TCP/IP Fundamentals

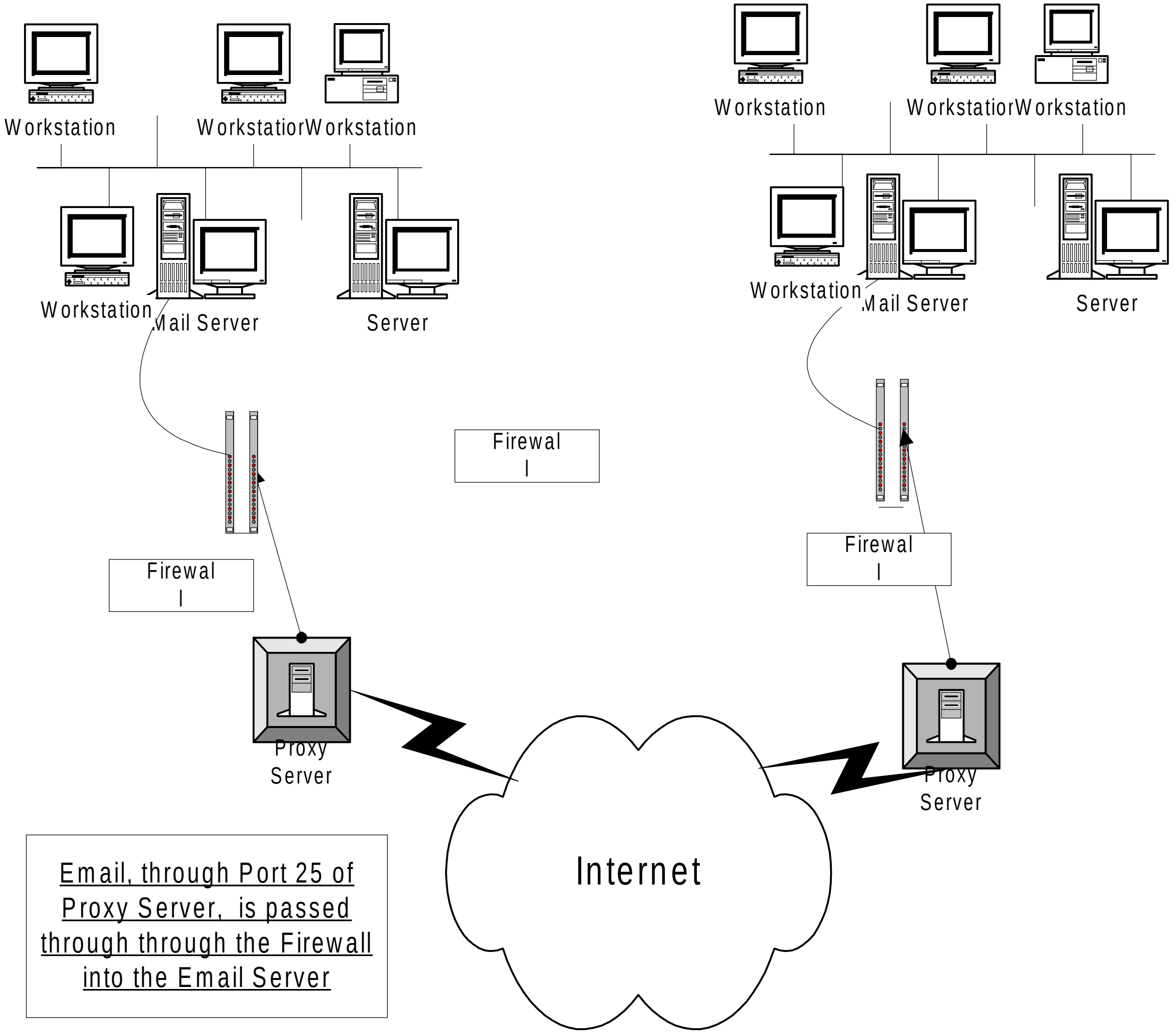
Edmund Lam
IT Audit Manager
University of California
edmund.lam@ucop.edu

What we will discuss:

- TCP/IP related to OSI Layers
- History of TCP/IP and what is it?
- TCP/IP Structure
- IP Address Structure
- IP Address Numbering
- IP Address Subnetting
- IP Routing
- Two Types of Routers
- IP Security Concerns
- IPv6 High Level Discussion

What we will not Discuss:

- Auditing of TCP/IP
- Network Vulnerability
- Internet Security
- Network Troubleshooting



<u>Email, through Port 25 of Proxy Server, is passed through through the Firewall into the Email Server</u>

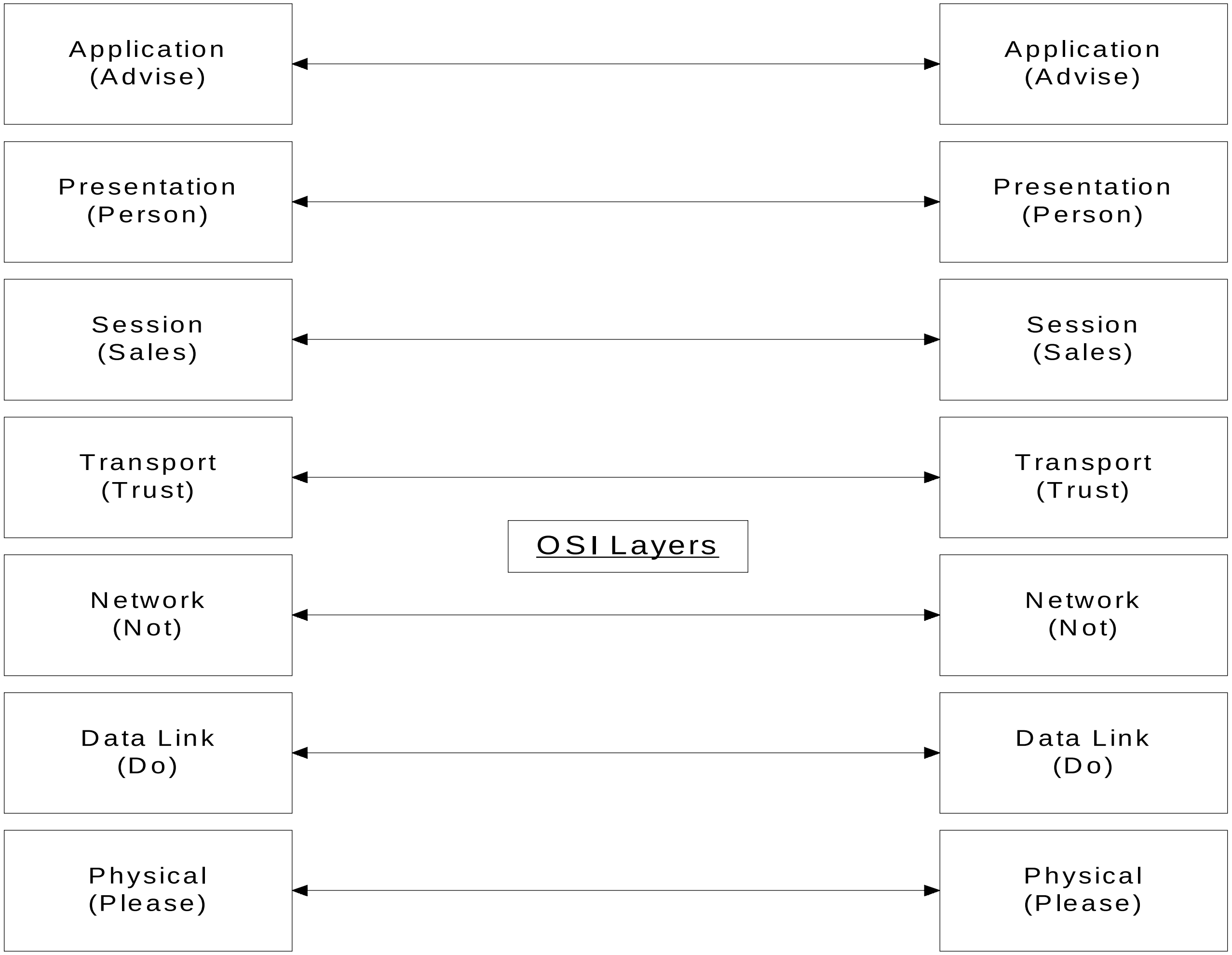
Open Systems Interconnections(OSI) Reference Model

- Physical Layer - Physical Connections between Computers and the network. Converts bits into voltages or light pulse. This defines topology (Connected through repeaters)
- Data Link -- Defines Protocol that Computers must follow. Token Ring, Ethernet (Connected with Bridges)
- Network Layer -- Defines how the small packets of data are routed and relayed. (Connected with Routers)

