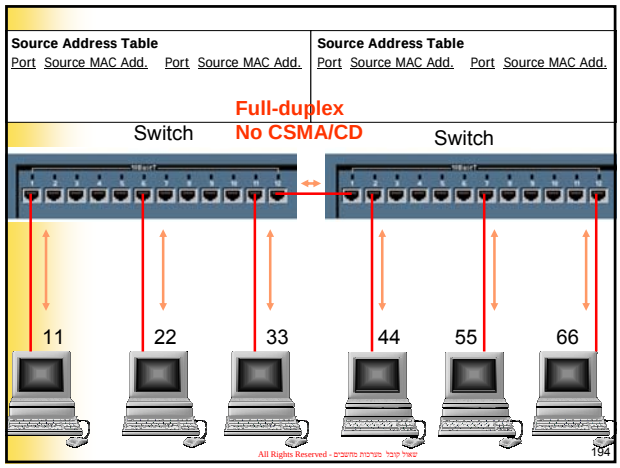
Stop Field

- The computer that transmits data must get the attention of other devices, in order to start a frame, and then claim it again, to end the frame.
- The length field implies the end, and the frame is considered ended after the FCS.
- Sometimes there is a formal byte sequence referred to as an end-frame delimiter.

HALF / FULL DUPLEX

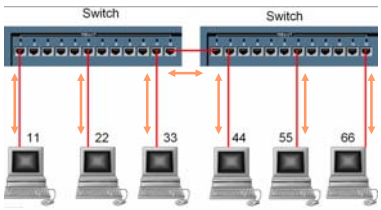


193



194

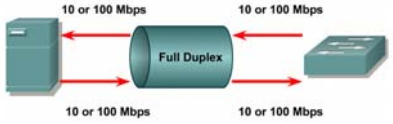
Full-duplex



- **Full-duplex** is an optional mode of operation allowing simultaneous communication between a pair of stations or devices.
- Specified in IEEE 802.3x in March 1997

195

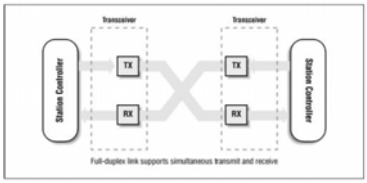
Full-duplex



- Full-duplex Ethernet allows the transmission of a packet and the reception of a different packet at the same time.
- The full-duplex Ethernet switch takes advantage of the two pairs of wires in the cable by creating a direct connection between the transmit (TX) at one end of the circuit and the receive (RX) at the other end.
- **Half Duplex Ethernet** usually can only use **50%-60%** of the available 10 Mbps of bandwidth because of **collisions** and **latency**.
- **Full-duplex Ethernet** offers **100% of the bandwidth in both directions**.
  - 10 Mbps Ethernet: This produces a potential 20 Mbps throughput, which results from 10 Mbps TX and 10 Mbps RX.

196

Full-duplex

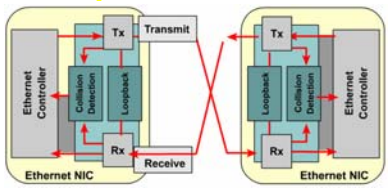


- **IEEE 802.3x** full-duplex standard requires:
  - The medium must have **independent transmit and receive** data paths that can operate simultaneously.
  - There are **exactly two stations** connected with a full-duplex point-to-point link.
    - There is **no CSMA/CD** multiple access algorithm, since there is no contention for a shared medium.
  - **Both stations** on the LAN are capable of, and have been configured to use, the **full-duplex mode of operation**.
- Ethernet **hubs and repeaters** can only operate in **half-duplex** mode.

197

Half-duplex Controller

Half-duplex controllers



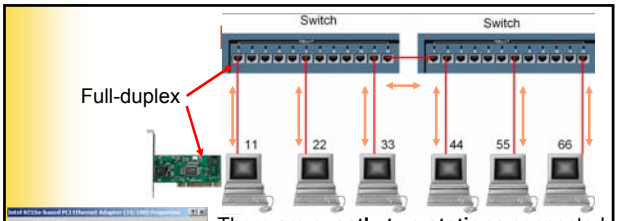
- With **half-duplex** NICs,a host can only **transmit or receive**.
- If the a carrier is detected, then the NIC will not transmit.
- In full-duplex the station ignores the carrier sense and does not defer to traffic being received on the channel.
- In full-duplex, the station ignores any collision detect signals that come from the transceiver.
- Ethernet hubs and repeaters can only operate in half-duplex mode.

