

www.vuCTn.com

CS610

PPT Slide Lec 1 To 45

Admin:

Merged date 19-11-20

Efforts: Laiba Mahi

Regards: Zarva Chaudhary

Chaudhary Moazzam

COMPUTER NETWORKS

CS610

Lecture-1

Hammad Khalid Khan

Course Answers the Basic Question:

How do COMPUTER NETWORKS and
INTERNET Operate?

Textbook

- ◆ Title
Computer Networks and Internets, with Internet Applications, 4th edition
- ◆ Author Douglas E. Comer
- ◆ Publisher Pearson Education
- ◆ Book website
<http://www.netbook.cs.purdue.edu>

Reference Books

- ◆ “Computer Networks” by Andrew S. Tanenbaum, Prentice Hall Publishers
- ◆ “Networking: A Top-Down Approach Featuring the Internet” by James F. Kurose and Keith W. Ross

Course Composition

- ◆ Four Main Parts
 - Using and Building Internet Applications (Chap. 1 - 3)
 - Data Transmission (Chap. 4 - 6)
 - Packet Transmission (Chap. 7-16)
 - Interntworking (Chap. 17-27)
 - Network Applications (Chap. 28-41)

Part 1: Data Transmission

- ◆ Transmission Media
- ◆ Local Asynchronous Communication (RS 232)
- ◆ Long Distance Communication (Modems and Carriers)

Part 2: Packet Transmission

- ◆ Packets and Frames
- ◆ Local Area Networks (LANs)
 - Hardware Addressing
 - Ethernet, WLAN and Bluetooth
 - Extending LANs: Fiber Modems, Repeaters, Bridges, Switches

Part 2: Packet Transmission (Cont'd)

- ◆ WAN Technologies and Routing
- ◆ Network Ownership and Service Paradigm
- ◆ Protocols and Layering

Part 3: Interntworking

- ◆ Concepts, Architecture and Protocols
- ◆ IP Addresses
- ◆ Binding Protocol Addresses

Part 3: Interntworking (Cont'd)

- ◆ IP Datagrams and Datagram Forwarding
- ◆ IP Encapsulation, Fragmentation and Reassembly
- ◆ TCP/IP

Part 4: Network Applications

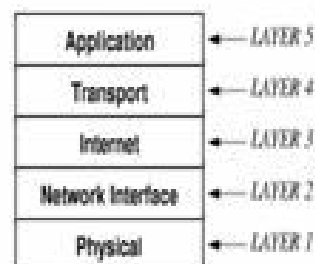
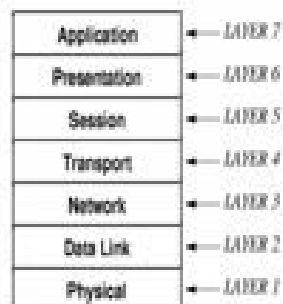
- ◆ Client-Server Interaction
- ◆ The Socket Interface
- ◆ Example Applications

Grade Distribution

- ◆ Assignments 15%
- ◆ Midterm Examination 35%
- ◆ GMDB 5%
- ◆ Final Examination 45%

COURSE INTRODUCTION

ISO Model and TCP/IP Protocol



CHAPTER No. 1 INTRODUCTION

Network and Internet

- ◆ **Network**

System for connecting computers using a single transmission technology

- ◆ **Internet**

Set of networks connected by routers that are configured to pass traffic among any computers attached to any network in the set

Classification of Networks

- ◆ By SIZE
 - ◆ Local Area Network (LAN) versus Wide Area Network (WAN)
- ◆ By Connectivity
 - ◆ Point-to-Point versus Broadcast
- ◆ By Communication Medium
- ◆ By Mobility
 - ◆ Fixed versus Mobile

Networks in Daily Life

- ◆ Now, networks are an important part of everyday activities
 - ◆ Business
 - ◆ Home
 - ◆ Government
 - ◆ Education

Mastering The Complexity

- ◆ Concentrate on understanding the concepts
- ◆ Learning the Networking Terminology
(summarized in a Glossary in Appendix 1)

Complexity in Network Systems

- ◆ Many different technologies exist
- ◆ No single underlying theory or model
- ◆ Models are either so simplistic or so complex
- ◆ No simple or uniform terminology

Review Lecture 1

- ◆ Course Introduction
- ◆ Network and Internet
- ◆ Classification of Networks
- ◆ Networks in Daily Life
- ◆ Complexity in Computer Networking
- ◆ Mastering the Complexity

COMPUTER NETWORKS

CS610

Lecture-2

Hammad Khalid Khan

CHAPTER No. 2

MOTIVATION and TOOLS

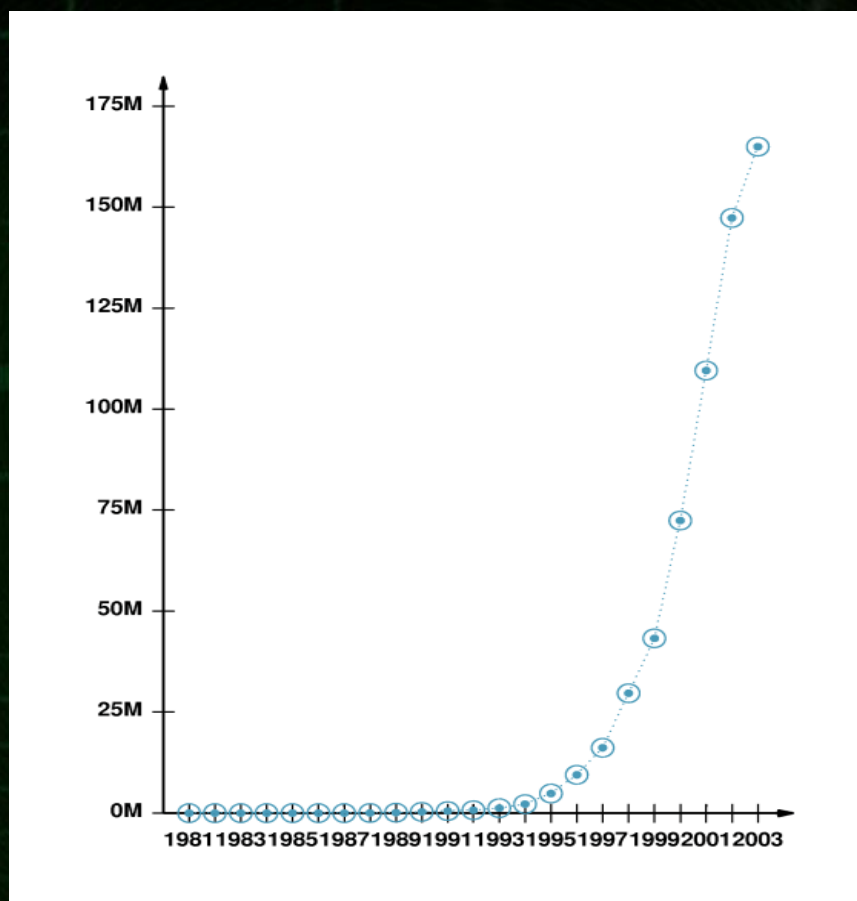
Resource Sharing

- ◆ Sharing a peripheral device such as a printer or a disk
- ◆ Sharing a large-scale computational power, because
 - Computers were extremely expensive
 - The government budgets were not sufficient to provide computers for all scientists and engineers

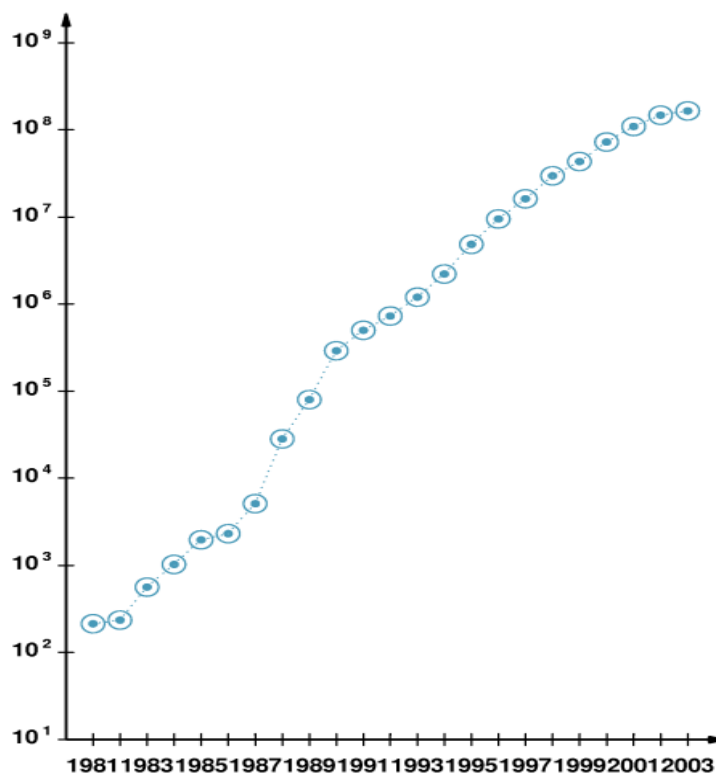
Growth of the Internet

- ◆ U.S Department of Defence Advanced Research Projects Agency (ARPA) started ARPANET project
- ◆ The early internet emerged in 1970s
- ◆ Has grown drastically since then

Growth of the Internet



Growth of the Internet



Probing The Internet

- ◆ “PING” program

```
D:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\zain>ping vu.edu.pk

Pinging vu.edu.pk [192.168.9.100] with 32 bytes of data:

Reply from 192.168.9.100: bytes=32 time<1ms TTL=128
Reply from 192.168.9.100: bytes=32 time<1ms TTL=128
Reply from 192.168.9.100: bytes=32 time<1ms TTL=128
Reply from 192.168.9.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.9.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Probing The Internet

- ◆ “PING” program

```
PING sears.com: 56 data bytes
64 bytes from 32.97.168.129: icmp_seq=0. time=49. ms
64 bytes from 32.97.168.129: icmp_seq=1. time=50. ms
64 bytes from 32.97.168.129: icmp_seq=2. time=48. ms
64 bytes from 32.97.168.129: icmp_seq=3. time=50. ms
64 bytes from 32.97.168.129: icmp_seq=4. time=48. ms
----sears.com PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 48/49/50
```

Probing The Internet

- ◆ Problems with the ping
 - “Ping” cannot tell the reason of the problem
 - Some networks or computers reject the ping packets
 - “Traceroute”

Probing The Internet

- ◆ Tracing A Route