Open Systems Interconnections(OSI) Reference Model (Cont’d)

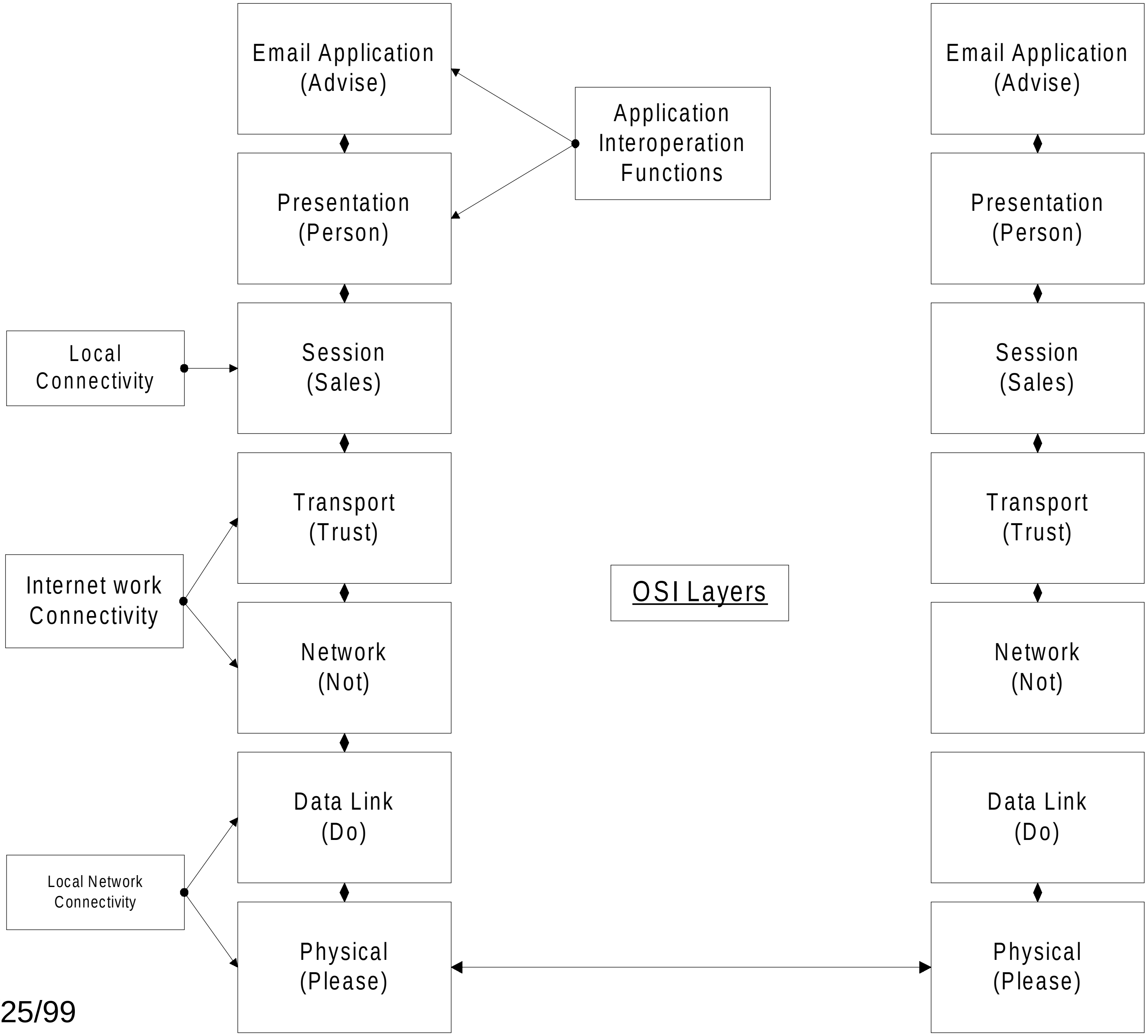
- Transport -- Defines how to address the physical locations/devices on the network.
- Presentation -- Defines how applications can enter the network. This layers allows devices to be referenced as name rather than addresses.
- Application -- Interfaces with users, gets information from databases, and transfer whole files. (Connected through Gateways)

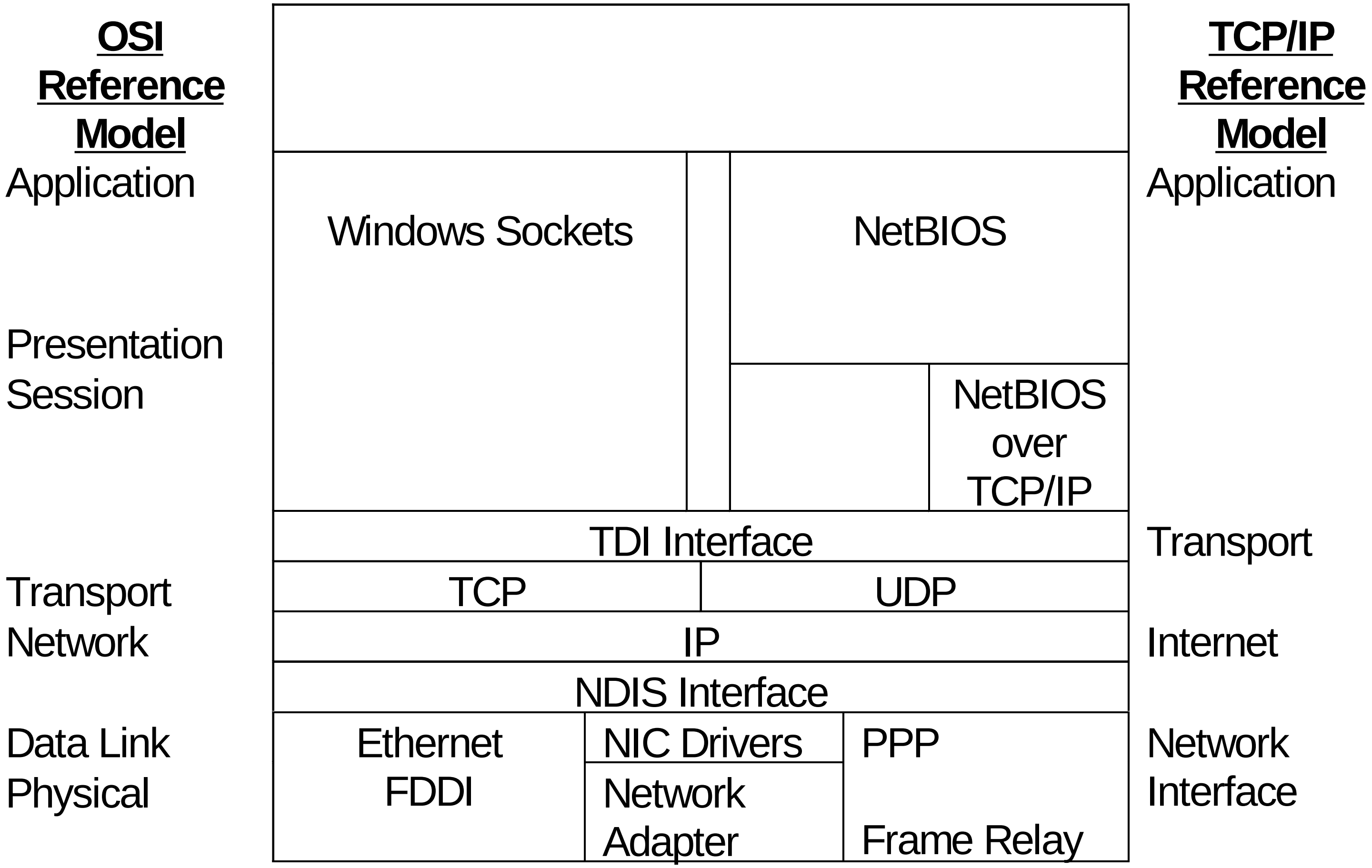
Open System Interconnections Reference Model:



Connectors:

- Physical -- 4 pairs, Fiber Optics, Coax, Network Interface Card
- Datalink -- Token Ring, Ethernet
- Network -- IPX, IP
- Transport -- TCP, UDP, NetBEUI, SPX
- Session -- FTP, Telnet, NCP
- Presentation -- SMB, NCP
- Applications -- Email, Appletalk, NFS


Email Application
(Advise)
Presentation
(Person)
Session
(Sales)
Transport
(Trust)
Network
(Not)
Data Link
(Do)
Physical
(Please)
Application
Interoperation
Functions
Local
Connectivity
Internet work
Connectivity
Local Network
Connectivity
OSI Layers
Email Application
(Advise)
Presentation
(Person)
Session
(Sales)
Transport
(Trust)
Network
(Not)
Data Link
(Do)
Physical
(Please)