198

Full-duplex

Etherne t Frame	IFG	Etherne t Frame	IFG	Etherne t Frame	IFG	Etherne t Frame	IFG

- Both half-duplex and full-duplex Ethernet uses an interframe gap (IFG).
- Full-duplex uses the IFG to ensure that the interfaces at each end of the link can keep up with the full frame rate of the link.
- **CSMA/CD not used** in **full-duplex Ethernet**:
  - **No CS (Carrier Sense)** – In full-duplex the station ignores carrier sense since it can *send whenever it likes*.
  - **No MA (Multiple Access)** – Since there is *only one station at the other end of the link* and the Ethernet channel between them is not the subject of access contention.
  - **No CD (Collision Detect)** – Since there is *no access contention*, there will be no collisions, and station can ignore CD.



There are **exactly two stations** connected with a full-duplex point-to-point link.

Both stations on the LAN are capable of, and have been configured to use, the **full-duplex mode of operation**.

Typically:

- Host-to-Switch
- Switch-to-Switch
- Switch-to-Router

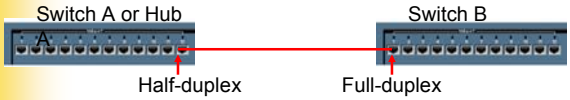
When to Use Ethernet 10/100Mb Auto-Negotiation

- **Auto-negotiation** is an optional function of the ***IEEE 802.3u Fast Ethernet standard*** that enables devices to automatically exchange information over a link about speed and duplex abilities.
- Auto-negotiation is targeted at ports which are allocated to areas where transient users or devices connect to a network.
  - For example, many companies provide shared offices or cubes for Account Managers and System Engineers to use when they are in the office rather than on the road.
  - Each office or cube will have an Ethernet port permanently connected to the office's network.
- Because it may not be possible to ensure that every user has either a 10Mb, a 100Mb Ethernet, or a 10/100Mb card in their laptop, the switch ports that handle these connections must be able to **negotiate their speed and duplex mode**.
- The **alternative** would be to provide both a 10Mb and a 100Mb port in each office or cube and label them accordingly.

When to Use Ethernet 10/100Mb Auto-Negotiation

- **One of the most common causes of performance issues** on 10/100Mb Ethernet links is when one port on the link is operating at half-duplex while the other port is operating at full-duplex.
  - This occasionally happens when one or both ports on a link are reset and the auto-negotiation process doesn't result in both link partners having the same configuration.
  - It also happens when users reconfigure one side of a link and forget to reconfigure the other side.
- Both sides of a link should have auto-negotiation on, **or** both sides should have it off.
- Our **current recommendation** is to leave auto-negotiation on for those devices compliant with 802.3u.
- Many performance-related support calls will be avoided by correctly configuring auto-negotiation.

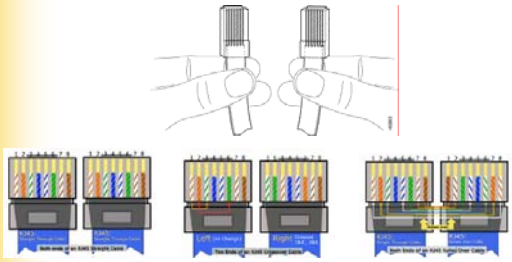
Half-duplex, Full-duplex Issue



- Switch A, the half-duplex end will sense a neutral carrier and send frames
- Switch B, the full-duplex end, senses the non-neutral carrier and since it doesn't care because it is configured as full-duplex, it transmits anyways.
- Switch A senses a collision (the half-duplex side) and stops sending the frame.
- Switch B (the full-duplex side) doesn't care and keeps on sending frames.
- Data ends up being transmitted only one-way most of the time, with collisions constantly happening on Switch A, causing performance issues on the network. (Remember, most network communications is bi-directional.
- This is also a common cause for **late collisions** (a collision that occurs after the first 512 bits (slot time) have been sent and the sender believes it has acquired the channel.