```
tracert to DANDELION-PATCH.MIT.EDU (18.181.0.31), 40 byte packets
 1  cisco1 (128.10.2.250)  2 ms  1 ms  2 ms
 2  cisco-tel-252.tcom.purdue.edu (128.210.252.22)  2 ms  1 ms  1 ms
 3  abilene.tcom.purdue.edu (192.5.40.10)  6 ms  8 ms  7 ms
 4  clev-ipls.abilene.ucaid.edu (198.32.8.26)  14 ms  14 ms  12 ms
 5  nycm-clev.abilene.ucaid.edu (198.32.8.30)  24 ms  27 ms  24 ms
 6  192.5.89.45 (192.5.89.45)  31 ms  34 ms  35 ms
 7  192.5.89.10 (192.5.89.10)  33 ms  33 ms  33 ms
 8  NW12-RTR-FDDI.MIT.EDU (18.168.0.16)  59 ms  34 ms  33 ms
 9  DANDELION-PATCH.MIT.EDU (18.181.0.31)  62 ms * 79 ms
```

Summary

- ◆ Resource Sharing
- ◆ Growth of the Internet
 - Linear Scale
 - Log Scale
- ◆ Tools for Probing the Internet
 - PING
 - TRACE ROUTE

COMPUTER NETWORKS

CS610

Lecture-3

Hammad Khalid Khan

Types of Multiplexing

- ◆ Frequency Division Multiplexing (FDM)
- ◆ Wave Division Multiplexing (WDM)
- ◆ Time Division Multiplexing (TDM)

Review Lecture 2

- ◆ Resource Sharing
- ◆ Growth of the Internet
 - Linear Scale
 - Log Scale
- ◆ Tools for Probing the Internet
 - PING
 - TRACE ROUTE

CHAPTER No. 4 TRANSMISSION MEDIA

Basic Idea

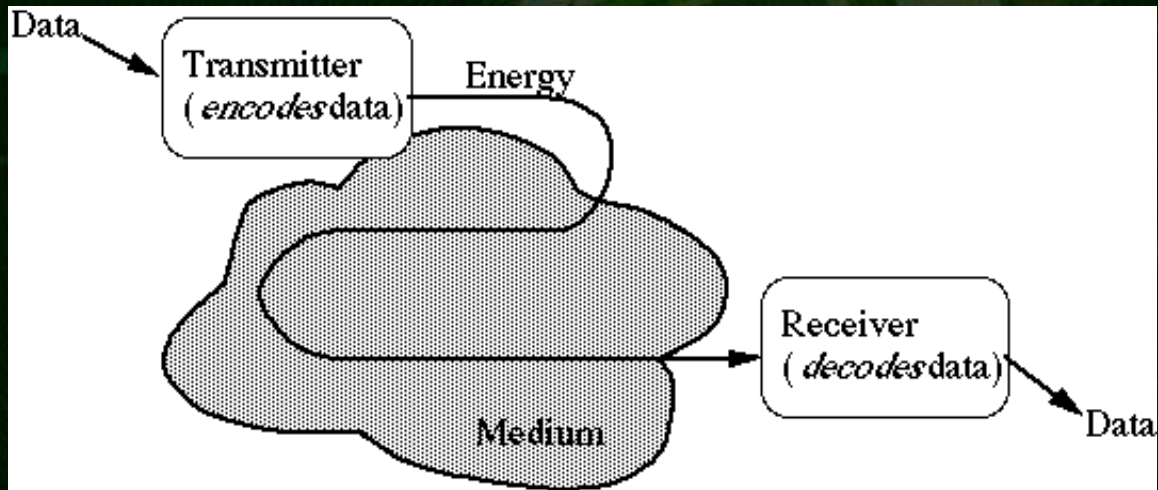
- ◆ Encode data as energy and transmit energy
- ◆ Decode energy at destination back into data
- ◆ Energy can be electrical, light, radio, sound, ...
- ◆ Each form of energy has different properties and requirements for transmission

Transmission media

- ◆ Transmitted energy is carried through some sort of medium
- ◆ Transmitter encodes data as energy and transmits energy through medium
 - Requires special hardware for data encoding
 - Requires hardware connection to transmission medium

Transmission media

- Media can be copper, glass, air, ...



Copper Wires

- Widely used because of low resistance to electric current, inexpensive and easy to install
- Twisted pair wires
 - Two insulated copper wires twisted together to reduce Interference
 - Examples: Telephone wiring (one pair). LAN wiring UTP cable (4 pairs of copper wire)

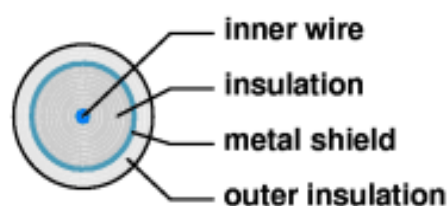


Types of Media

- ◆ GUIDED Media:
 - ◆ Uses physical path
 - Examples: copper wires, optical fiber, coaxial cables etc.
- ◆ UNGUIDED Media:
 - ◆ Uses no physical path
 - Example: Radio waves

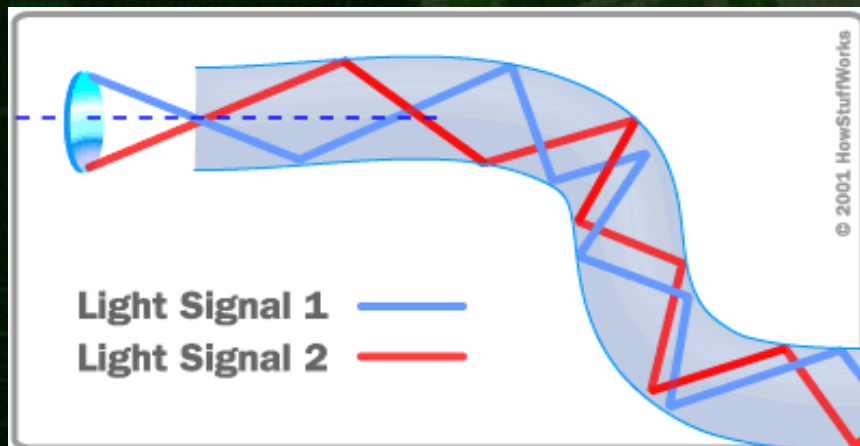
Coaxial Cable

- ◆ Single wire surrounded by an insulation and a metal shield against interference
- ◆ Example use: Cable TV wiring and early LAN wirings



Optical Fibers

- ◆ Uses light to transport data



Advantages of Optical Fibers

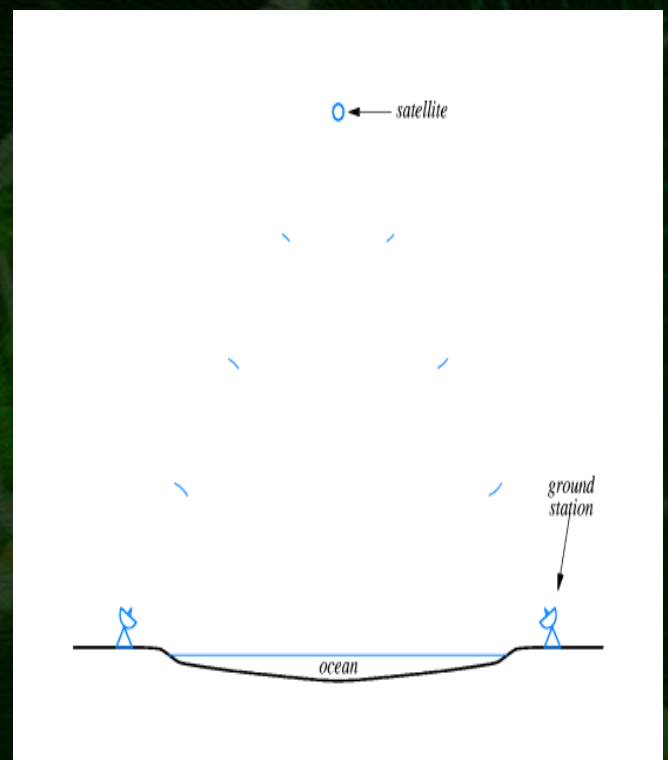
- ◆ Neither causes nor susceptible to electrical interference
- ◆ Can carry pulse much farther than copper
- ◆ Light can encode more information than electric
- ◆ One single fiber is sufficient to carry data

Radio

- ◆ Used for public radio and TV broadcast
- ◆ Data transmission is said to operate at Radio Frequency (RF)
- ◆ Transmission range depends on antenna size

Satellites

- ◆ Satellites for long distance transmission
- ◆ Satellite transponders receive, amplify, and transmit the RF signal back to the ground



Geosynchronous Satellites

- ◆ Placed in an orbit (at 35,785 km or 22,223 miles above the earth) that is exactly synchronized with the rotation of the earth
- ◆ From the ground, it appears to stay at the same position at all times

Low Earth Orbit Satellites

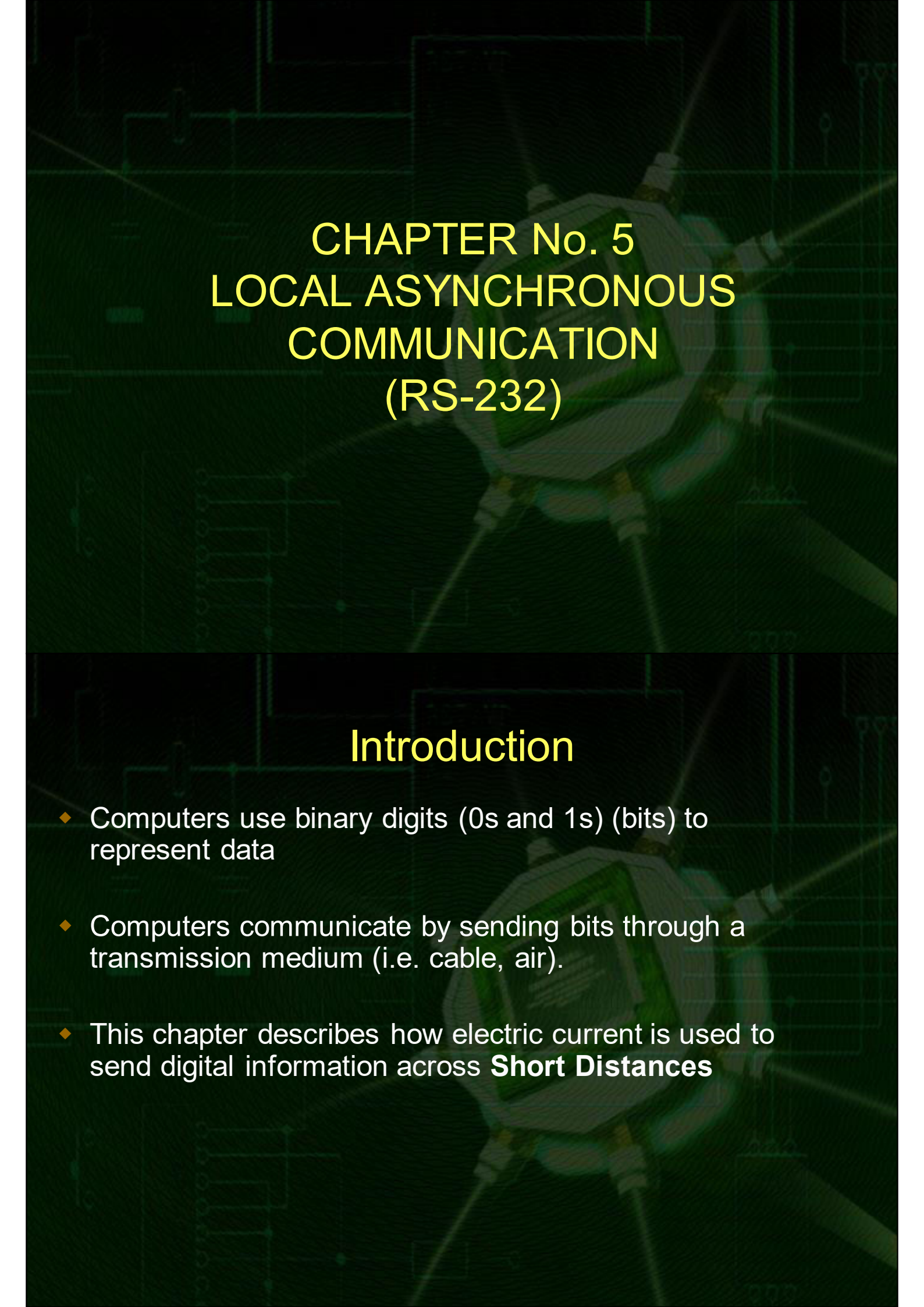
- ◆ Rotates faster than the rotation of the earth at 200 to 400 miles above the earth
- ◆ They do not appear to remain stationary
- ◆ Low Earth Orbit Satellite Arrays is a set of satellites communicating with each other and with the earth surface

Microwave

- ◆ Electromagnetic radiation beyond the frequency range used for radio and TV
- ◆ It can be aimed in a single direction
- ◆ Can carry more information than low frequency RF transmissions

Infrared

- ◆ Remote controls used with TV etc uses IR
- ◆ Inexpensive wireless communication
- ◆ Limited to a small area
- ◆ Convenient for portable computers



CHAPTER No. 5

LOCAL ASYNCHRONOUS COMMUNICATION (RS-232)

Introduction

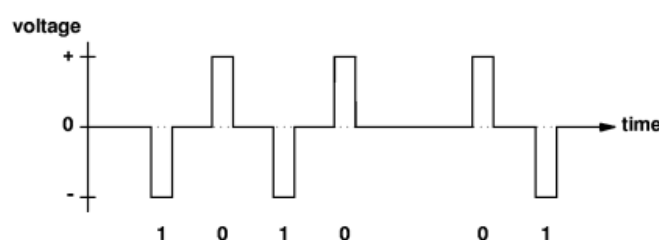
- ◆ Computers use binary digits (0s and 1s) (bits) to represent data
- ◆ Computers communicate by sending bits through a transmission medium (i.e. cable, air).
- ◆ This chapter describes how electric current is used to send digital information across **Short Distances**

The Need For Async Communication

- ◆ In **asynchronous** communication the sender and receiver do not need to coordinate (synchronize) before the transmission begins
- ◆ In an asynchronous system, the receiving hardware must be ready to accept and interpret the signal whenever it arrives

Using Electric Current to Send Bits

- ◆ A small electric current is used to encode data
- ◆ Example: Negative voltage to represent a 0 bit, positive voltage to represent a 1 bit.



Standards For Communication

- ◆ Standard specifies both the timing of the signals and the electrical details of voltage and current
- ◆ **RS232-C** (by EIA) is one of the most widely used standard to transfer characters between a computer and a device such as modem, keyboard etc.
- ◆ RS-232 defines a **serial** (bits are sent one after another) **asynchronous** communication

RS232-C Specifications

- ◆ Cable length < 50 feet (20mt)
- ◆ -15v (bit 1) , +15v (bit 0)
- ◆ One character => 7 or 8 data bits
- ◆ No delay between character bits
- ◆ When idle, puts -15v (bit 1) on the wire
- ◆ Each character start with a start bit(0), and end with a stop bit(1)

Baud Rate, Framing, And Errors

- ◆ Baud rate:
 - The number of changes in the signal per second
- ◆ For simple RS-232, Baud rate = Number of bits/sec
- ◆ If the voltage measurements do not all agree or if the stop bit does not occur exactly at the same time expected, framing errors occur

Full-Duplex Asynchronous Comm

- ◆ Electrical circuits require at least two wires, one of them to carry the data signal, the other is used as the return path, called ground
- ◆ Simultaneous transfers in two directions are known as full-duplex transmission

Full-Duplex Asynchronous Comm

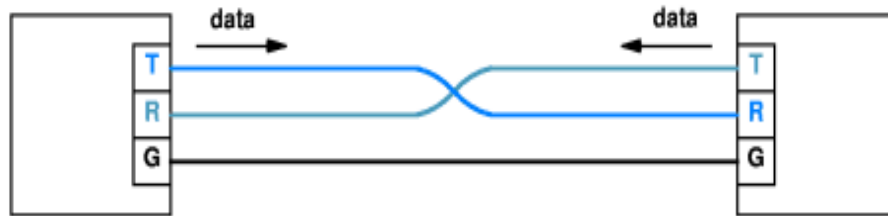


Figure 5.3 The minimal wiring required for full-duplex RS-232 communication. Although the two circuits carry data independently, it is possible for them to share a single ground wire.

CHAPTER No. 6 LONG DISTANCE COMMUNICATION (Carriers, Modulation and Modems)

Long Distance Communication

- ◆ Electric current becomes weaker as it travels over copper
- ◆ Signal loss occurs when RS232 is attempted to use to communicate to a remote site