OSI Reference Model

Application

Presentation

Session

Transport

Network

Data Link

Physical

Windows Sockets

NetBIOS

NetBIOS over TCP/IP

TDI Interface

TCP

UDP

IP

NDIS Interface

Ethernet
FDDI

NIC Drivers

Network Adapter

PPP

Frame Relay

TCP/IP Reference Model

Application

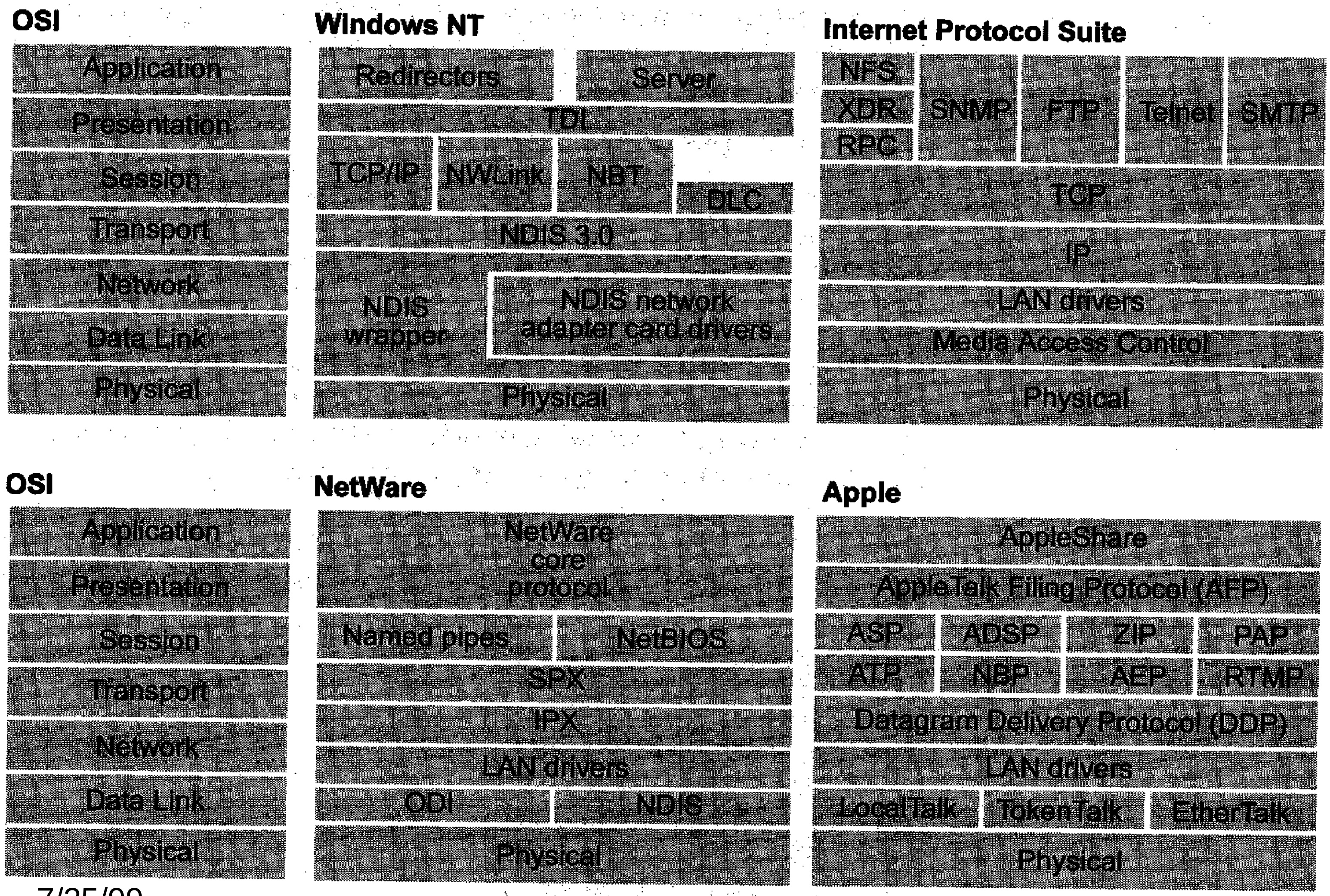
Transport

Internet

Network Interface

Protocol Standards

The OSI model is used to define what protocols should be used at each layer. Products from different vendors that subscribe to this model can communicate with each other.



OSI

Application
Presentation
Session
Transport
Network
Data Link
Physical

Windows NT

Redirectors | Server
TDI
TCP/IP | NWLink | NBT | DLC
NDIS 3.0
NDIS wrapper | NDIS network adapter card drivers
Physical

Internet Protocol Suite

NFS | XDR | RPC | SNMP | FTP | Telnet | SMTP
TCP
IP
LAN drivers
Media Access Control
Physical

OSI

Application
Presentation
Session
Transport
Network
Data Link
Physical

NetWare

NetWare core protocol
Named pipes | NetBIOS
SPX
IPX
LAN drivers
ODI | NDIS
Physical

Apple

AppleShare
AppleTalk Filing Protocol (AFP)
ASP | ADSP | ZIP | PAP
ATP | NBP | AEP | RTMP
Datagram Delivery Protocol (DDP)
LAN drivers
LocalTalk | TokenTalk | EtherTalk
Physical

Three Services that are important:

- DNS -- Domain Name Server (This server provides the translation between IP address and Domain Name e.g. www.abc.com to 121.11.131.11)
- WINS -- Windows Internet Name Service (Microsoft only device to resolve name resolution)
- DHCP -- Dynamic Host Configuration Protocol(A service that enables the assignment of dynamic TCP/IP network addresses, based on a specified pool of available addresses)

TCP/IP

Definition:

An industry standard suite of protocols providing communication in a heterogeneous environment. It provides a routable, enterprise networking protocol and access to the Internet and its resources

TCP/IP History

- DOE commissioned APANET in 1969
- First Telnet specification(RFC 318) in 1972
- File Transfer Protocol(FTP-RFC 454)introduced in 1973
- TCP specified in 1974
- IP standard(RFC -791) published 1981
- Defense Communications Agencies established TCP/IP as a suite in 1982
- Domain Name System (DNS) introduced in 1984

TCP (Transmission Control Protocol)

- Connection - oriented
  - Session is established before exchanging data
- Reliable Delivery
  - Sequence numbers
  - Acknowledgements(ACKs)
- Byte-Stream Communications
- Uses Port Numbers as Endpoints to Communicate

Some of the Well Know TCP Ports:

A TCP port provides a specific location for delivery of TCP Segments. Port Numbers below 1024 are well-known, and are assigned by Internet Assigned Numbers Authority (IANA) – Refer to RFC 1170.

TCP Port Number	Description
20	FTP (Data Channel)
21	FTP (Control Channel)
23	Telnet
25	Email
80	HyperText Transfer Protocol(HTTP) used for the WWW
139	NetBIOS Session Service

TCP Packet Structure:

TCP Source Port - Port of sending host.

Destination Port – Port of End Point Destination.

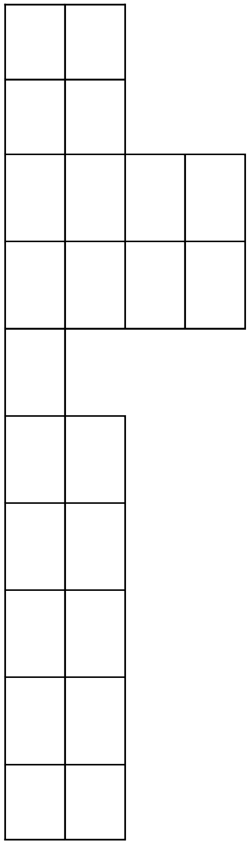
Sequence #. – Sequence of Bytes transmitted in a segment, required to verify all bytes are received.
Acknowledgment Number – The sequence number of the byte the local host expects to receive next.
Data Length – Length of the TCP Segment.

Reserved for Future Use.

Flags – Specified what content is in the segment.

Window – How much space is currently available in the TCP window.
Checksum – Verify that the Header is not corrupted.

Urgent Pointer – When urgent data is being sent.