Cables, Duplex, Troubleshooting

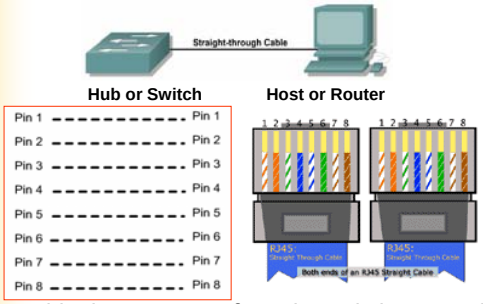
Unshielded Twisted Pair (UTP)



Straight-through Cross-over Rollover

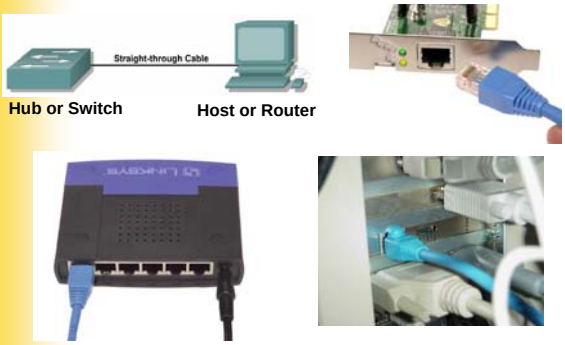
www.cisco.com/warp/ public/701/14.html

UTP Straight-through Cable

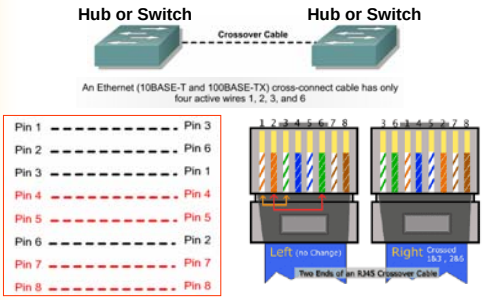


- The cable that connects from the switch port to the computer NIC port is called a straight-through cable.
- Connects unlike devices.

UTP Straight-through Cable

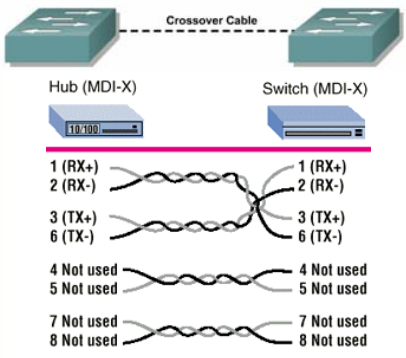


UTP Cross-over Cable

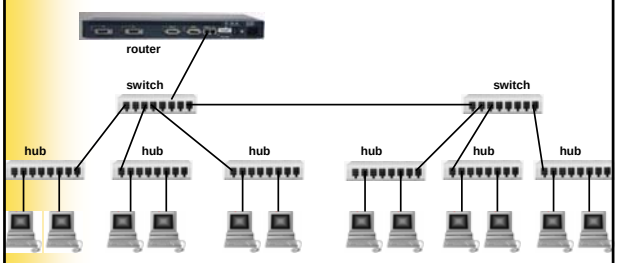


- The cable that connects from one switch port to another switch port is called a crossover cable.
- Connects like devices.

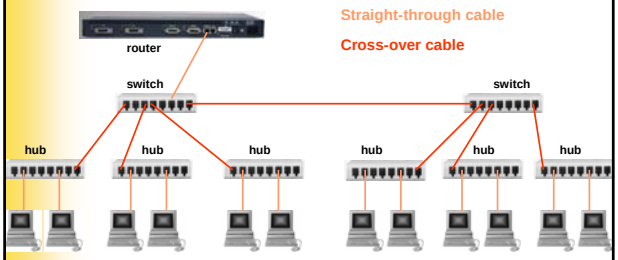
UTP Cross-over Cable



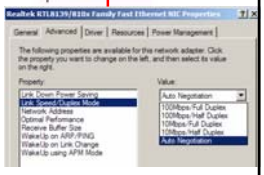
Cabling – Show the straight-through and cross-over cables