- ◆ A continuous, oscillating signal, called a Carrier, propagates farther than other signals

Modulation

- ◆ To send data, a transmitter slightly modifies the original information by using a carrier
- ◆ Such modifications are called “Modulation”
- ◆ The receiver
 - monitors the incoming carrier,
 - detects modulation,
 - reconstructs the original data, and
 - discards the carrier

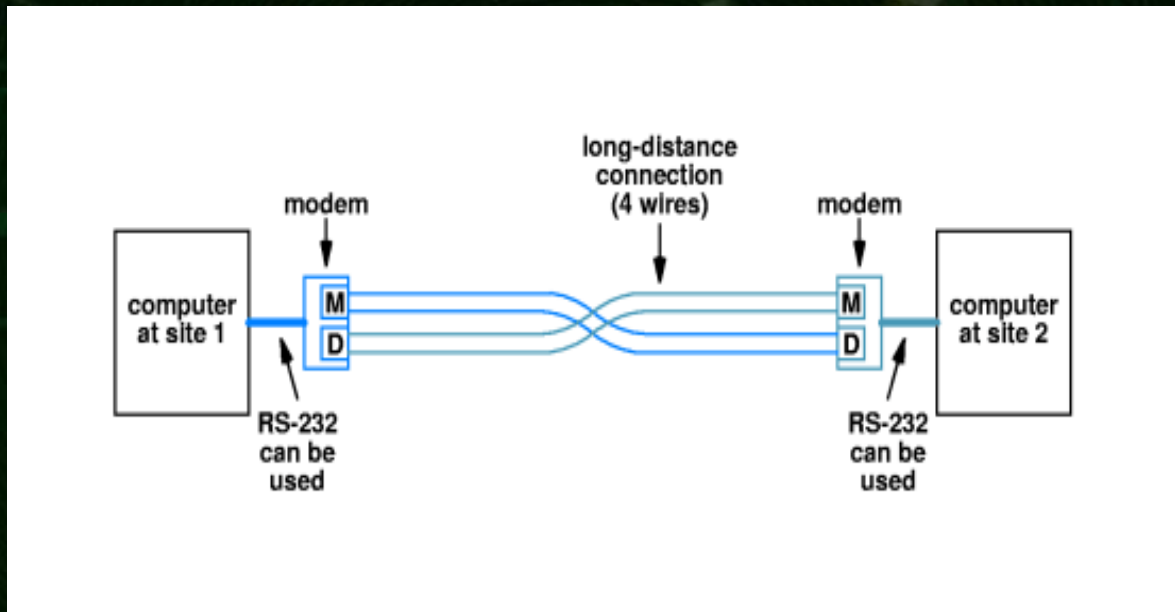
Types of Modulation

- ♦ Three of the modulation schemes are:
 - Amplitude Modulation (AM)
 - Frequency Modulation (FM)
 - Phase Modulation (PM)

Modem

- ♦ A Modulator is a hardware circuit that
 - accepts a sequence of data bits
 - applies modulation to a carrier wave according to the bits
- ♦ A Demodulator is a hardware circuit that
 - accepts a modulated carrier wave and
 - recreates the sequence of data bits
- ♦ A Modem is a hardware that combines both modulator and demodulator in a single device

Modem

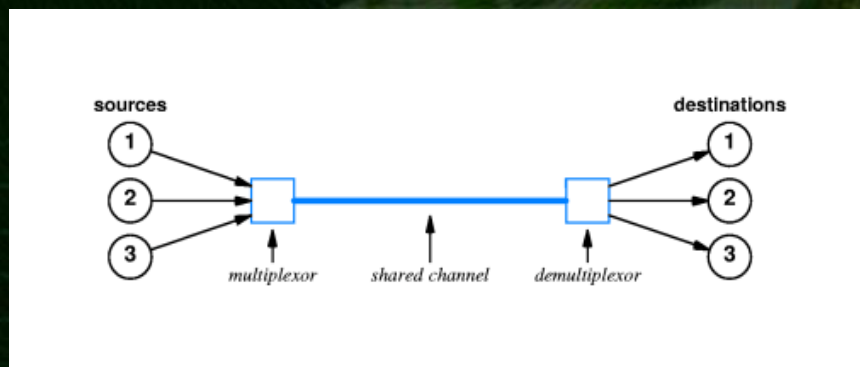


Multiplexing

- ◆ Q: How can two or more signals can be transmitted simultaneously over a single wire ?
- ◆ A: By using different carrier frequencies

Career Frequencies And Multiplexing

- ◆ Frequency division multiplexing (FDM)
 - Using multiple carrier frequencies to allow independent signals, to travel through a medium



Wavelength Division Multiplexing (WDM)

- ◆ FDM concept applied to the optical transmission systems (optical fibers) is known as Wave Division Multiplexing

Time Division Multiplexing (TDM)

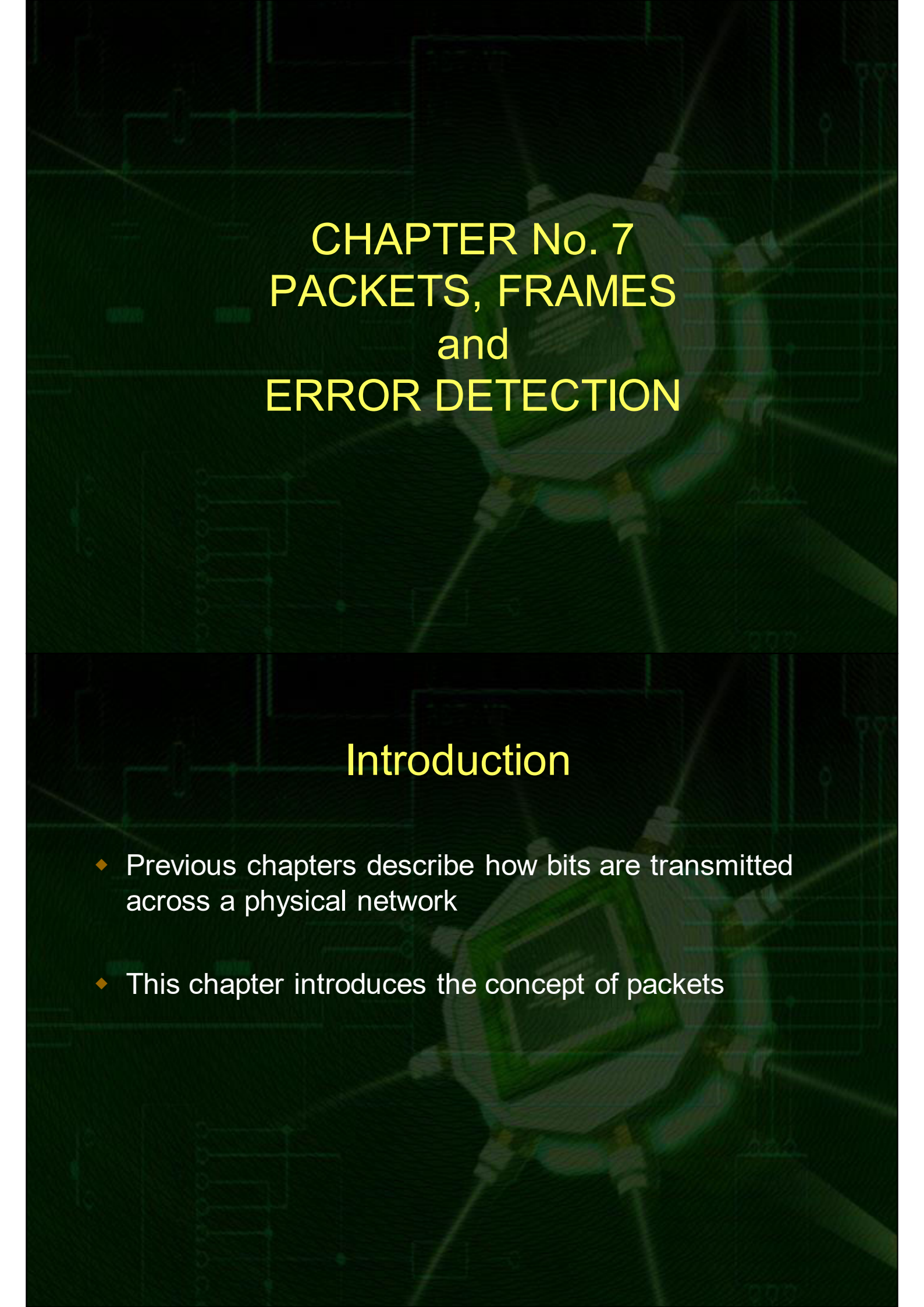
- ◆ Sources sharing a medium “take turns” to send data
- ◆ Synchronous TDM gives each source an opportunity to send data
- ◆ Statistical TDM does not give chance to a source that does not have data to send

COMPUTER NETWORKS

CS610

Lecture-4

Hammad Khalid Khan



CHAPTER No. 7 PACKETS, FRAMES and ERROR DETECTION

Introduction

- ◆ Previous chapters describe how bits are transmitted across a physical network
- ◆ This chapter introduces the concept of packets

The Concept Of Packets

- ◆ The problems:
 - A sender and a receiver need to coordinate to detect transmission errors
 - Individual connections between each pair of computers is not possible

The Concept Of Packets

- ◆ The solution:
 - Shared network connections among many workstations.

Reasons For Using Packets

- ◆ Resource Sharing
- ◆ To Detect The Errors

Use of Packets



Figure 7.1 An illustration of one reason computer networks use packets. While one pair of computers communicate, others must wait.

Problems with the Sharing

- ◆ Demand high – Many computers need to use the shared networks
- ◆ Some applications have large data transfers – Holds the network for a long time
- ◆ Some applications cannot wait
- ◆ Need mechanism for fairness

Solution for Fairness

- ◆ Divide the data into small blocks/chunks called “PACKETS”
- ◆ Computers take turns to send one packet at a time over the shared connection.
- ◆ Because each packet is small, no computer experiences a long delay

Example



Figure 7.1 An illustration of one reason computer networks use packets. While one pair of computers communicate, others must wait.

Example

♦ WITHOUT PACKETS

- 5MB file transferred across network with 56Kbps capacity will require 12 minutes:

$$\frac{5 \times 10^6 \text{ bytes} * 8 \text{ bits/byte}}{60 \text{ secs/minute} * 56 \times 10^3 \text{ bits/second}} = 11.9 \text{ minutes}$$

- All other computers will be forced to wait 12 minutes before initiating other transfers

Example

♦ WITH PACKETS

- If file is broken into packets, other computers must only wait until packet (not entire file) has been sent
- Suppose file is broken into 1000 byte packets

$$\frac{1000 \text{ bytes} * 8 \text{ bits/byte}}{56 \times 10^3 \text{ bits/second}} = .143 \text{ seconds}$$

- Now each packet takes less than .2 seconds to transmit

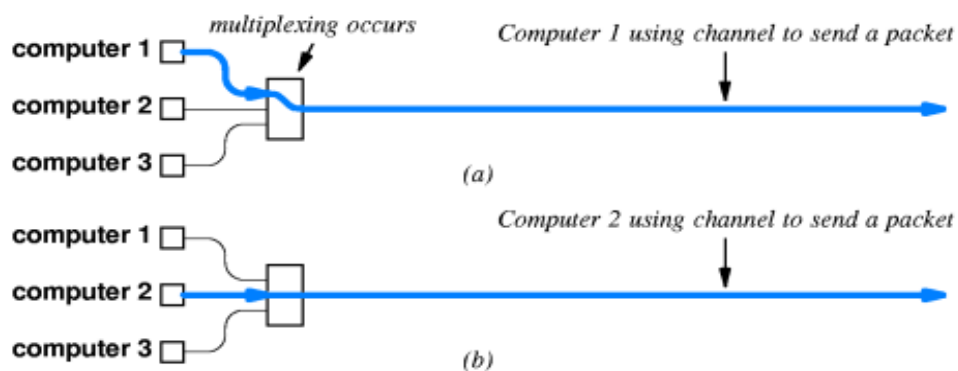
Advantage

- ♦ Other computer must only wait .143 seconds before beginning to transmit
- ♦ Note:
 - If both files are both 5MB long, each now takes 24 minutes to transmit
 - BUT if second file is only 10KB long, it will be transmitted in only 2.8 seconds, while 5MB file still takes roughly 12 minutes

Packets and TDM

- ◆ Dividing data into small packets allows Time-Division Multiplexing
- ◆ Each packet leaves the source and is switched onto the shared communication channel through a Multiplexer
- ◆ At the destination, the packet is switched through a Demultiplexer to the destination

Packets and TDM



Packets and Frames

- ◆ Packet is ``generic" term that refers to a *small block of data*
- ◆ Each hardware technology uses different packet format
- ◆ Frame or *hardware frame* denotes a packet of a specific format on a specific hardware technology

Frame Format

- ◆ Need to define a standard format for data to indicate the beginning and end of the frame
- ◆ Header and trailer used to “frame” the data

Frame Format



Disadvantages of Framing

- ◆ Incurs extra overhead - soh and eot take time to transmit, but carry no data

Advantages

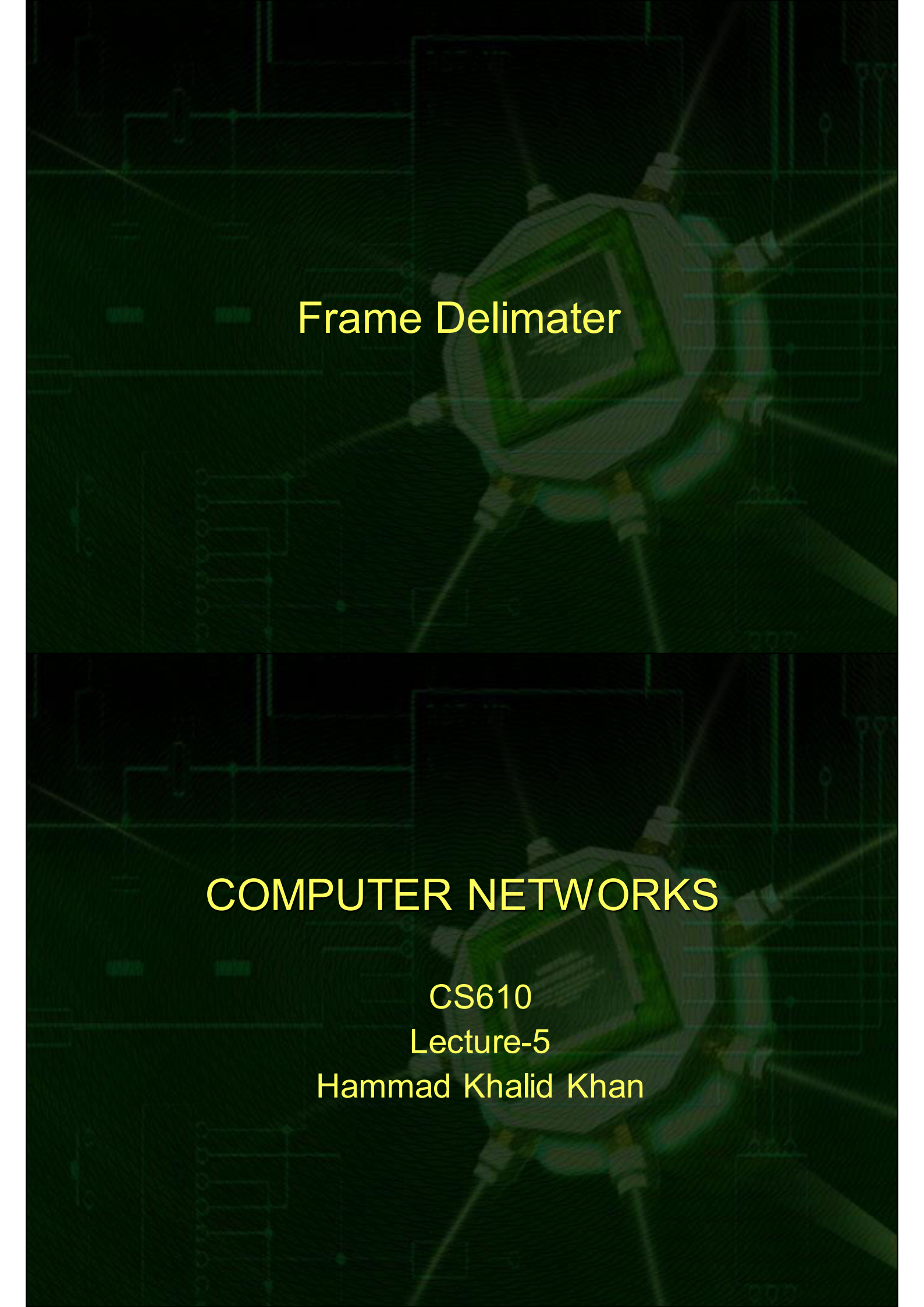
- ◆ Accommodates transmission problems:
 - Missing eot indicates sending computer crashed
 - Missing soh indicates receiving computer missed beginning of message
 - Bad frame is discarded

Data Stuffing

- ◆ Sometimes, the special characters (i.e. *soh* or *eot*) may appear in the data
- ◆ Problem: *soh* and *eot* as part of data will be misinterpreted as framing data
- ◆ Solution: *Data stuffing*

Summary

- ◆ The Concept of Packets
- ◆ Why use Packets?
- ◆ Packets and Frames
- ◆ Data Stuffing



Frame Delimiter

COMPUTER NETWORKS

CS610

Lecture-5

Hammad Khalid Khan

Review Lecture 4

- ◆ The Concept of Packets
- ◆ Why use Packets?
- ◆ Packets and Frames
- ◆ Byte Stuffing

Byte Stuffing

- ◆ Sometimes, the special characters (i.e. soh or eot) may appear in the data
- ◆ Problem: soh and eot as part of data will be misinterpreted as framing data
- ◆ Solution: Byte stuffing

Byte Stuffing (cont'd)

- ◆ Byte stuffing translates each reserved byte into two unreserved bytes
- ◆ For example, can use esc as prefix, followed by x for soh, y for eot and z for esc

Byte Stuffing (cont'd)

- ◆ The sender replaces each occurrence of special characters with a combination of two characters (i.e.esc x, esc y, esc z)
- ◆ The receiver then replaces each occurrence of esc x, esc y, esc z, by the corresponding single character

Byte Stuffing (cont'd)

Character In Data	Characters Sent
<code>soh</code>	<code>esc x</code>
<code>eot</code>	<code>esc y</code>
<code>esc</code>	<code>esc z</code>

Byte Stuffing (cont'd)

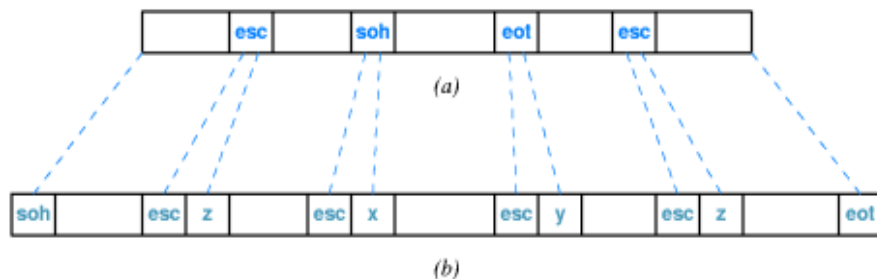