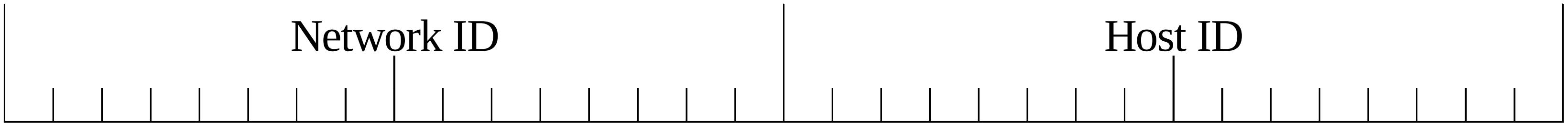
IP Packet Structure

- Source IP Address
- Destination IP Address
- Protocol (Whether to pass up to TCP or UCP)
- Checksum (Verify that the packet arrives intact)
- Time to Live(TTL) (Designates the number of second the datagram is allowed to stay in the network before it is discarded -- NT defaults at 128 Seconds

Who has a UNIQUE IP addresses:

Each Server, workstation, printer, router and other Internet enabled devices

IP Format



Each IP address is a 32 bits long, and is composed of 4 8-bit fields, called Octets. Each Octet represents a decimal number in the range of 0-255. This format is called dotted decimal notation.

E.g.. Binary number as follow:

10000011.01101011.00000011.00011000

Dotted Decimal notation:

131.107.3.24

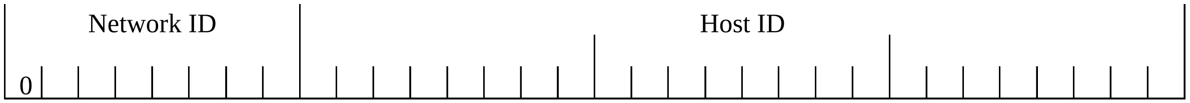
Converting IP Address from Binary to Decimal

1	1	1	1	1	1	1	1

128	64	32	16	8	4	2	1

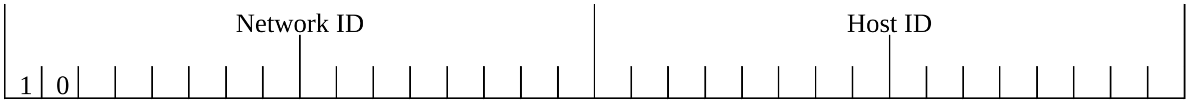
Binary Code	**Bit Values**	**Decimal Value**
00000000	0	0
00000001	1	1
00000011	2+1	3
00000111	4+2+1	7
00001111	8+4+2+1	15
00011111	16+8+4+2+1	31
00111111	32+16+8+4+2+1	63
01111111	64+32+16+8+4+2+1	127
11111111	128+64+32+16+4+2+1	255

Address Classes:



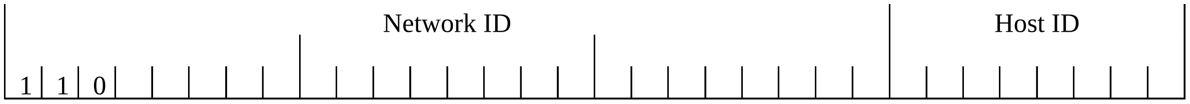
Class A Address Range 0 – 127.X.X.X

N . H . H . H



Class B Address Range 128 – 191.X.X.X

N . N . H . H



Class C Address Range 192 – 233.X.X.X

N . N . N . H

Possible Values for Each Class

	Number of Networks	Number of Hosts per Network	Range of Network Ids (First Octet)
Class A	126	16,777,214	1 –126(Note 1)
Class B	16,384	65,534	128-191(Note 2)
Class C	2,097,152	254	192 – 223 (Note 3)

Note 1 – First Digit in first Octet is a “0”, and 127 is reserved for Loopback function.

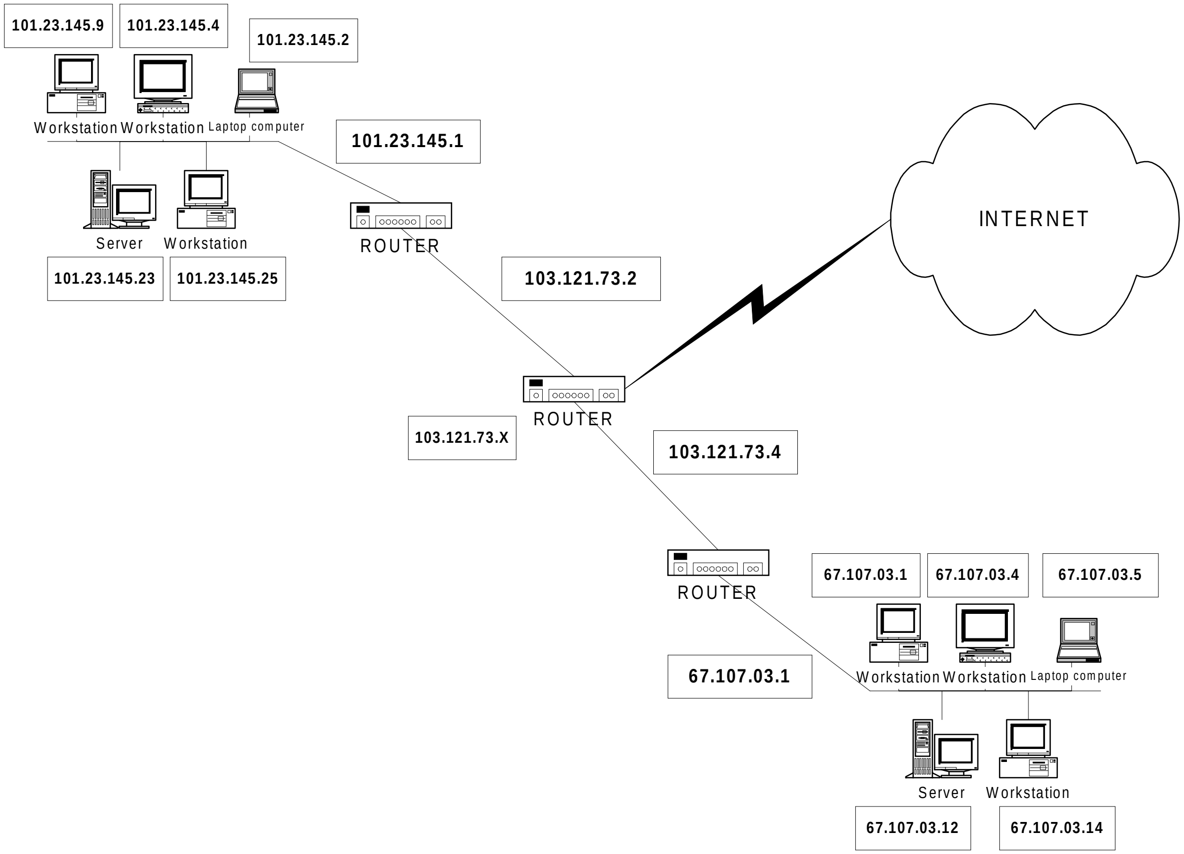
Note 2 – First two Digits in first Octet are “10”.

Note 3 – First three Digits in the first Octet are “110”

Other IP Address Rules:

- Net ID cannot be 127
- Net ID and Host ID cannot be 255(All bits set to 1), it is reserved for broadcast
  - I.e. cannot be 255.255.255.1
- Network ID and Host ID cannot be 0 (All bits set to 0), it means “local network only”
  - I.e. cannot be 0.0.0.0
- Host ID Must be unique to the Network
  - I.e. cannot have two networks on the same physical wire

Typical Network IP Numbering



7/25/99

Subnet Mask:

- A 32 bit address used to:
  - Block out a portion of the IP address to distinguish the network ID from the host ID
  - Specify whether the destination host’s IP address is located on a local or remote network

Default Subnet Mask:

Address Class	Bits Used for Subnet Mask	Network Prefix	Dotted Decimal Notation
Class A	11111111 00000000 00000000 00000000	/8	255.0.0.0
Class B	11111111 11111111 00000000 00000000	/16	255.255.0.0
Class C	11111111 11111111 11111111 00000000	/24	255.255.255.0

- Using a Class B Subnet Mask:
  - IP Address: 045.121.16.23
  - Subnet Mask: 255.255.0.0
  - Network ID: 045.121.x.x/16
  - Host ID: x.x.16.23/16
- All bits that corresponds to the Net ID are 1s
- All bits that corresponds to the Host ID are 0s

Determining the Network IP Address:

IP Address	00101101	01111001	00010000	00010111
Subnet Mask	11111111	11111111	00000000	00000000

Result	00101101	01111001	00000000	00000000

- Use the logic of the AND Gate to calculate the final result to identify the Net ID
  - I.e. 1 and 1 is a 1
  - 1 and 0 is a 0
  - 0 and 0 is a 0
- Network ID -- 045.121.x.x/16
- Host ID - 045.121.16.23/16

Why Subnet?

- As Class A, B, and C IP Addresses are not available, this allows a business/organization to separate networks into different sub-networks as it grows
- Overcome limitations of current technologies, such as exceeding the maximum number of hosts per segments
- Reduce network congestion as traffic grows within or outside business/organizations.