Cabling – Show the straight-through and cross-over cables

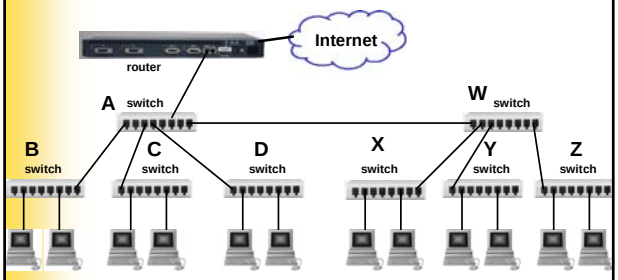


Configuring Speed and Duplex



- Negotiation between NIC and switch port.
  - Duplex: Full-duplex or Half-duplex
  - Speed: 10/100/1000 Mbps
  - Autonegotiation
    - Both sides of a link should have auto-negotiation on, or both sides should have it off.

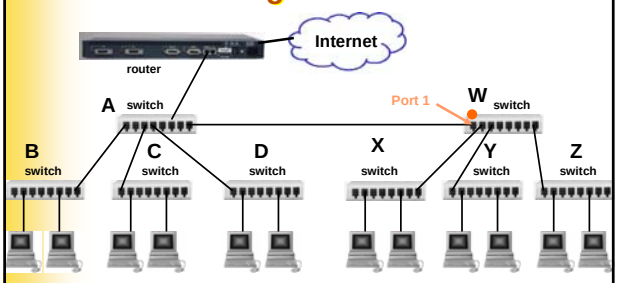
Real World Troubleshooting - Symptom



- Hosts connected to switches B, C and D can reach each other and the Internet with no problems.
- However, hosts on X, Y, and Z can either not access hosts on B, C, and D or the Internet, or if they can it is extremely slow.

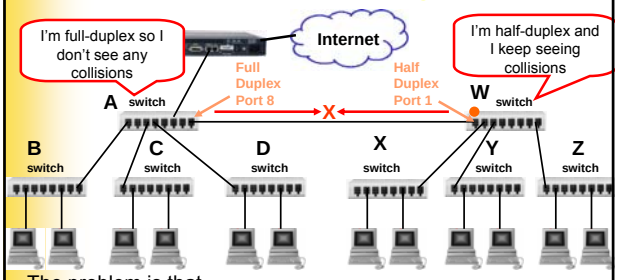
Lights and indicators

Real World Troubleshooting – Diagnostics



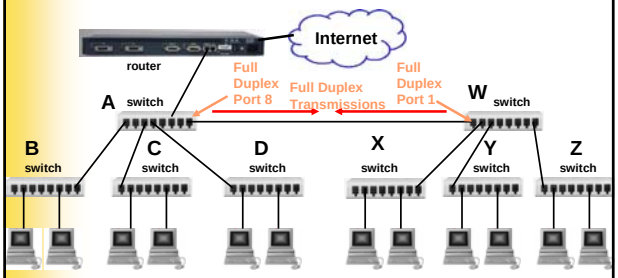
- You notice that a collision light (or looking at some diagnostic output) on Switch W, port 1 is always on indicating a very large number of collisions detected on that port.

Real World Troubleshooting – Problem



- The problem is that
  - Switch A, Port 8 is in Full-duplex mode
  - Switch W, Port 1 is in Half-duplex mode
- Switch A sends whenever it wants to without listening first to see if Switch W is sending.

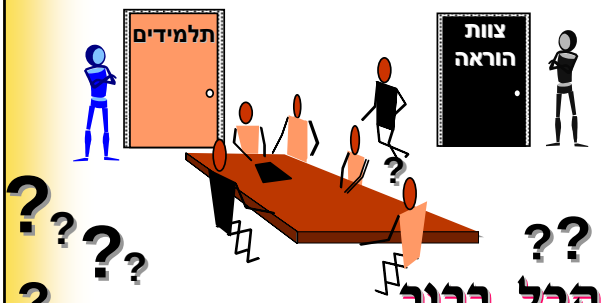
Real World Troubleshooting – Solution



- Configure Switch W, Port 1 to be in full duplex, the same as Switch A, Port A.

217

סיכומים וחזרות לחומר הלימוד



Any Questions ?

הכל ברור

218

219

זה הכול להיום

220

יום שישי 05 מאי 2006

saul@coval.net
http://www.coval.net