Figure 7.5 Illustration of byte stuffing, where (a) is an example of data that includes characters such as *soh*, and (b) is the frame after byte stuffing. The dashed lines show the locations in the original data where characters have been replaced or new characters added.

Transmission Errors

- ♦ Interference or power surges may destroy data during transmission
 - Bits may be lost
 - Bit values may be changed
- ♦ Frames include additional information to detect / correct errors
 - Inserted by the sender
 - Checked by the receiver

Error Detection & Correction

- ♦ Error detection - send additional information so that incorrect data can be detected and rejected
- ♦ Error correction - send additional information so that incorrect data can be corrected and accepted

Parity Checking

- ◆ Parity refers to the number of bits set to 1 in the data item
 - Even parity - An even number of bits are 1
 - Odd parity - An odd number of bits are 1

Parity Checking

- ◆ A Parity Bit is an extra bit transmitted with a data item, chose to give the resulting bits even or odd parity
 - Even parity - data: 10010001, parity bit 1
 - Odd parity - data: 10010111,
 - parity bit 0

Parity and Error Detection

- ◆ If noise or other interference introduces an error, one of the bits in the data will be changed from a 1 to a 0 or from a 0 to a 1
- ◆ Parity of resulting bits will be wrong
 - Original data and parity: 10010001+1 (even parity)
 - Incorrect data: 10110001+1 (odd parity)

Limitations of Parity Checking

- ◆ Parity can only detect errors that change an odd number of bits
 - Original data and parity: 10010001+1 (even parity)
 - Incorrect data: 10110011+1 (even parity!)
- ◆ Parity usually used to catch one-bit errors

Alternative Error Detection Schemes

- ◆ Alternative error detection mechanisms have been introduced
- ◆ Differences among mechanisms:
 - The size of the additional information (transmission overhead)
 - Computational complexity of the algorithm (computational overhead)
 - The number of bit error that can be detected (how well errors are detected)

Checksum

- ◆ Checksum is calculated before transmission
 - Treats data as a sequence of integers
 - Computes their arithmetic sum
 - Carry bits are added into the final sum
- ◆ Calculated checksum is sent along with data
- ◆ Receiver then performs the same calculation

Checksum

H	e	l	l	o		w	o	r	l	d	.
48	65	6C	6C	6F	20	77	6F	72	6C	64	2E

$4865 + 6C6C + 6F20 + 776F + 726C + 642E + \text{carry} = 71FC$

Checksum

- ◆ Can be 8-, 16- or 32-bit integers
- ◆ Easy to do - uses only addition
- ◆ May not detect all errors

Data Item In Binary	Checksum Value	Data Item In Binary	Checksum Value
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
totals	7		7

Cyclic Redundancy Check (CRC)

- ◆ Problem : How can a network system detect more errors without increasing the amount of information in each packet?
- ◆ Answer: Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC)

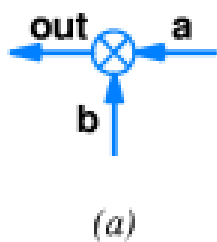
- ◆ Consider data in message as coefficients of a polynomial
- ◆ Divide that coefficient set by a known polynomial
- ◆ Transmit remainder as CRC
 - Good error detection properties
 - Easy to implement in hardware

Hardware Components

- ◆ Uses two hardware components:
 - Shift Register
 - Exclusive or (xor) unit

Hardware Components

- ◆ Exclusive OR (XOR) unit

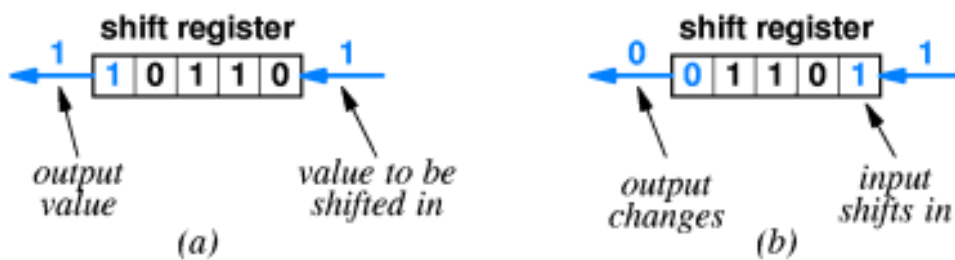


a	b	out
0	0	0
0	1	1
1	0	1
1	1	0

(b)

Hardware Components

- ◆ Shift Register: Performs two operations:
 - Initialize : Sets all bits to zero
 - Shift: Moves all bits to the left one position



SUMMARY

- ◆ Byte Stuffing
- ◆ Transmission Errors
- ◆ Error Detection
 - Parity Check
 - Checksum
 - CRC

COMPUTER NETWORKS

CS610

Lecture-6

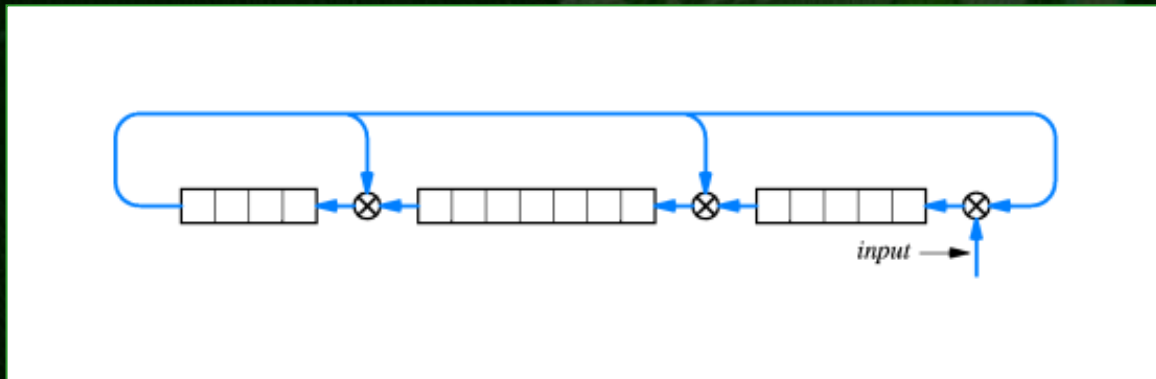
Hammad Khalid Khan

Review of lecture 5

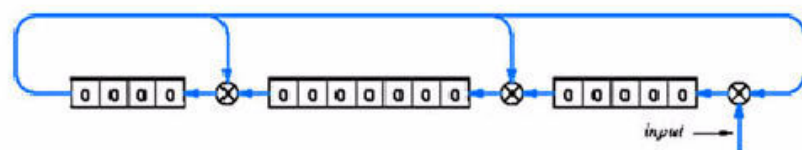
- ◆ Byte Stuffing
- ◆ Transmission Errors
- ◆ Error Detection
 - Parity Check
 - Checksum
 - CRC

Chapter 7 (cont'd) Combining Building Blocks

- ◆ Example 16-bit CRC hardware that uses three shift registers and three exclusive or (xor) units



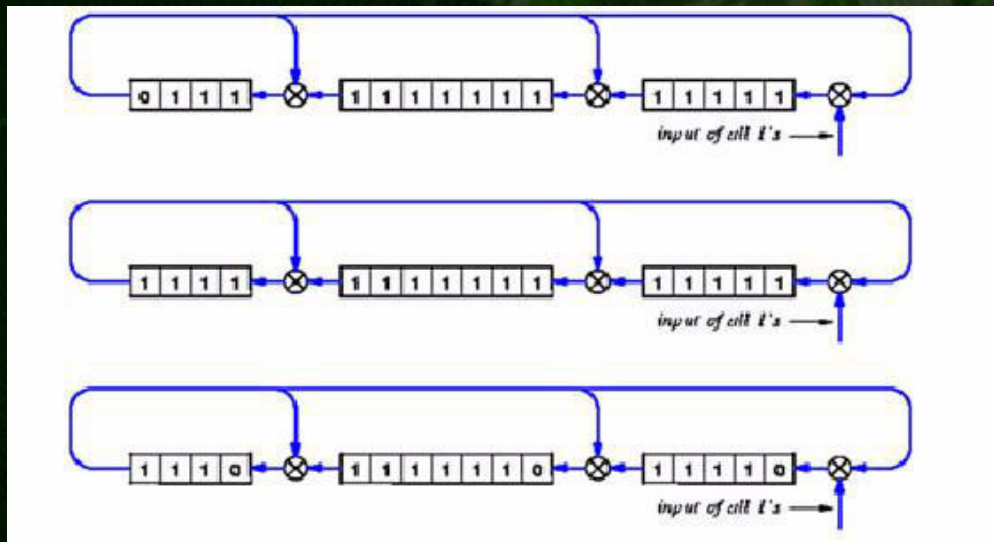
Combining Building Blocks (cont'd)



- Computes 16-bit CRC
- Registers initialized to zero
- Bits of message shifted in
- CRC found in registers

Combining Building Blocks (cont'd)

- Input data is all 1s
- CRC shown after 15,16,17 bits shifted
- Feedback introduces 0s in CRC



**DIRECT POINT-TO-POINT
COMMUNICATION**

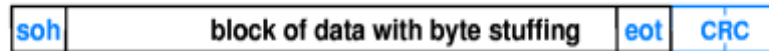
Types of Errors

- CRCs can detect the following errors better than checksums
 - Vertical errors: Occur due to a hardware failure e.g. Damaged second bit of every character
 - Burst errors: Changing a small set of bits near a specific location, caused by lightening, electric motor start, etc.

Frame Format And Error Detection

- Modified frame format including CRC
- Error in frame typically causes receiver to discard frame
- Is Byte stuffing also required for CRC itself?

Frame Format And Error Detection



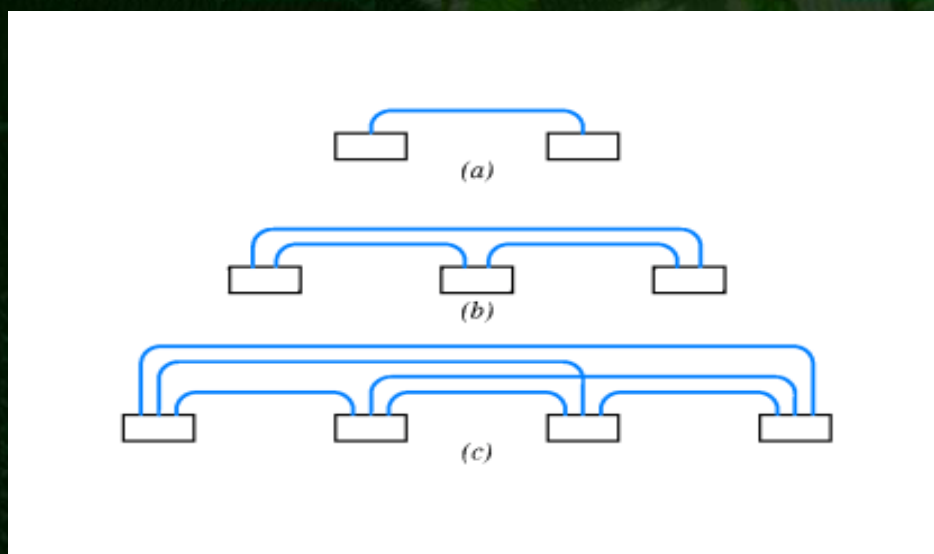
CHAPTER No. 8 LAN TECHNOLOGIES and NETWORK TOPOLOGIES

Introduction

- ◆ Most networks are Local and are designed to share resources among multiple computers
- ◆ Hardware technologies used for Local networks allow multiple devices to connect with a shared network
- ◆ The computers must take turns using the shared medium

Direct Point-to-Point Communication

- ◆ Each communication channel connects exactly two computers
- ◆ Form a MESH or a POINT-to-POINT network



Direct Point-to-Point Communication

♦ Advantages:

- The connection type of individual connections can be different
- Individual connection can choose a different frame format, error detection mechanisms, etc
- Easy to enforce Security and Privacy

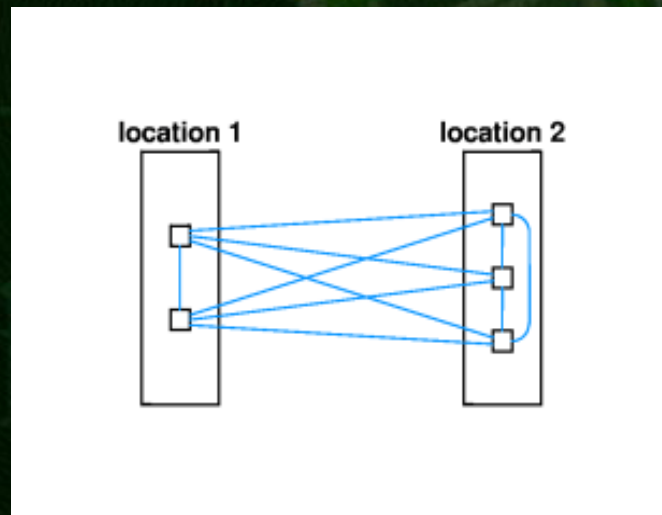
Direct Point-to-Point Communication

♦ Disadvantages:

- The number of connections grow more rapidly than the number of computers
 - For 'N' computers:
$$\text{Connections} = \frac{N^2 - N}{2}$$
- Most connections use the same physical path
- Expensive

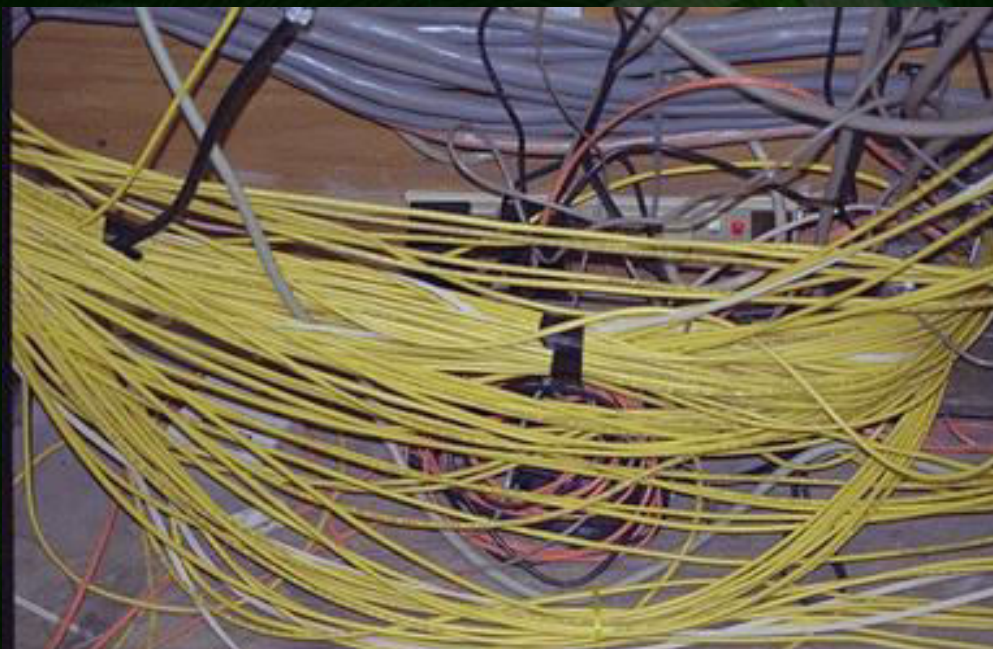
Direct Point-to-Point Communication

- ◆ Disadvantages:
 - Adding a new computer to the network requires 'N-1' new connections



Star Topology in Practice

- ◆ The Result is:



Summary

- ◆ CRC Hardware Components
- ◆ Frame Format and CRC
- ◆ LAN technology and Network topology (Chapter 8)
- ◆ Direct Point-to-Point Communication

COMPUTER NETWORKS

CS610

Lecture-7

Hammad Khalid Khan

Review Lecture 6

- ◆ CRC Hardware Components
- ◆ Frame Format and Error Detection
- ◆ LAN technology and Network Topology (Chapter 8)