Subnetting Process:

- Determine the number of Required Network Ids
- Determine the number of Required Host Ids per Subnet
- Define One Subnet Mask Based on Requirements
- Define a Unique Subnet ID for Each Physical Segment Based on the Subnet Mask
- Define Valid Hosts Ids for Each Subnet Based on the Subnet ID

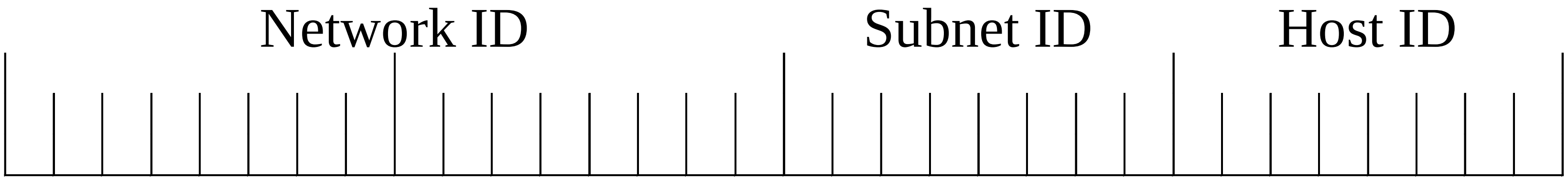
Determine the Number of Networks

- One for each subnet
- One for each wide-area network connections
- Subnetting allows Network Administrator to set up more networks than the number of Class A/B/C IP addresses allows.

Determines the Number of Host Ids per Subnet

- One required for each TCP/IP host
- One required for each router interface
- By limiting the number of Hosts ID on each subnet -- especially for smaller networks, the Network Administrator can implement more networks within the organizations to enhance traffic flow

How Subnet Mask Work?



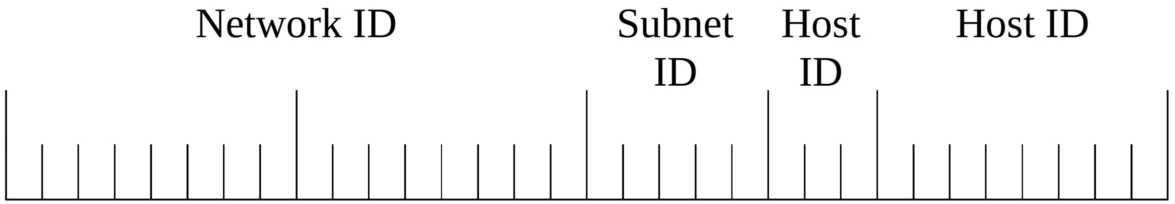
For a normal Class B Address

Number of Network – 1

Number of Subnets – 255 (0 – 254)

Total number of Hosts – 65280 (255 Subnets X 256/Subnet)

Defining Subnet Mask from a Partial Octet



For a normal Class B Address

Subnet Mask : 255.255.248.0 or/21 (2^7+2^6+2^5+2^4+2^3 = 248)

Number of Network – 1

Number of Subnets – 32 (2^4+2^3+2^2+2^1+1)

All Zeros and All Ones cannot be used as a Subnet or Host IDs

Total number of Hosts – 65472 (32 Subnets X 2046/Subnet)

Subnet Conversion Tables:

(Class A)

Number of Subnets	No. of Required Bits	Subnet Mask	Number of Hosts per Subnet
0	1	Invalid	Invalid
2	2	255.192.0.0	4,194,302
6	3	255.224.0.0	2,097,150
14	4	255.240.0.0	1,048,574
30	5	255.248.0.0	524,286
62	6	255.252.0.0	262,142
126	7	255.254.0.0	131,070
254	8	255.255.0.0	65,534

Class A Subnet Using One Octet

Subnet Conversion Tables:

(Class B)

Number of Subnets	No. of Required Bits	Subnet Mask	Number of Hosts per Subnet
0	**1**	**Invalid**	**Invalid**
2	**2**	**255.255.192.0**	**16,382**
6	**3**	**255.255.224.0**	**8,190**
14	**4**	**255.255.240.0**	**4,094**
30	**5**	**255.255.248.0**	**2,046**
62	**6**	**255.255.252.0**	**1,022**
126	**7**	**255.255.254.0**	**510**
254	**8**	**255.255.255.0**	**254**

Class B Subnet Using One Octet

Subnet Conversion Tables:

(Class C)

Number of Subnets	No. of Required Bits	Subnet Mask	Number of Hosts per Subnet
0	**1**	**Invalid**	**Invalid**
2	**2**	**255.255.255.192**	**62**
6	**3**	**255.255.255.224**	**30**
14	**4**	**255.255.255.240**	**14**
30	**5**	**255.255.255.248**	**6**
62	**6**	**255.255.255.252**	**2**
126	**7**	**255.255.255.254**	**Invalid**
254	**8**	**255.255.255.255**	**Invalid**

Class C Subnet Using One Octet

Another Way to Define No. of Subnet Ids:

- Formula:
  - No. of Subnet available with “n” bits you are using for subnetting = 2^n -2
- Example:
  - We are using three digits from Octet to calculate the number of subnets:
  - 2^3 - 2 = 8-2 = 6 subnets possible

From a Subnet Mask and NetID

- Assume a Class B Address:
  - 121.045.X.X
- Using Subnet Mask of:
  - 11111111.11111111.11110000.00000000
- We will come up with a list of Subnet Ids, using matrix in Slide 36, on Slide 38.

Defining Subnet ID

(Class B with 4 used for Subnet in 3rd Octet)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0 (Not Valid)
0	0	0	1	0	0	0	0	= 16
0	0	1	0	0	0	0	0	= 32
0	0	1	1	0	0	0	0	= 48
0	1	0	0	0	0	0	0	= 64
0	1	0	1	0	0	0	0	= 80
0	1	1	0	0	0	0	0	= 96
0	1	1	1	0	0	0	0	= 112
1	0	0	0	0	0	0	0	= 128
1	0	0	1	0	0	0	0	= 144
1	0	1	0	0	0	0	0	= 160
1	0	1	1	0	0	0	0	= 176
1	1	0	0	0	0	0	0	= 192
1	1	0	1	0	0	0	0	= 208
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240 (Not Valid)

Subnet ID Identification

(Class B with 4 used for Subnet in 3rd Octet)

Subnet Octal Decimal Value	**Net ID**
= 0 (Not Valid)	
= 16	121.045.16.X
= 32	121.045.32.X
= 48	121.045.48.X
= 64	121.045.64.X
= 80	121.045.80.X
= 96	121.045.96.X
= 112	121.045.112.X
= 128	121.045.128.X
= 144	121.045.144.X
= 160	121.045.160.X
= 176	121.045.76.X
= 192	121.045.192.X
= 208	121.045.208.X
= 224	121.045.224.X
= 240 (Not Valid)	

- Subnet ID is not consecutively numbered.
- Only 14 could be identified with 4 bits used in third Octet for Subnetting

Defining Host ID for a Subnet:

Octet Bit Value	Subnet Octet Decimal Value	Beginning Range Value	Ending Range Value
00000000	0(Not Valid)	Invalid	Invalid
00010000	16	X.X.16.1	X.X.31.254
00100000	32	X.X.32.1	X.X.47.254
00110000	48	X.X.48.1	X.X.63.254
01000000	64	X.X.64.1	X.X.79.254
01010000	80	X.X.80.1	X.X.95.254
00110000	96	X.X.96.1	X.X.111.254
01110000	112	X.X.112.1	X.X.127.254
10000000	128	X.X.128.1	X.X.143.254
10010000	144	X.X.144.1	X.X.159.254
10100000	160	X.X.160.1	X.X.175.254
10110000	176	X.X.176.1	X.X.191.254
11000000	192	X.X.192.1	X.X.207.254
11010000	208	X.X.208.1	X.X.223.254
11100000	224	X.X.224.1	X.X.239.254
11110000	240(Not Valid)	Invalid	Invalid

Subnetting:

- Allows Network Administrators overcome the physical limitations of network’s capacity.
- Allows an effective increase in network bandwidth, by cutting down on the amount of broadcasts a network must process.