- ◆ Direct Point-to-Point Communication

Shared Communication Channels

- ◆ LANs developed in late 1960s and early 1970s
- ◆ Key idea
 - Reduce number of connections by sharing connections among many computers

Shared Communication Channels

- ◆ Each LAN consists of a single shared medium
- ◆ The computers take turns using the medium
- ◆ Sharing a single medium over long distances is inefficient, due to the long delays

Growth of LAN Technologies

- ◆ LAN technologies reduce cost by reducing number of connections
- ◆ But ... attached computers compete for use of shared connection
- ◆ Local communication almost exclusively LAN
- ◆ Long distance almost exclusively point-to-point

Significance Of LANs And Locality Of Reference

- LANs are most popular form of computer networks
- LAN technologies are inexpensive
- The demand for LANs is related to the “Locality of Reference” principle

Locality Of Reference Principle

- ◆ Principle of Locality of Reference helps predict computer communication patterns:
 - Spatial (or physical) locality of reference
 - Computers are likely to communicate with other computers that are located nearby
 - Temporal locality of reference
 - Computers are likely to communicate with the same computers repeatedly

Locality Of Reference Principle

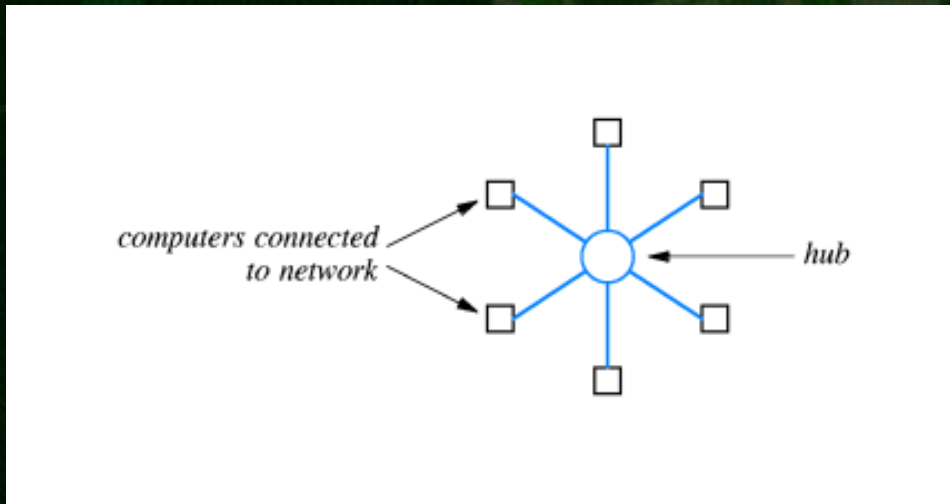
- ◆ Thus
 - LANs are effective because of spatial locality of reference,
 - and
 - Temporal locality of reference may give insight into which computers should be on a LAN

LAN Topologies

- ◆ Networks may be classified by shape
- ◆ Three most popular:
 - Star
 - Ring
 - Bus

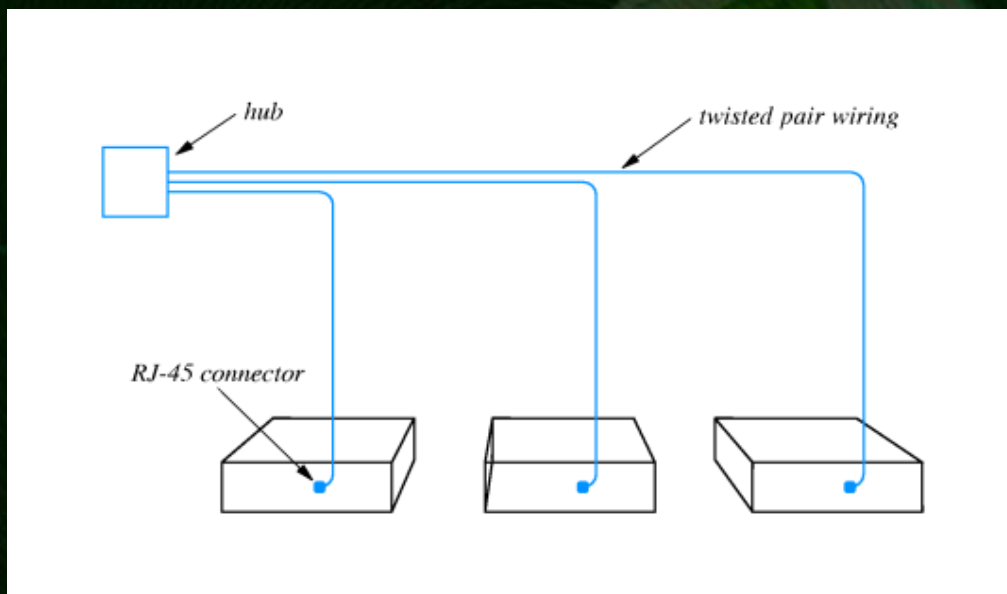
Star Topology

- ◆ All computers are attached to a central point
- ◆ Center of star is sometimes called a “Hub”
- ◆ Logical versus Physical Star



Star Topology in Practice

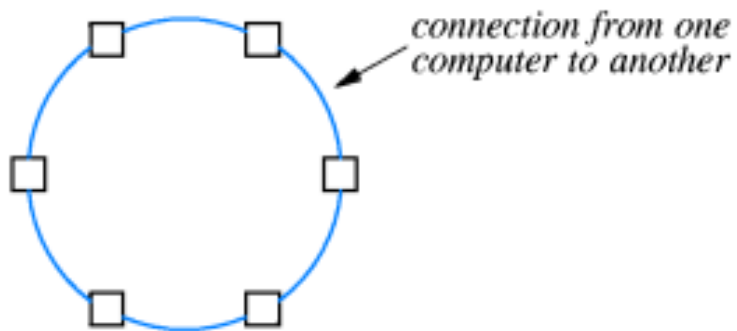
- ◆ Previous diagram is idealized



Ring Topology

- ◆ Computers connected in a closed loop
- ◆ First passes data to second, second passes data to third, and so on
- ◆ Logical versus Physical Ring

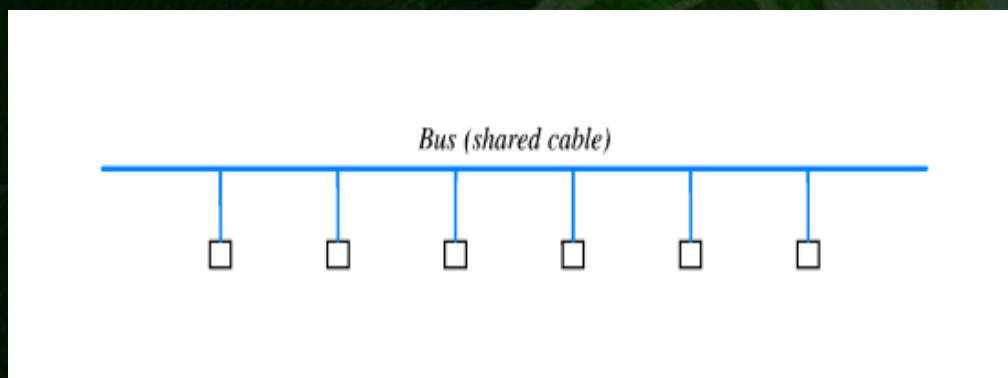
Ring Topology



Bus Topology

- ◆ All computers are attached to a single long cable
- ◆ Any computer can send data to any other computer
- ◆ Coordination required to decide which computer uses the line at what time

Bus Topology



Reason for Multiple Topologies

- ◆ Each topology has advantages and disadvantages
 - In a Ring, it is easy to coordinate access, however entire network is disabled if a cable cut occurs
 - In a Star, only one computer is affected, when a cable cut occurs
 - In a Bus, needs fewer wires than a star, however entire network is disabled when a cable cut occurs

Example Bus Network: Ethernet

- ◆ Widely used LAN technology
 - Invented at Xerox PARC (Palo Alto Research Center) in 1970s
 - Defined in a standard by Xerox, Intel and Digital Equipment Corporation - *DIX* standard
 - Standard now managed by IEEE (802.3) defines formats, voltages, cable lengths, ...

Example Bus Network: Ethernet

- ◆ Uses Bus Topology
 - Single coax cable - the Ether
 - Multiple computers connect
- ◆ One Ethernet cable is sometimes called a Segment
 - Limited to 500 meters in length
 - Minimum separation between connections is 3 meters

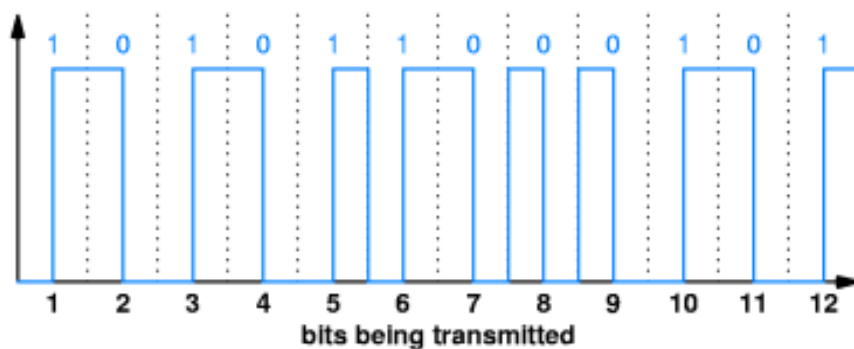
Ethernet Speeds

- ◆ Originally 3Mbps
- ◆ Current standard is 10Mbps
- ◆ Fast Ethernet operates at 100Mbps
- ◆ Giga-Bit Ethernet

Encoding used in Ethernet

- ◆ Manchester Encoding: Uses signal changes to encode data
 - A change from positive voltage to 0 encodes a 0 bit
 - A change from 0 voltage to positive voltage encodes a 1 bit

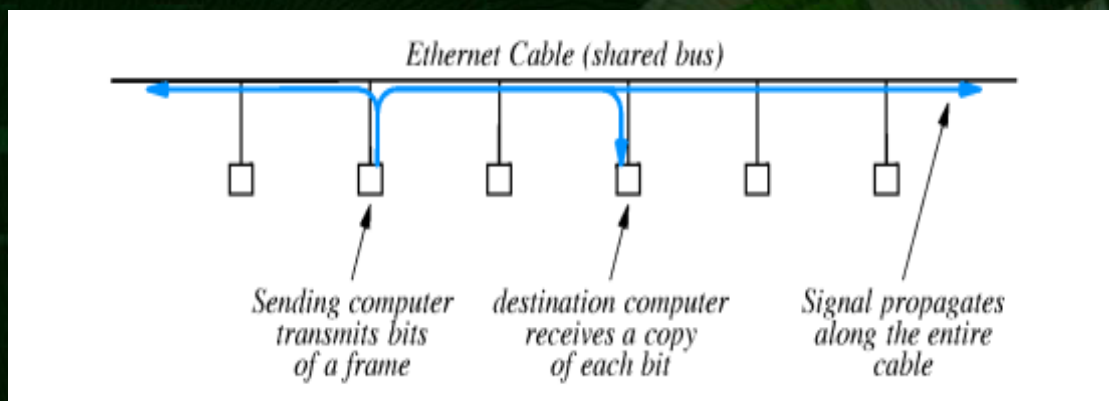
Encoding used in Ethernet



Ethernet Operation

- ◆ One computer transmits at a time
- ◆ Signal propagates from transmitter in both directions along length of segment

Ethernet Operation



Carrier Sense Multiple Access Networks (CSMA)

- ◆ No central control management when computers transmit on Ether
- ◆ Ethernet employs CSMA to coordinate transmission among multiple attached computers

Summary

- ◆ Shared Communication Channel
- ◆ Locality of Reference Principle
- ◆ LAN Topologies
 - Star
 - Ring
 - Bus
- ◆ Ethernet

COMPUTER NETWORKS

CS610

Lecture-8

Hammad Khalid Khan

Review Lecture 7

- ◆ Shared Communication Channel
- ◆ Locality of Reference Principle
- ◆ LAN Topologies
 - Star
 - Ring
 - Bus
- ◆ Ethernet

Carrier Sense Multiple Access

- ◆ A coordination scheme that defines how to take turns using a shared cable
- ◆ A computer listens to the cable (carrier sense)
 - If the cable is idle then starts transmitting
 - If the cable is in use, then waits
- ◆ If Simultaneous transmissions occur, the frames interfere with each other called a Collision

Collision Detection - CD

- ◆ Signals from two computers will interfere with each other
- ◆ Overlapping frames is called a Collision
 - No harm to hardware
 - Data from both frames is Garbled

Ethernet CD

- ◆ Ethernet interfaces include hardware to detect transmission
 - Monitor outgoing signal
 - Garbled signal is interpreted as a collision
- ◆ After collision is detected, computer stops transmitting
- ◆ So, Ethernet uses CSMA/CD to coordinate transmissions

Recovery from Collision

- ◆ Computer that detects a collision sends special signal to force all other interfaces to detect collision
- ◆ Computer then waits for ether to be idle before transmitting
 - If both computers wait same length of time, frames will collide again
 - Standard specifies maximum delay, and both computers choose random delay less than maximum

Recovery from Collision

- ◆ After waiting, computers use carrier sense to avoid subsequent collision
 - Computer with shorter delay will go first
 - Other computers may transmit later

Exponential Backoff

- ◆ Even with random delays, collisions may occur
- ◆ Especially likely with busy segments
- ◆ Computers double delay with each subsequent collision
- ◆ Reduces likelihood of sequence of collisions

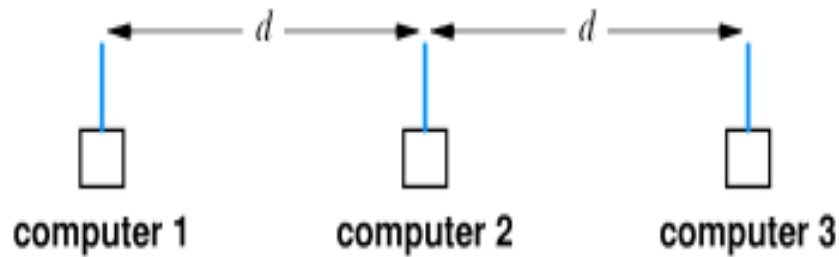
802.11 Wireless LANs And CSMA/CA

- ◆ Use radio signals at 2.4 GHz (IEEE 802.11)
- ◆ Data rate at 11Mbps
- ◆ Older devices use radio signals at 900MHz
- ◆ Data rate of 2Mbps
- ◆ Bluetooth specifies a wireless LAN for short distances
- ◆ Shared medium - radio instead of coax

Limited Connectivity with Wireless

- ◆ In contrast with wired LAN, not all participants may be able to reach each other
 - Low signal strength
 - Propagation blocked by walls, etc.
- ◆ Can't depend on CD; not all participants may hear

Limited Connectivity with Wireless



CSMA/CA

- ♦ Wireless uses Collision Avoidance rather than Collision Detection