Subnetting does not provide:

- An easy way to classify the Host to easily be identified in a certain sub-network
- Easy calculations to identify where a host is
  - Requires network diagrams to troubleshoot network problems

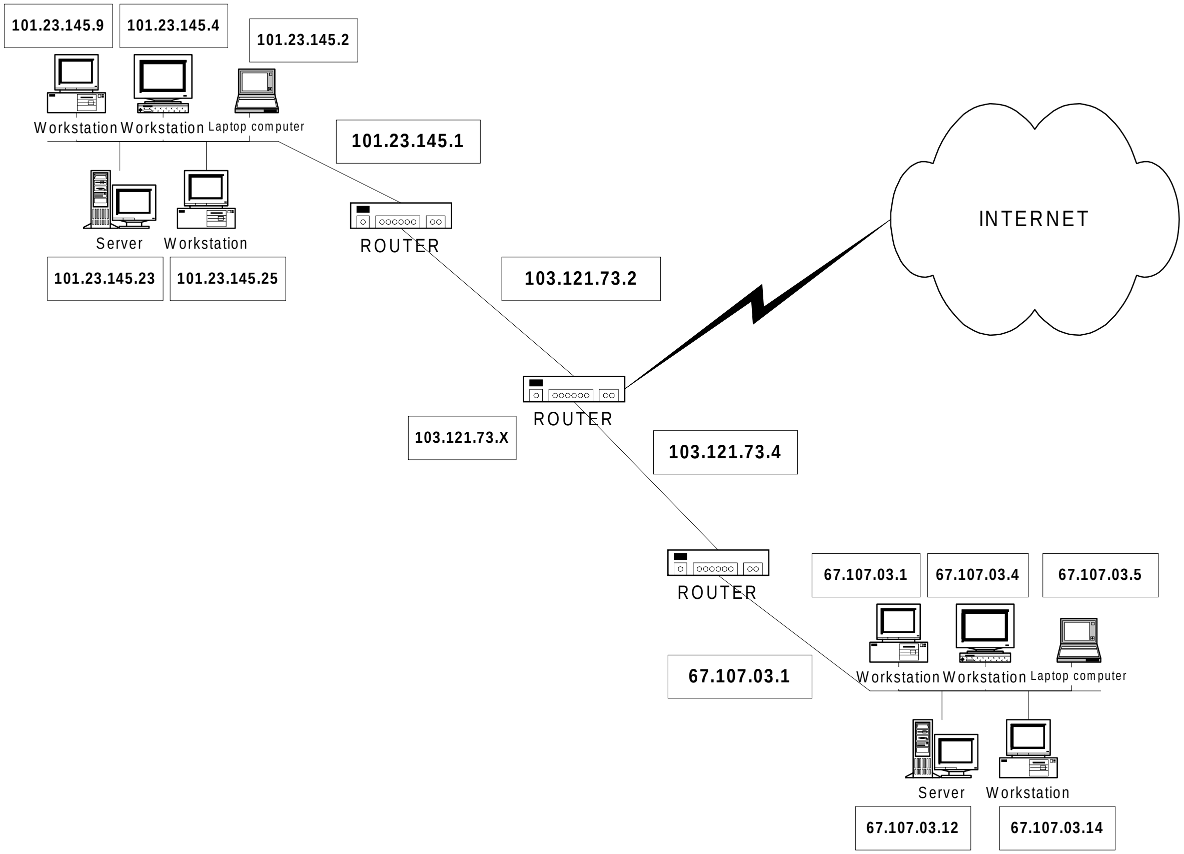
What is IP Routing?

- Routing is the process of choosing a path over which to send packets
- This occurs when a TCP/IP host sends IP packets and routing occurs at an IP router.
- Notice the difference among repeater,bridge, and routers -- refer to Definitions

How Does Router Work?

- Communicating IP Hosts determines whether the communicated host is on local or remote network
  - Local -- same network/sub-network
  - Remote -- Outside Local network
- If Remote, Host checks router IP routing Table for a route to send through which port. Host and Network address must be specific

Typical Network IP Numbering



7/25/99

How Does Router Work?

- If no IP address and port is found, it sends to a default gateway address.
- The Routing Table in the default gateway is then consulted, and this process continues for a determined number of times before the packet is returned if the IP is not found.

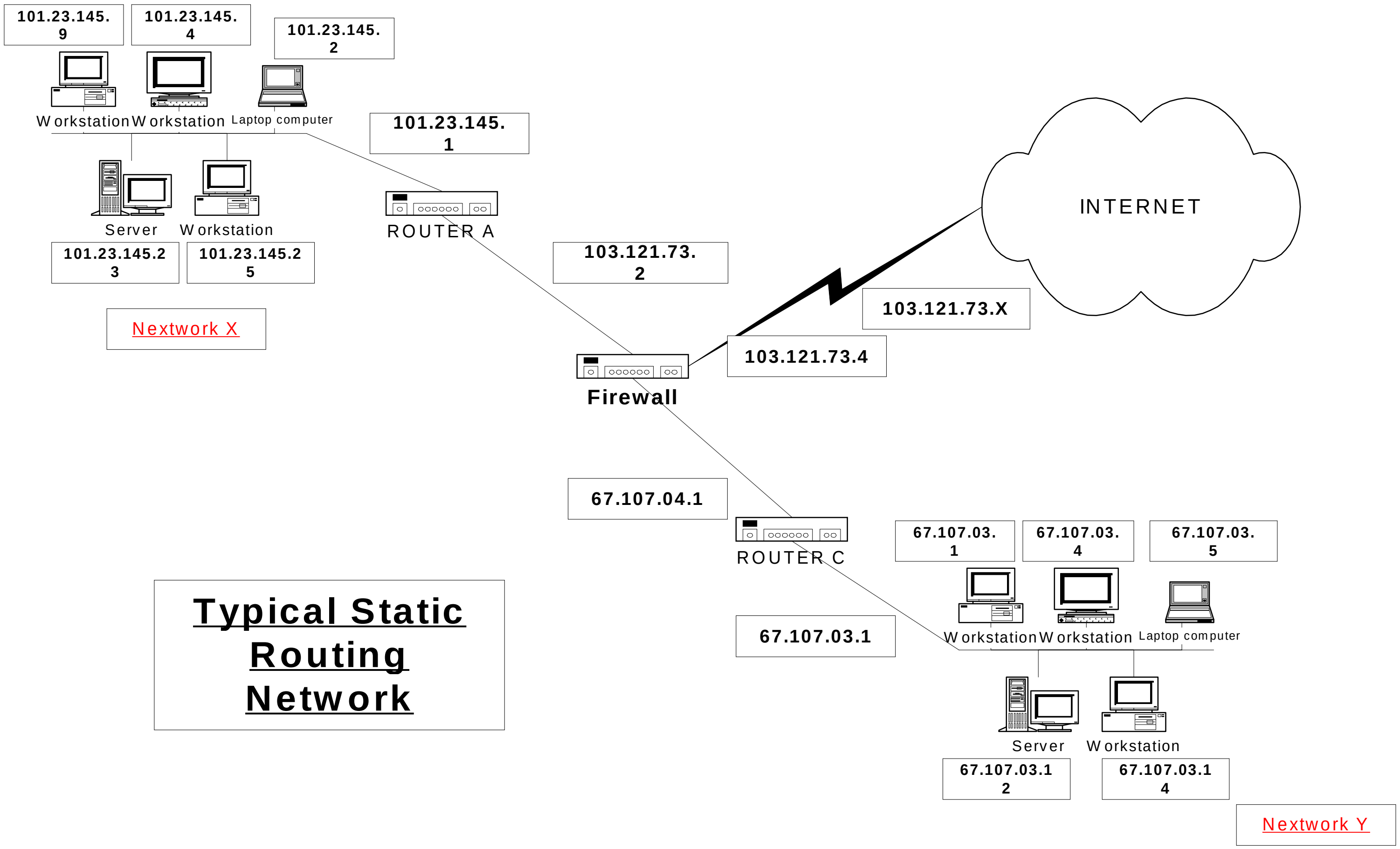
Two Types of Routers:

- Static Routing -- Function of IP
  - Routers do not share routing information
  - Routing tables are built manually
- Dynamic Routing -- Function of Inter-Routing Protocols
  - Routers share routing information automatically
  - Requires routing protocol, e.g RIP or OSPF.

Static IP Routing:

- The router only communicates with networks with a configured interface
- It does not send new configuration downstream
  - Excellent for Firewall and high security environment

Static IP Routing Typical Arrangements:



Typical Static Routing Network

How It Works:

- Router A has only local connection to Network X and Firewall Router. Hosts on Network X cannot directly communicate with Hosts on Network Y without going through the Firewall Router. Same for Host in Network Y
- To route IP packets to other networks:
  - – Each address must be manually entered onto the Routing Table to route IP packets
  - – A default gateway address to another router's local interface is required

Typical Routing Table:

Routing Table for Router A		
Network Address	**Network Mask**	**Gateway Address**
103.121.73.4	255.255.255.0	101.121.73.2
67.107.04.1	255.255.255.0	101.121.73.2
67.107.03.0	255.255.255.0	101.121.73.2

Dynamic IP Routing:

- Using RIP protocol, routers automatically exchange routes to known networks with each other, and update any changes
- Normally installed on large intra-networks
- Only need to set the default gateway address to match the IP address of the local router's interface

TCP/IP Security Concerns

- IP Addresses can be spoofed -- snooped and replaced
- Syn Flood Attack
- Spamming through incorrect IP addresses
- Denial of Service Attack

Packet Filtering Firewall

- Packet Filtering
  - Using Routers, and packet filtering rules to grant or deny access.
  - Source and Destination Addresses in the IP packet header can be spoofed.
  - Do not protect against IP or DMS address Spoofing.
  - Does not support logging or user authentication.
  - Attackers will have direct access to host once they pass through firewalls.