 - Transmitting computer sends very short message to receiver
 - Receiver responds with short message reserving slot for transmitter
- ♦ Response from receiver is broadcast, so all potential transmitters receive reservation

Collisions

- ◆ Receiver may receive simultaneous requests
 - Results in collision at receiver
 - Both requests are lost
 - Neither transmitter receives reservation; both use backoff and retry
- ◆ Receiver may receive closely spaced requests
 - Selects one
 - Selected transmitter sends message
 - Transmitter not selected uses backoff and retries

Limited Connectivity with Wireless



Local Talk

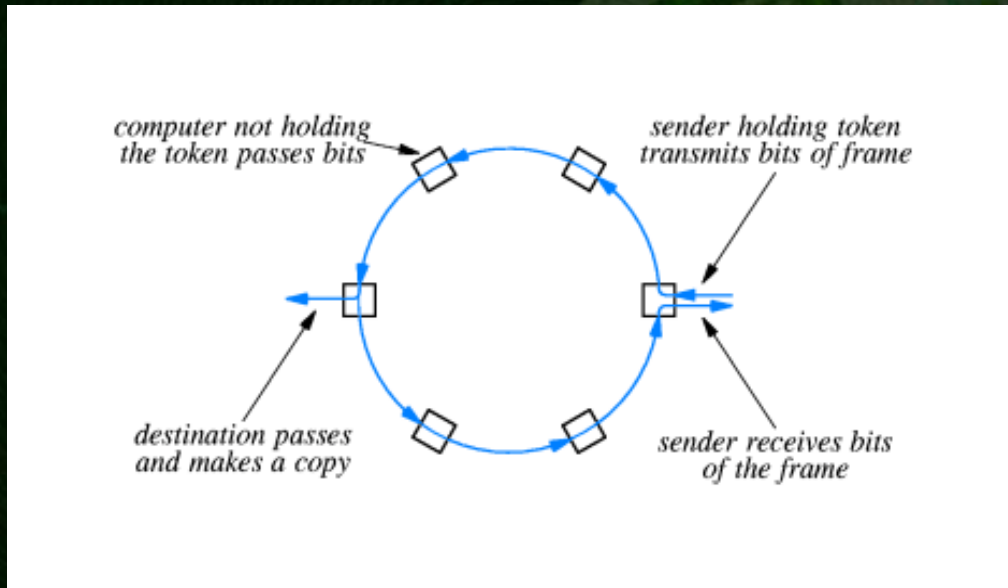
- ◆ LAN technology invented by Apple that uses bus topology
- ◆ Interface included with all Macintosh computers
- ◆ Relatively low speed - 230.4Kbps
- ◆ Low cost ("free" with a Macintosh); easy to install and connect
- ◆ Uses CSMA/CA

Token Ring

- ◆ Many LAN technologies that use ring topology use token passing for synchronized access to the ring
- ◆ Ring itself is treated as a single, shared communication medium
- ◆ Bits pass from transmitter, past other computers and are copied by destination

Token Ring

- ◆ Hardware must be designed to pass token even if attached computer is powered down



Using the token

- ◆ When a computer wants to transmit, it waits for the token
- ◆ After transmission, computer transmits token on ring
- ◆
- ◆ Next computer ready to transmit receives token and then transmits

Token and Synchronization

- ◆ Because there is only one token, only one computer will transmit at a time
 - Token is short, reserved frame that cannot appear in data
 - Hardware must regenerate token if lost

Token and Synchronization

- ◆ Token gives computer permission to send one frame
 - If all ready to transmit, enforces ``Round-Robin" access
 - If none ready to transmit, token circulates around ring

IBM Token Ring

- ◆ Very widely used
- ◆ Originally 4mbps, now 16Mbps
- ◆ Uses special connector cable between computer and ring interface

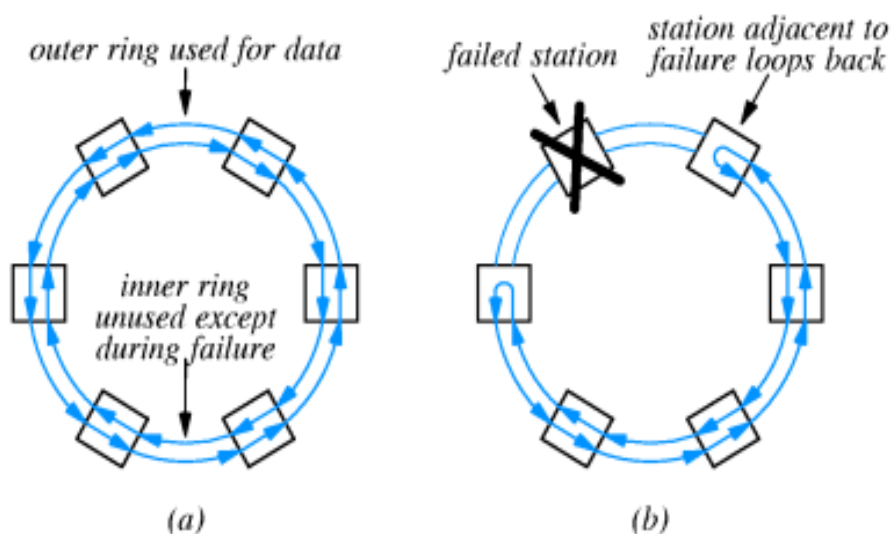
FDDI

- ◆ Fiber Distributed Data Interconnect (FDDI) is another ring technology
 - Uses fiber optics between stations
 - Transmits data at 100Mbps
- ◆ Uses pairs of fibers to form two concentric rings

FDDI and Reliability

- ◆ FDDI uses counter-rotating rings in which data flows in opposite directions
- ◆
- ◆ In case of fiber or station failure, remaining stations loop back and reroute data through spare ring
- ◆ All stations automatically configure loop back by monitoring data ring

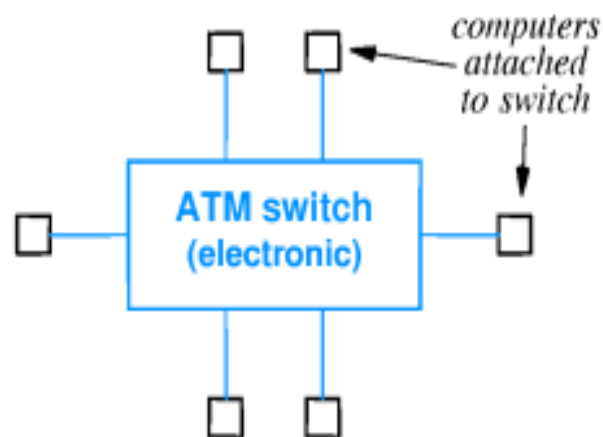
FDDI and Reliability



ATM – Star Network

- ◆ Asynchronous Transfer Mode technology consists of electronic packet switches to which computers can connect
- ◆ ATM switches form hub into which computers connect in a star topology
- ◆ Computers get point-to-point connections - data from transmitter is routed directly through hub switches to destination
 - If none ready to transmit, token circulates around ring
 - If all ready to transmit, enforces ``Round-Robin" access

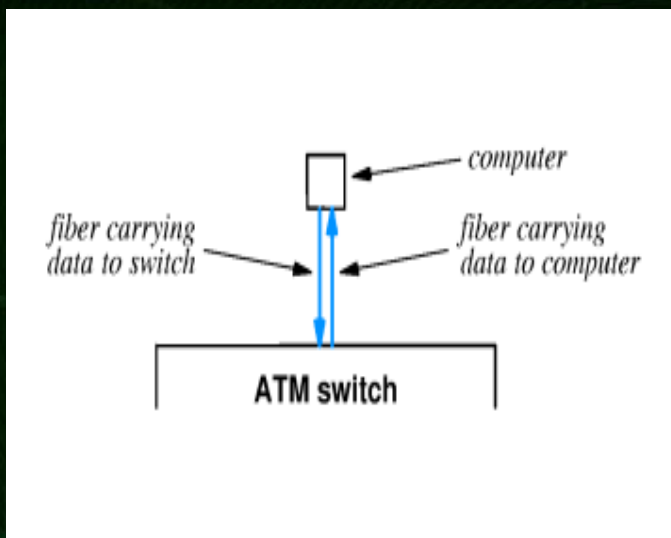
ATM – Star Network



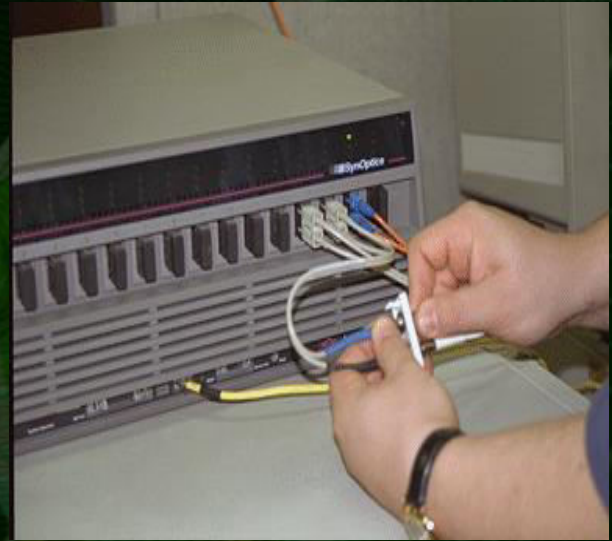
ATM Details

- ◆ Transmits data at over 100Mbps
- ◆ Uses fiber optics to connect computer to switch
- ◆ Each connection includes two fibers

ATM Details



ATM Switches



Summary

- ◆ CSMA/CD
- ◆ Wireless LANs and CSMA/CA
- ◆ Token Ring
- ◆ FDDI
- ◆ ATM

COMPUTER NETWORKS

CS610

Lecture-9

Hammad Khalid Khan

Review Lecture 8

- ◆ CSMA/CD
- ◆ Wireless LANs and CSMA/CA
- ◆ Token Ring
- ◆ FDDI
- ◆ ATM

Chapter 9

Hardware Addressing and Frame Type Identification

Introduction

- ◆ Need to devise technique for delivering message through LAN medium to single, specific destination computer
- ◆
- ◆ Sending computer uses a Hardware Address to identify the intended destination of a frame
- ◆
- ◆ Sending computer also identifies Type of data carried in the frame

Specifying a Destination

- ◆ Data sent across a shared network reaches all attached stations - for all LAN topologies
- ◆ Interface hardware detects delivery of frame and extracts frame from medium
- ◆ But ... most applications want data to be delivered to One specific application on another computer - not All computers

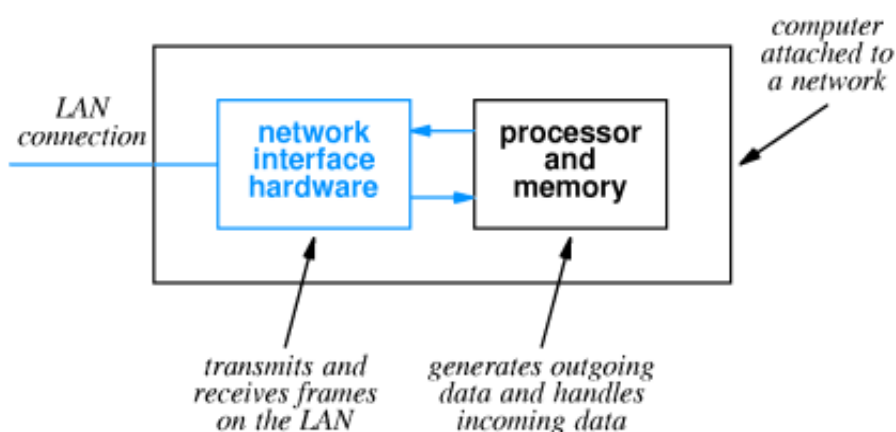
Hardware Addressing

- ◆ Most network technologies have a hardware addressing scheme that identifies stations on the network
- ◆ Each station is assigned a numeric Hardware Address or Physical Address

Hardware Addressing

- ◆ Sender includes hardware address in each transmitted frame
- ◆ Only station identified in frame receives copy of frame
- ◆ Most LAN technologies include sender's hardware address in frame, too

LAN Hardware and Packet Filtering



LAN Interface

- ◆ LAN interface handles all details of frame transmission and reception
 - ◆ Adds hardware addresses, error detection codes, etc. to outgoing frames
 - ◆
 - ◆ May use DMA to copy frame data directly from main memory
 - ◆
 - ◆ Obeys access rules (e.g., CSMA/CD) when transmitting

LAN Interface

- Checks error detection codes on incoming frames
- May use DMA to copy data directly into main memory
- Checks destination address on incoming frames
 - Station's address, a copy of the frame is passed to the attached computer
- Frames not addressed to the local computer are ignored and don't affect the local computer in any way

Format of Hardware Addresses

- ◆ Numeric value
- ◆ Size selected for specific network technology
- ◆ Length is one to six bytes

Assigning Hardware Addresses

- ◆ Hardware addresses must be unique on a LAN
- ◆ How can those address be assigned and who is responsible for uniqueness?

Assigning Hardware Addresses

Static	Hardware manufacturer assigns permanent physical address to each network interface .	Manufacturer must ensure every interface has a unique address
Configurable	Address can be set by end user, either manually (e.g., switches or jumpers on the interface) or electronically (e.g., through software	System administrators must coordinate to avoid conflict
Dynamic	Interface automatically assigns physical address each time it is powered up	Automatic scheme must be reliable to prevent conflicts

Broadcasting

Problems with Broadcasting

- ♦ For every broadcast frame on the network, each computer uses computational resources:
 - Places contents into memory
 - Interrupts the CPU
 - Allows system software to make a decision whether to discard or use the frame

Problems with Broadcasting

- If a pair of computers, use broadcasting, instead of sending them directly, all other computers waste CPU time while discarding the frames.

Multicasting

- ◆ Solution: The restricted form of broadcasting: Multicasting:
 - It works like broadcasting
 - However it does not forward frames automatically to the CPU
 - The interface hardware is programmed in advance to accept certain frames that have multicast address as the destination address

Summary

- ◆ Hardware Addressing
- ◆ Specifying a Destination
- ◆ Packet Filtering
- ◆ Assigning Hardware Addresses
- ◆ Broadcasting
- ◆ Multicasting

COMPUTER NETWORKS

CS610

Lecture-10

Hammad Khalid Khan

Review Lecture 9

- ◆ Hardware Addressing
- ◆ Specifying a Destination
- ◆ Packet Filtering
- ◆ Assigning Hardware Addresses
- ◆ Broadcasting
- ◆ Multicasting

Problems with Broadcasting

- ♦ For every broadcast frame on the network, each computer uses computational resources:
 - Places contents into memory.
 - Interrupts the CPU.
 - Allows system software to make a decision whether to discard or use the frame.

Problems with Broadcasting

- If a pair of computers, use broadcasting, instead of sending them directly, all other computers waste CPU time while discarding the frames.

Multicasting

Multicast Addressing

- ◆ If an application program wishes to receive certain frames, then
 - it programs the interface hardware to accept an additional set of addresses.
- ◆ The interface hardware then begins accepting:
 - those frames (multicast frames),
 - broadcast frames and
 - frames that are destined to the station itself.

Multicast Addressing

- ◆ For example: Computers running an audio application
 - can receive audio frames, if the interfaces are programmed to receive them.
 - The other computers that are not running that audio application will not waste resources.

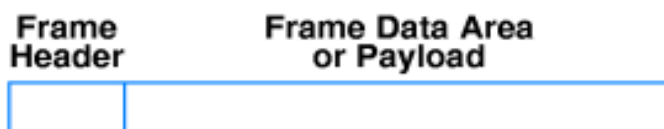
Identifying Packet Contents

- ◆ Destination must get some clue about how to interpret frame data.
- ◆ Can use:
 - Explicit Frame Type - Identifying value included with frame describes type of included data.
 - Implicit Frame Type - Receiver must infer type from frame data.

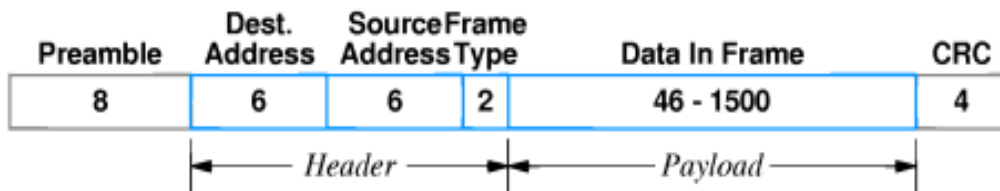
Headers and Frame Formats

- ◆ LAN technology standards define frame format for each technology.
- ◆ All contemporary standards use the following general format:
 - Frame header has address and other identifying information.
 - Information typically in fields with fixed size and location.
 - Data area may vary in size.

Headers and Frame Formats



Ethernet Frame Format



Ethernet Frame Format

<u>Field</u>	<u>Purpose</u>
Preamble	Receiver synchronization
Dest. addr.	Identifies intended receiver
Source addr.	Hardware address of sender
Frame type	Type of data carried in frame
Data	Frame payload
CRC	32-bit CRC code

Ethernet Fields

- ◆ Preamble and CRC often not shown
- ◆ Destination address of all 1s is the broadcast address.
- ◆ Special values are reserved for frame type field.

Ethernet Fields

Value	Meaning
0000-05DC	Reserved for use with IEEE 802.3
0800	Internet IP Version 4
0805	CCITT X.25
0900	Ungermann-Bass Corporation network debugger
0BAD	Banyan Systems Corporation VINES
1000-100F	Berkeley UNIX Trailer encapsulation
6004	Digital Equipment Corporation LAT
6559	Frame Relay
8005	Hewlett Packard Corporation network probe
8008	AT&T Corporation
8014	Silicon Graphics Corporation network games
8035	Internet Reverse ARP
8038	Digital Equipment Corporation LANBridge
805C	Stanford University V Kernel
809B	Apple Computer Corporation AppleTalk
80C4-80C5	Banyan Systems Corporation
80D5	IBM Corporation SNA
80FF-8103	Wellfleet Communications
8137-8138	Novell Corporation IPX
818D	Motorola Corporation
FFFF	Reserved

Frames without Type Fields

- ◆ Some LAN technologies do not include a type field.
- ◆ Sender and receiver can agree on interpretation:
 - Agree on a single data format and use only that format.
 - Limits LAN to one type of data.
 - All computers on LAN must use one format.
 - Agree to encode the data format in the first few bytes of the data field.

Encoding the Data Type

- ◆ Illustration of using data area to encode data type:



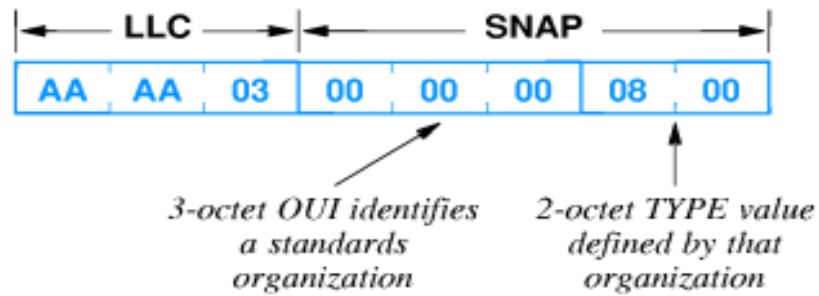
Encoding the Data Type

- ◆ To ensure interoperability, format of encoding area must be universally agreed upon.
- ◆ Format typically set by standards body.

IEEE 802.2 LLC

- ◆ To ensure IEEE 802.2 standard includes Logical Link Control (LLC) Sub Network Attachment Point (SNAP) header.
- ◆ SNAP/LLC format widely used; e.g., by Ethernet.

IEEE 802.2 LLC



IEEE 802.2 LLC

- ♦ LLC portion indicates SNAP field to follow.
- ♦ OUI (Organizationally Unique Identifier) identifies Ethernet specification organization.
- ♦
- ♦ TYPE field interpreted as in Ethernet (in this case, IP).

Unknown Types

- ◆ For either encoding format, some computers may not be prepared to accept frames of some types like:
 - Protocol type not installed
 - Newly defined type
- ◆ Receiving computer examines type field and discards any frames with unknown type.

Network Analyzers

- ◆ A network analyzer or network monitor or Network Sniffer is used to examine the performance of or debug a network.
- ◆ Can report statistics such as capacity utilization, distribution of frame size, collision rate or token circulation time.

Operation of Network Analyzer

- ◆ Basic idea is a computer with a network interface that receives all frames.
- ◆ Sometimes called Promiscuous Mode.
- ◆ Many desktop computers have interface that can be configured for promiscuous mode.
- ◆
 - Combined with software, computer can examine any frame on LAN.
 - Communication across a LAN is not guaranteed to be private!

Operation of Network Analyzer

- ◆ Computer receives and displays (but does not respond to) frames on the LAN.

Filtering Incoming Frames

- ◆ Analyzer can be configured to filter and process frames.
 - Count frames of a specific type or size.
 - Display only frames from or to specific computers.
 - In general, can be configured to match value of any field and capture only those frames meeting the filter specification.

Summary

- ◆ Multicasting
- ◆ Frame Type Identification
- ◆ Ethernet Frame Format
- ◆ Frame Without Type Fields
- ◆ Network Analyzer

COMPUTER NETWORKS

CS610

Lecture-11

Hammad Khalid Khan

Review Lecture 10

Multicasting

Frame Type Identification

Ethernet Frame Format

Frame Without Type Fields

Network Analyzer

Chapter 10

LAN WIRING, PHYSICAL TOPOLOGY, and INTERFACE HARDWARE

Introduction

- ◆ Interface cards:
 - Why a separate card?
 - How to connect the interface to the computer?
 - What is a Transceiver?
- ◆ LAN Wiring Schemes
- ◆ Logical and Physical Topology

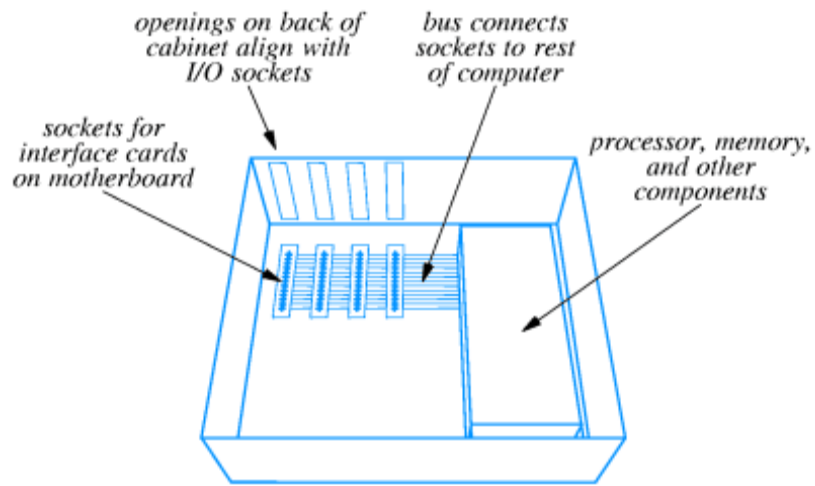
Speeds of LANs and Computers