Application Gateways Firewall:

- The Proxy Server Program examines external request, and forward legitimate ones to internal hosts to provide requested services
  - Considered most secured Firewall.
  - Gateway can be configured as the only external IP address.
  - Prevent Direct Access to servers and services.
  - Strong User Authentication and detailed Logging.
  - Requires a proxy for each service.

Hybrid or Complex Gateway:

- Combination of Packet Filtering and Proxy Server Gateway.
  - In Parallel -- will only secure the least secure of both methods.
  - In Series -- the overall security is enhanced.

Firewall Architectures:

- Multi-homed:
  - A host(firewall) that has more than one network interface, each connected to a separate physical network.
  - Dual homed (2-NIC cards - One facing External, the other facing Internal)

Firewall Architecture: (Cont’d)

- Screened Host:
  - Use a Bastion Host to filter all external requests prior to routing, e.g. using packet filtering. These hosts are normally set at the outside of the internal network.

Screened Subnet Firewall:

- Same as Screened Host, however, extra security is added by creating a network which the bastion host resides. They are separate from internal network.

Strength and Weakness of Firewalls:

Firewall Technique	Advantages	Disadvantages
Packet Filtering	• Completely transparent. • Easy to Filter Access at the host or network level. • Inexpensive: Can use existing routers to implement.	• Reveals internal network topology. • Does not provide enough granularity for most security policies. • Difficult to Configure. • Does not Support Certain Traffic • Susceptible to address-spoofing. • Limited or no logging and alarms. • No user authentication.
Application Gateway	• Application-level security. • Strong user access control. • Strong logging and auditing support. • Ability to Conceal internal network.	• Requires Specialized proxy for each service. • Slower to implement new services. • No support for client software that does not support redirection.
Hybrid	• Combines the strength of Packet Filtering and Application if implemented correctly.	• Requires network security expertise, and need to be well managed. • Requires adequate security administration to be effective.

Overview of IPv6

- IP Version 1 - 3 were not formally assigned
- IP Version 4 - TCP/IP -- 32 bit IP address, currently used
- IP Version 5 -- Streamed Protocol(ST), a connection-oriented internet-level protocol
- IP Version 6 -- Designed to Replace IPv4 -- 128 bit IP address.

IPv6 has following Advantages:

- Essentially Unlimited Addresses
  - 296 times more than the number of IPv4 addresses
- Simplified auto-configuration: IP addresses are generated when hardware is plugged into network
- IPv6 header is designed for optimized processed

IPv6 has following Advantages:

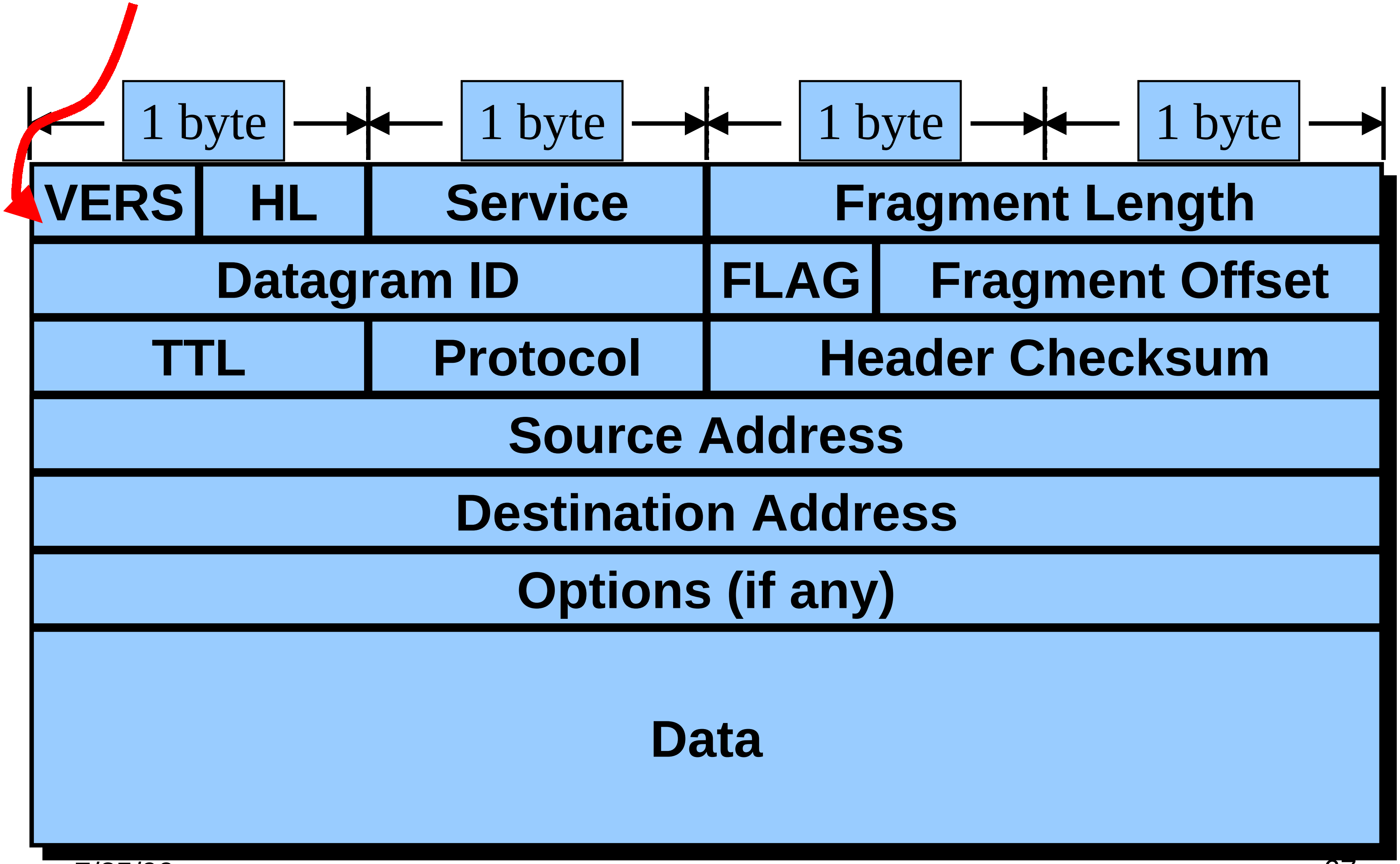
(Cont'd)

- Must implement standardized set of security features
  - Authentication Header
  - Encapsulating Security Payload(ESP) service
- Native multicast support
- Support to automatically renumber entire networks

IPv6 Security:

- IPv6 Authentication Header gives network applications a guarantee that a packet did come from an authenticated source
- ESP encrypts the IP datagram so that the information will not be visible to snoopers

IPv4 Header



4 for IPv4

VERS | HL | Service | Fragment Length

Datagram ID | FLAG | Fragment Offset

TTL | Protocol | Header Checksum

Source Address

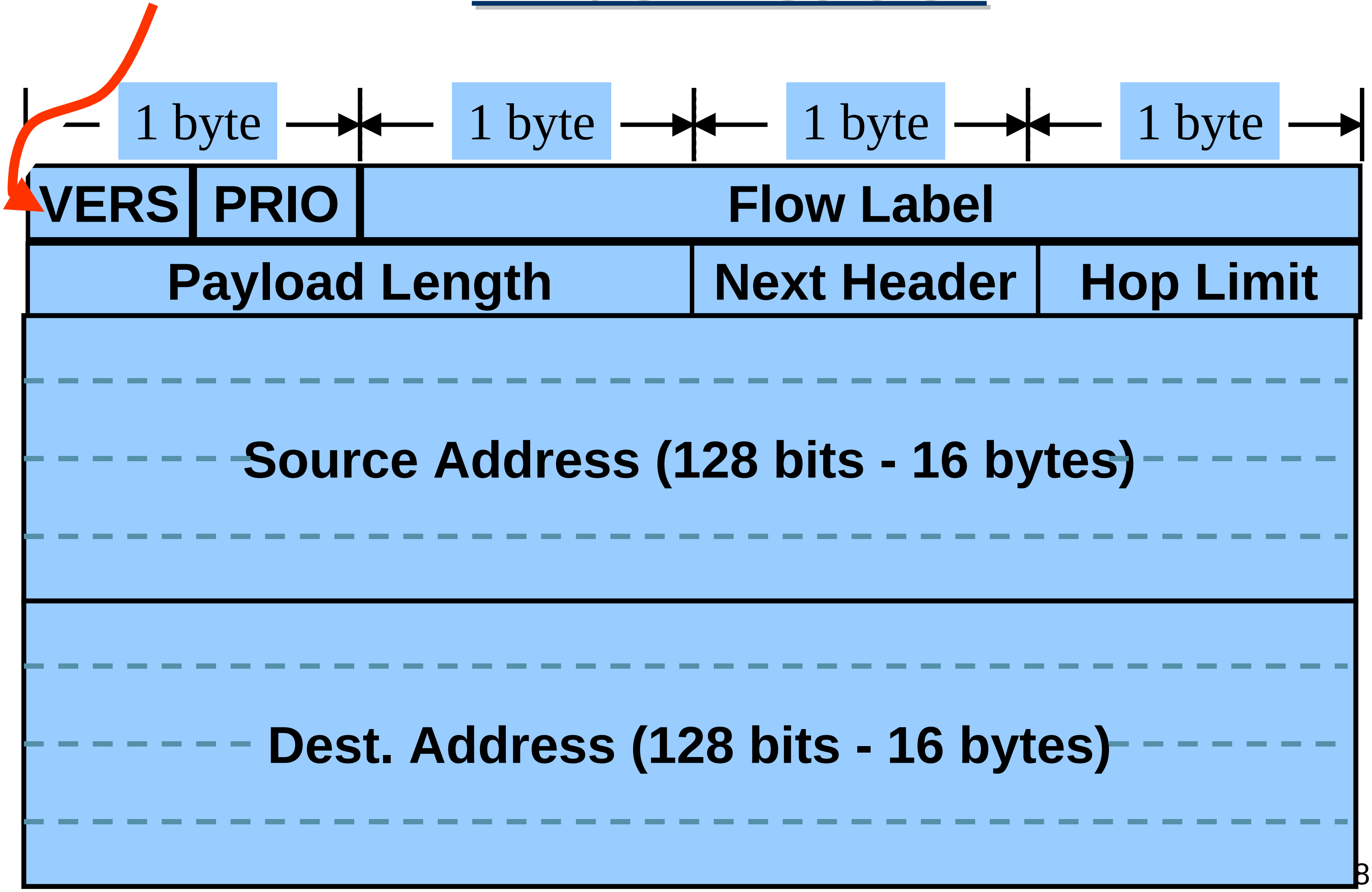
Destination Address

Options (if any)

Data

IPv6 Header

6 for IPv6



1 byte

1 byte

1 byte

1 byte

VERS | PRIO | Flow Label

Payload Length | Next Header | Hop Limit

Source Address (128 bits - 16 bytes)

Dest. Address (128 bits - 16 bytes)

IPv6 Header Fields

- VERS: 6 (IP version number)
- Priority: will be used in congestion control
- Flow Label: experimental - sender can label a sequence of packets as being in the same flow.
- Payload Length: number of bytes in everything following the 40 byte header, or 0 for a *Jumbogram*.

IPv6 Header Fields

- Next Header is similar to the IPv4 “protocol” field - indicates what type of header follows the IPv6 header.
- Hop Limit is similar to the IPv4 TTL field (but now it really means hops, not time).

IPv6 Addresses

- 128 bits - written as eight 16-bit hex numbers.

```
5f1b:df00:ce3e:e200:0020:0800:2078:e3e3
```

- High order bits determine the *type* of address. The book shows the breakdown of address types.

IPv6
Aggregate Global Unicast Address

3	13	32	16	64
001	**TLA ID**	**NLA ID**	**SLA ID**	**Interface ID**

TLA: top-level aggregation
NLA: next-level
SLA: site-level

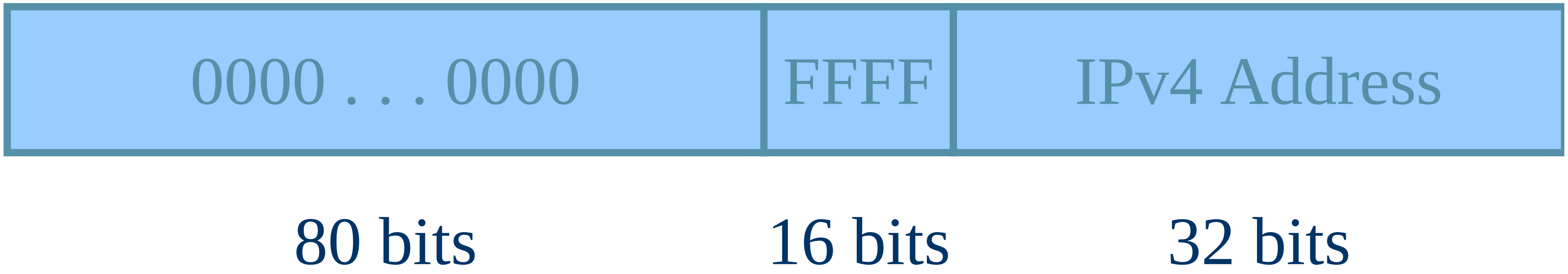
Interface ID is based on hardware MAC address

IPv4-Mapped IPv6 Address

- IPv4-Mapped addresses allow a host that support both IPv4 and IPv6 to communicate with a host that supports only IPv4.
- The IPv6 address is based completely on the IPv4 address.

IPv4-Mapped IPv6 Address

- 80 bits of 0s followed by 16 bits of ones, followed by a 32 bit IPv4 Address:



0000 . . . 0000	FFFF	IPv4 Address
80 bits	16 bits	32 bits

IPv4-Compatible IPv6 Address

- An IPv4 compatible address allows a host supporting IPv6 to talk IPv6 even if the local router(s) don’t talk IPv6.
- IPv4 compatible addresses tell endpoint software to create a tunnel by encapsulating the IPv6 packet in an IPv4 packet.

Definitions:

- Appletalk -- A dedicated protocol for Apple network
- IPX/SPX -- Basic Protocol used on a Netware network
- NFS -- Network File System -- A UNIX dedicated protocol
- SMB, NCP -- Server Message Block, Netware Core Protocol, they are redirectors protocols to intercept requests, format them according to protocol in use, and pass the messages to lower level
- NetBUEI -- NetBios Extended User Interface, a non-routable protocol used in smaller networks

Definitions (Cont'd)

- UDP -- User Datagram Protocol, a connectionless protocol that sends packets to different computers or systems
- TDI -- Transport Driver Interface (Lets application programmers create components for Session layer to communicate down to Transport Layer)
- NDIS -- Network Device Interface Specification(An Application Program Interface designed to facilitate communication between transport protocol drivers and the underlying network interface drivers. It provides the ability to use more than one protocol over a single network card)

Definitions (Cont’d)

- FDDI -- Fiber Distributed Data Interface (Very fast and expensive fiber network access method -- Up to 100Mbps)
- PPP -- Point to Point protocol (A communication protocol that provides dial-up access to a network, normally used to connect to Internet)
- Frame Relay -- A point to point network communications media that moves packets without stripping any information on the packets.
- NetBIOS -- The main protocol used by Windows NT

Definitions (Cont'd)

- Router -- A router is a device that forwards the packets from one physical network to another -- normally known as a gateway. Routers are connected at Network Layer
- A Bridge -- A device that joins two LANs. It allows stations on either network to access resources on the other. Bridges are connected at the Data Link Layer
- Repeater -- A device that regenerates signals so they can travel on additional cable length. Repeaters connected at Physical Layer

Definitions (Cont’d)

- RIP -- Routing Information Protocol, a protocol that enables communication between routers on a network to facilitate the exchange of routing tables.
- OSPF -- Open Shortest Path First, a link state routing algorithm. This allows routers to respond quickly to changes in network, and uses the Dijkstra algorithm to calculate the routes based on no. of hops, line speed, traffic, and cost.

References for this Presentation:

- Networking Essentials - Microsoft Press
- Internetworking with TCP/IP in MS Windows NT 4.0 - Microsoft Education
- Practical UNIX & Internet Security -- O'Reilly $ Associates
- Windows NT Server - Introduction to TCP/IP White Paper -- Microsoft
- Exam CRAM - TCP/IP -- Certification Insider Press
- Handbook of Information Security Management -- 1999 -- Auerbach Press
- RFC 2373 -- IPv6 Addressing Architecture (7/1998)