- ◆ LAN data transmission speeds are typically Fast relative to CPU speeds.
- ◆ LAN speeds are defined independent of any specific processor speeds.
 - Allows for mix of attached systems.
 - New computers can be attached without affecting LAN speeds.

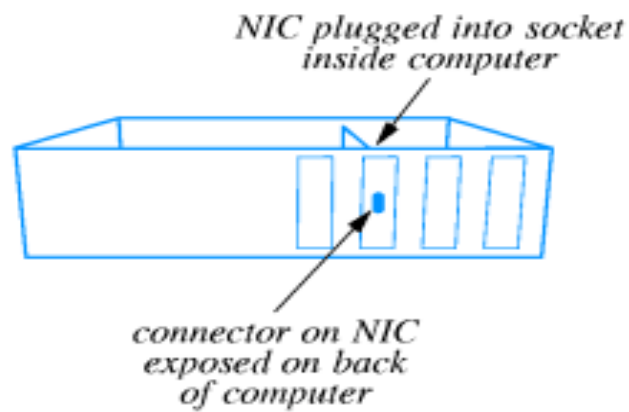
Network Interface Hardware

- ◆ CPU can't process data at network speeds.
- ◆ Computer systems use special purpose hardware for network connection.
 - Typically a separate card in the backplane.
 - Network adapter card or network interface card (NIC).
- ◆ Connector at back of computer then accepts cable to physical network.

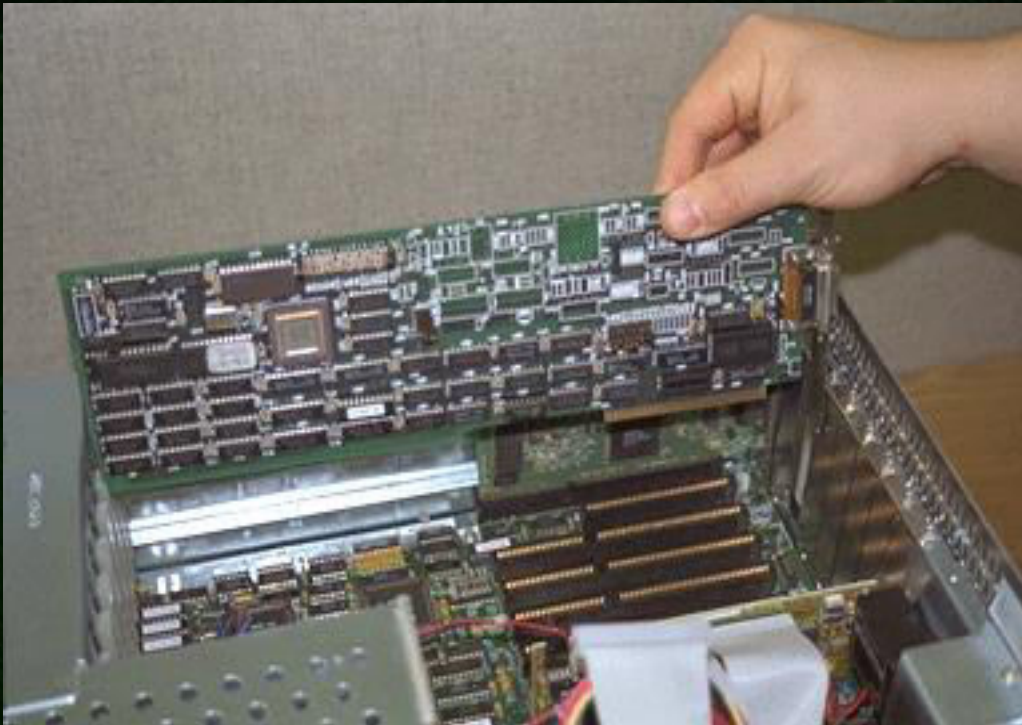
I/O Interfaces



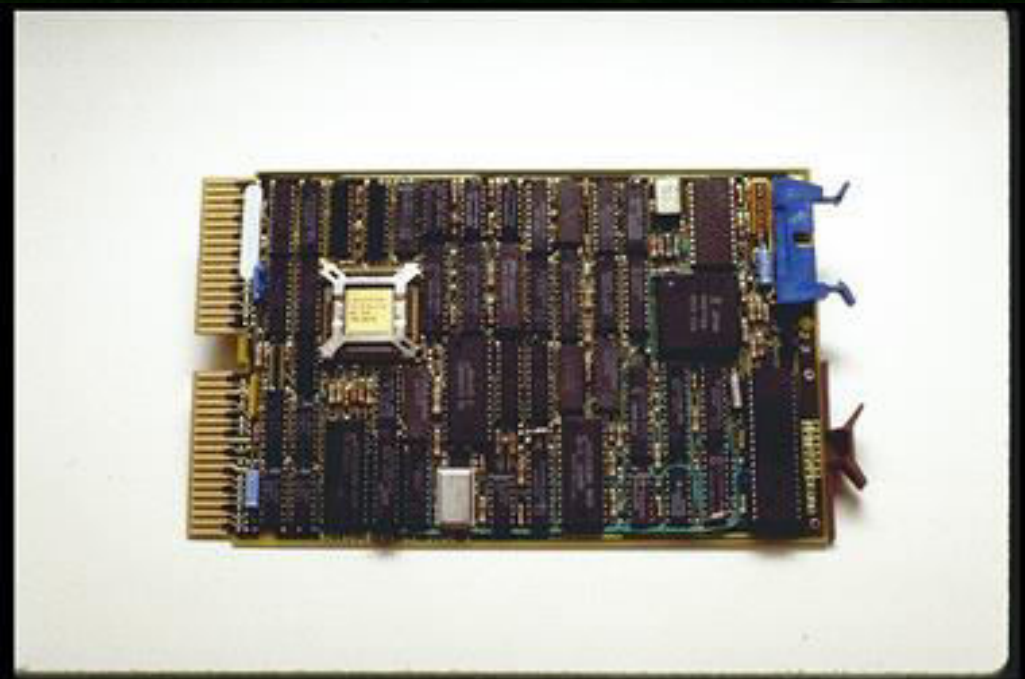
Network Connector



Network Interface Card (NIC)



Network Interface Card (NIC)



NICs and Network Hardware

- ◆ NIC is built for one kind of physical network.
 - Ethernet interface can't be used with token ring.
 - ATM interface can't be used with FDDI.
- ◆ Some NICs can be used with different, similar hardware.
 - Thick, thin and 10Base-T Ethernet.
 - 10Mbps and 100Mbps Ethernet.

NIC and CPU Processing

- ◆ NIC contains sufficient hardware to process data independent of system CPU.
 - Some NICs contain separate microprocessor.
 - Includes analog circuitry, interface to system bus, buffering and processing.
- ◆ Looks like any other I/O device to system CPU.
 - System CPU forms message request.
 - Sends instructions to NIC to transmit data.
 - Receives interrupt on arrival of incoming data.

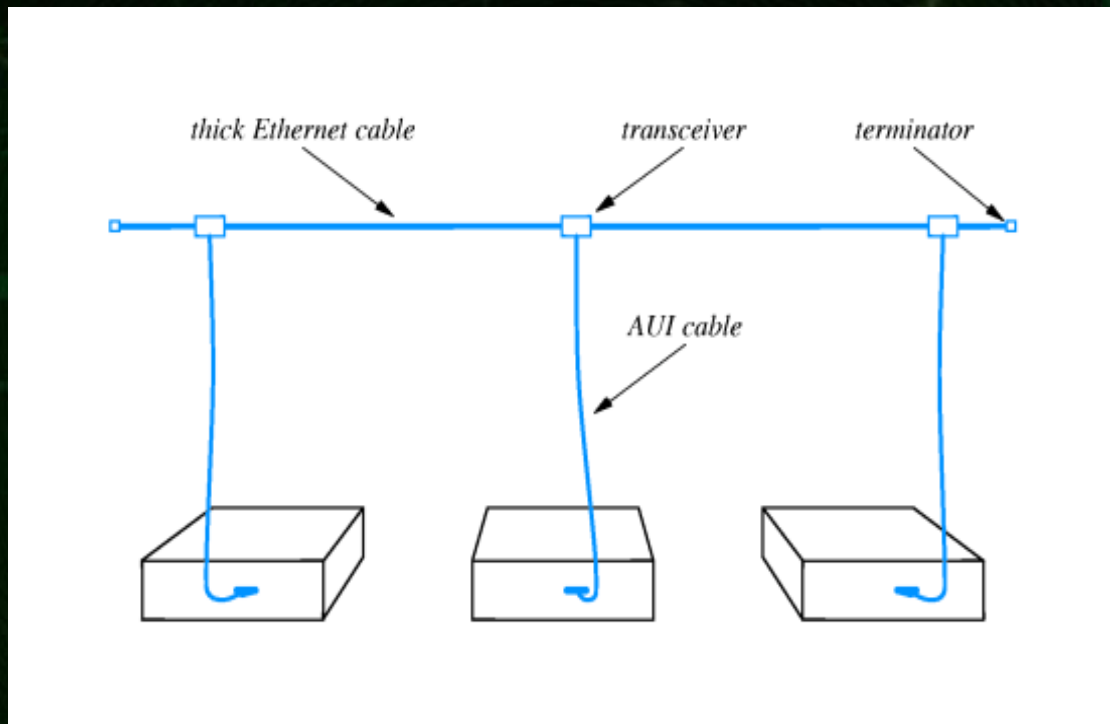
Connection between NIC and Physical Network

- ◆ Two alternatives:
 - NIC contains all circuitry and connects directly to network medium.
 - Cable from NIC connects to additional circuitry that then attaches to the network medium.
- ◆ Thin Ethernet vs. 10Base-T:
 - Both are Ethernet; network technology not limited to one style of connection.

Thick Ethernet Wiring

- ◆ Uses thick coax cable.
- ◆ AUI cable (or transceiver or drop cable connects from NIC to transceiver.
- ◆ AUI cable carries digital signal from NIC to transceiver.
- ◆ Transceiver generates analog signal on coax.
- ◆ Wires in AUI cable carry digital signals, power and other control signals.
- ◆ Thick Ethernet also requires Termination to avoid signal reflectance.

Thick Ethernet Example



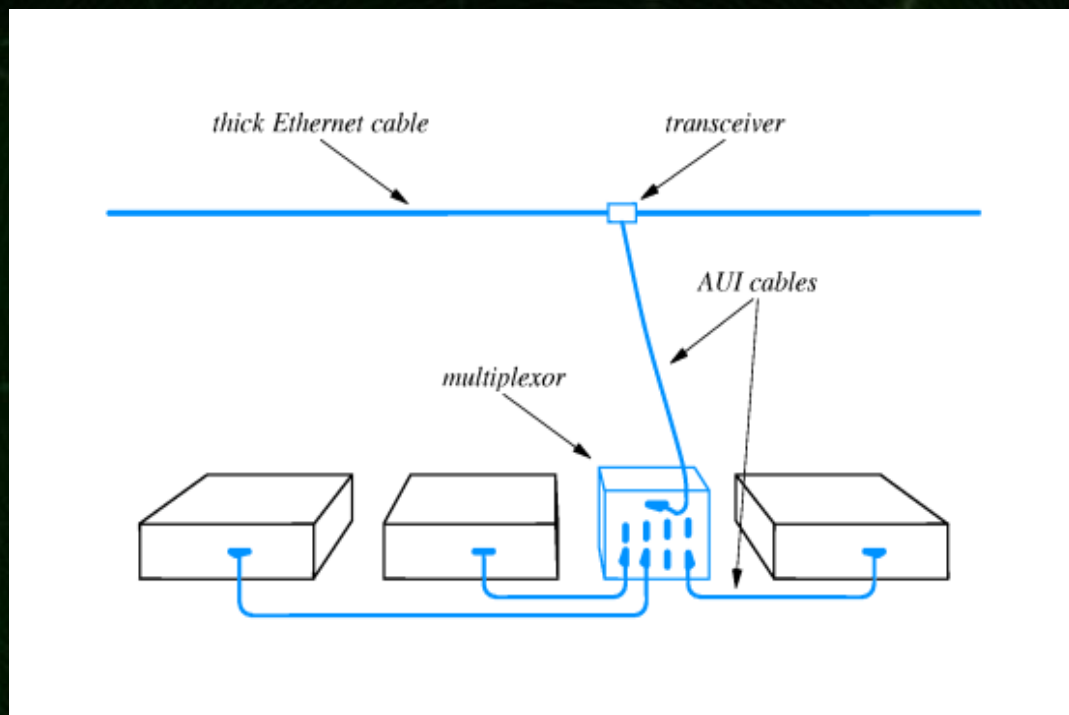
Thick Ethernet
(10 base 5)

Thin Ethernet (10 base 2)

Connection Multiplexing

- ◆ In some circumstances, transceivers may be inconvenient; e.g., workstations in a lab.
- ◆ Connection Multiplexer connects multiple computers to a single transceiver.
 - Each computer's AUI cable connects to connection multiplexor.
 - One AUI from multiplexor to Ethernet coax.

Connection Multiplexing



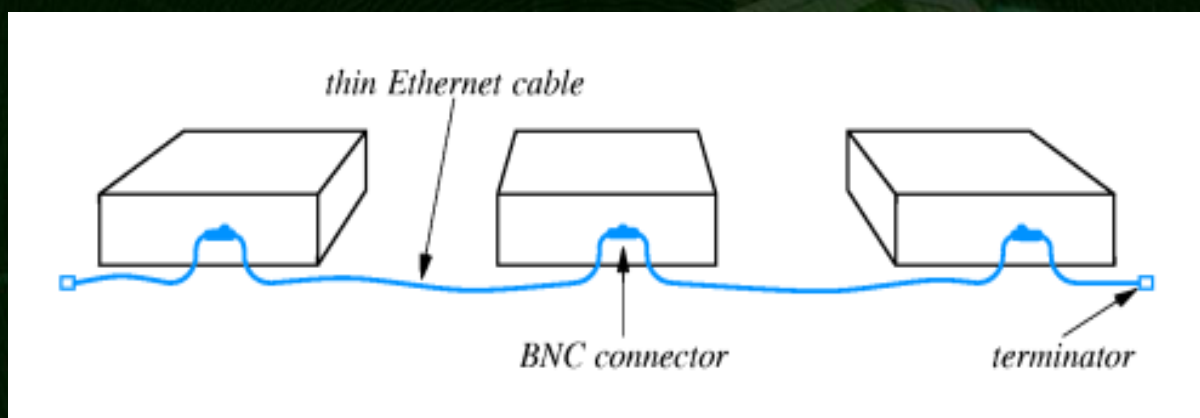
Thin Ethernet Wiring

- ◆ Uses thin coax that is cheaper and easier to install than thick Ethernet coax.
- ◆ Transceiver electronics built into NIC; NIC connects directly to network medium.
- ◆ Coax cable uses BNC connector.

Thin Ethernet Wiring

- ♦ Coax runs directly to back of each connected computer.
- ♦ T-Connector attaches directly to NIC.

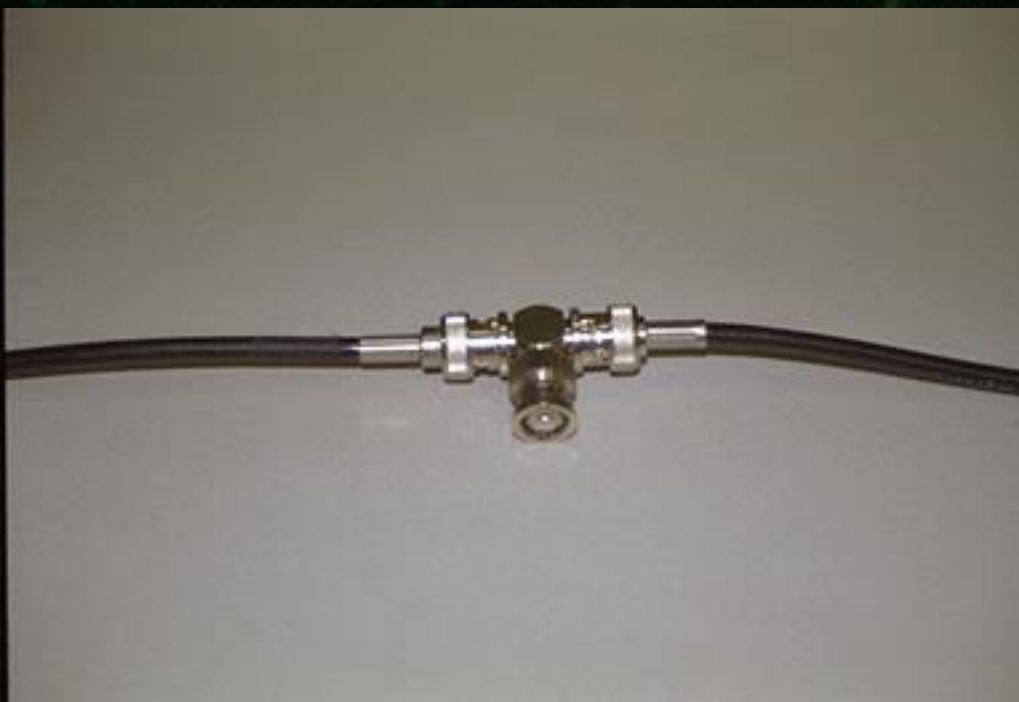
Thin Ethernet Wiring



Thin Ethernet



Thin Ethernet



Thin Ethernet

- ♦ Useful when many computers are located close to each other.
- ♦ May be unreliable - any disconnection disrupts entire net.

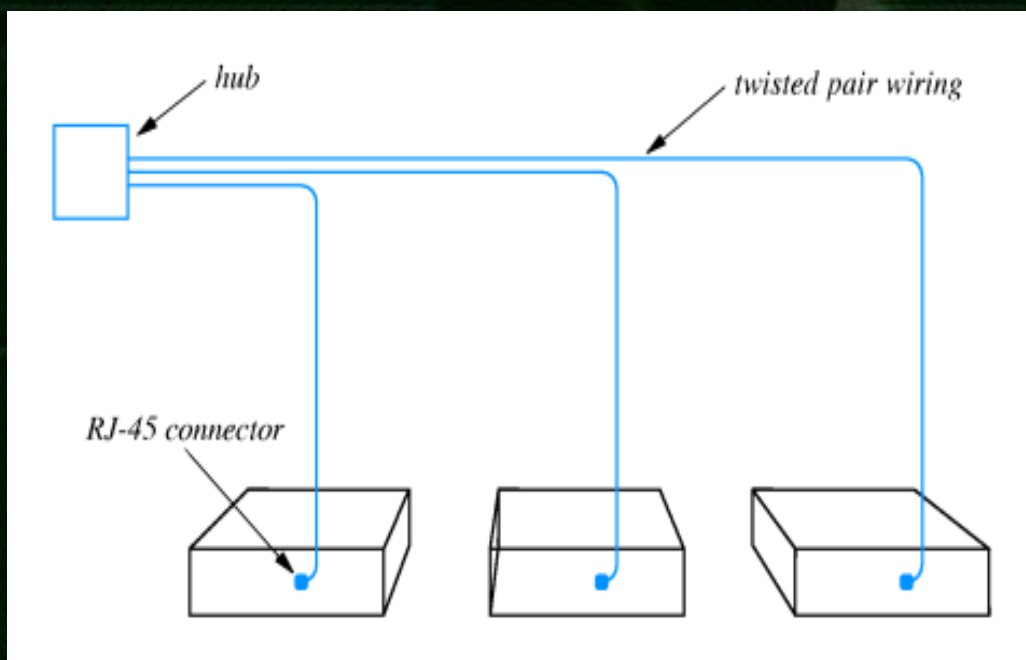
Thin Ethernet



10Base-T

- ◆ Commonly called 10Base-T, Twisted Pair or TP Ethernet.
- ◆ Replaces AUI cable with twisted pair cable.
- ◆ Replaces thick coax with Hub.

10Base-T



10Base-T



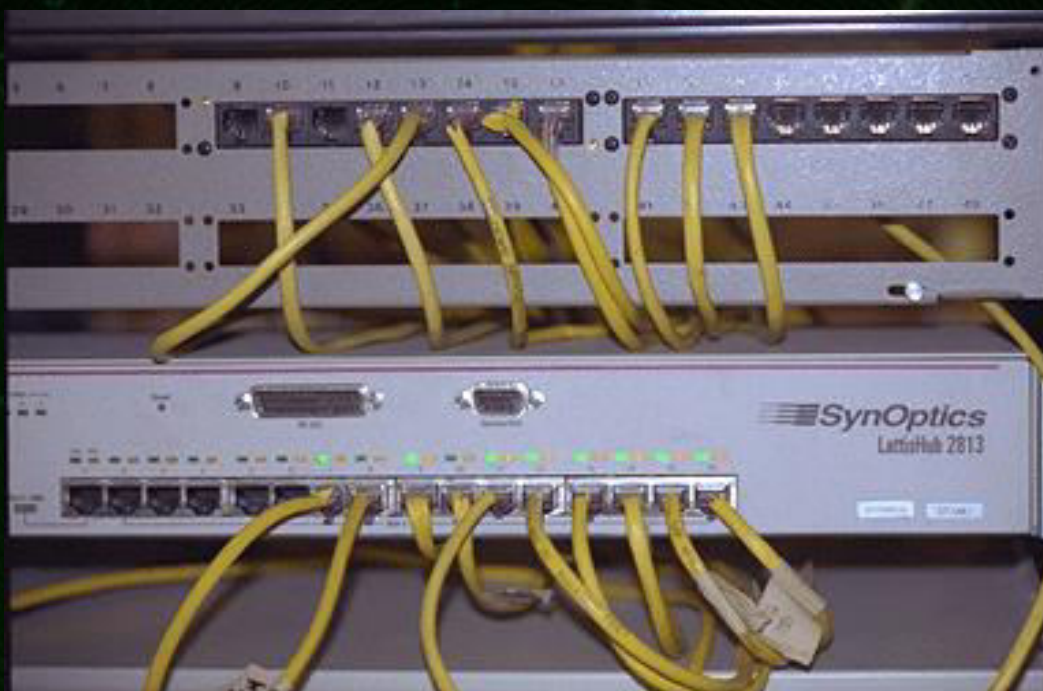
10Base-T



Hubs

- ◆ Extension of connection multiplexing concept.
- ◆ Sometimes called “Ethernet-in-a-Box”.
- ◆ Effectively a very short Ethernet with very long AUI cables.
- ◆ Can be connected into larger Ethernets.

Hubs



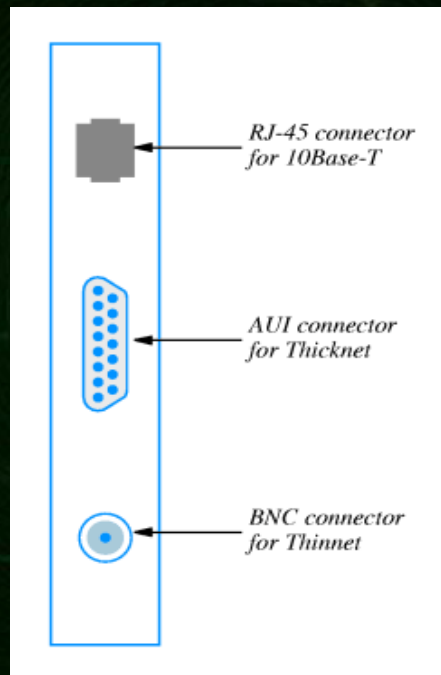
Hubs



Protocol Software and Ethernet Wiring

- ♦ All wiring technologies use identical Ethernet specification.
 - Same frame format.
 - Same CSMA/CD algorithms.
- ♦ Can mix different technologies in one Ethernet.
- ♦ NICs can provide all three connection technologies.
- ♦ Protocol software can't differentiate among wiring technologies.

Protocol Software and Ethernet Wiring



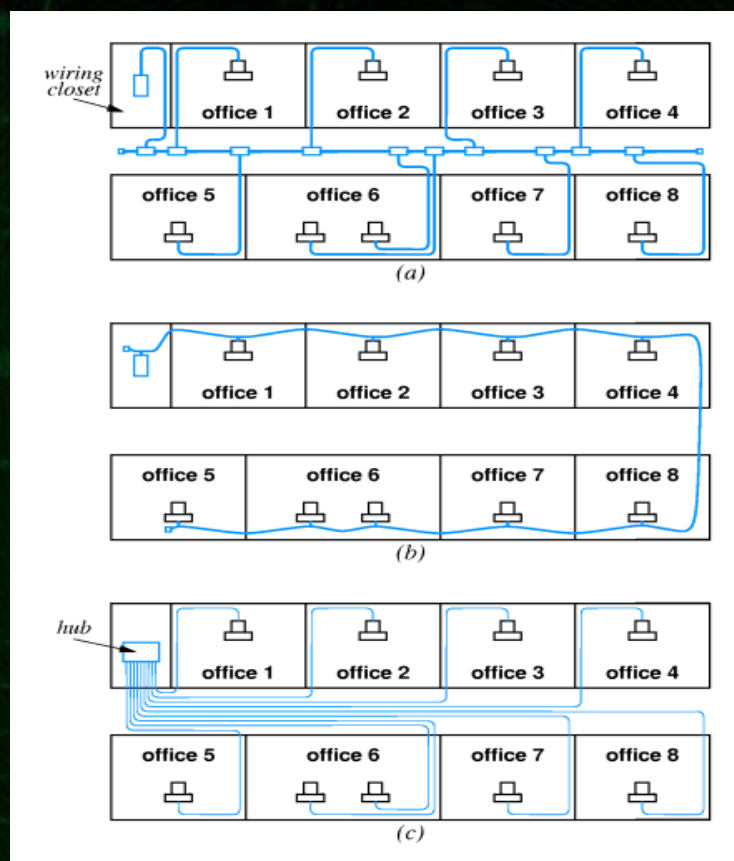
Comparison of Wiring Schemes

- ◆ Separate transceiver allows computer to be powered off or disconnected from network without disrupting other communication.
- ◆ Transceiver may be located in an inconvenient place.
- ◆ Finding malfunctioning transceiver can be hard.

Comparison of Wiring Schemes

- ♦ Thin coax takes minimum of cable.
- ♦ Disconnecting one computer (or one loose connection) can disrupt entire network.
- ♦ Hub wiring centralizes electronics and connections, making management easier.
- ♦ Bottom line - 10Base-T most popular because of cost.

Comparison of Wiring Schemes



Topologies and Network Technologies

- ◆ 10Base-T network topology is a bus; wiring topology is a star.
- ◆ Token ring network topology is a ring; wiring topology is a star.
- ◆ Remember to distinguish between Logical and Physical Topologies.

Filtering Incoming Frames

- ◆ Analyzer can be configured to filter and process frames.

Summary

- ◆ Network Interface Hardware
- ◆ Connection Between NIC and Physical Network
- ◆ Thick Ethernet (10 BASE 5)
- ◆ Thin Ethernet (10 BASE 2)
- ◆ 10BASE-T
- ◆ Comparison Of Wiring Schemes

COMPUTER NETWORKS

CS610

Lecture-12

Hammad Khalid Khan

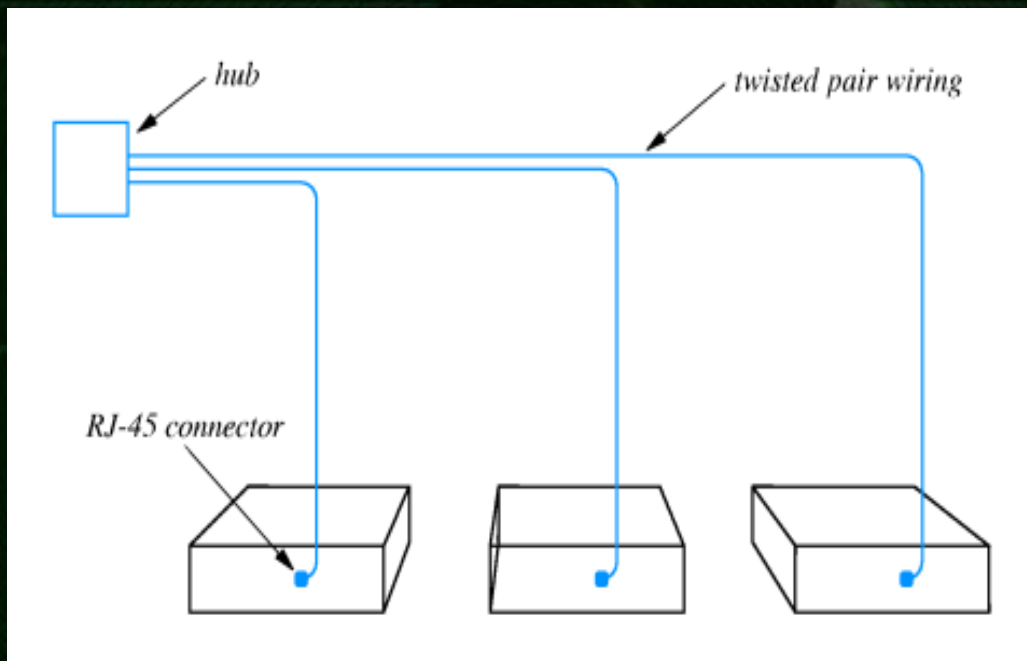
Review Lecture 11

- ◆ Network Interface Hardware
- ◆ Connection Between NIC and Physical Network
- ◆ Thick Ethernet (10 BASE 5)
- ◆ Thin Ethernet (10 BASE 2)
- ◆ 10BASE-T
- ◆ Comparison Of Wiring Schemes

10Base-T

- ◆ Formally known as 10BaseT
- ◆ Does not use coaxial cable, uses twisted pair wiring with RJ-45 connectors
- ◆ Each computer has a dedicated connection to a central electronic device called an Ethernet Hub

10Base-T



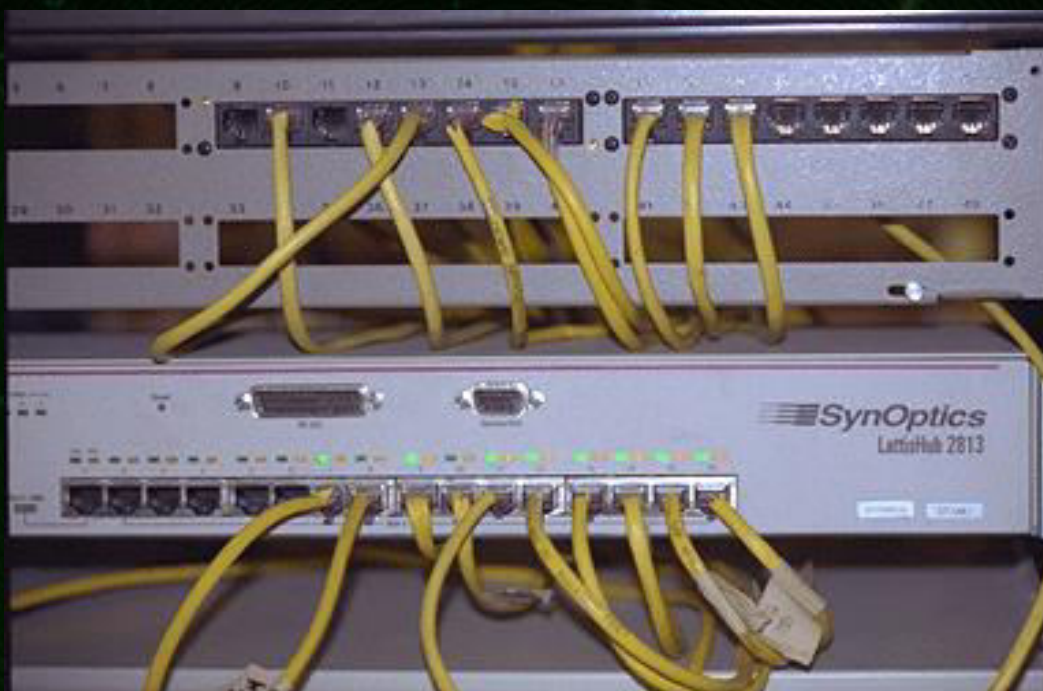
10Base-T



Hubs

- ◆ Extension of connection multiplexing concept
- ◆
- ◆ Sometimes called “Ethernet-in-a-Box”
- ◆ Electronic components in a Hub simulate a shared physical cable, making the entire system operate like a conventional Ethernet

Hubs



Hubs



Advantages and Disadvantages of Wiring Schemes

- ♦ Each of the three wiring schemes has advantages and disadvantages:
 - **Reliability issues:**
 - Wiring that uses a transceiver for each connection does not affect the entire network if a transceiver cable is disconnected
 - A cable cut occurring in a Hub wiring only affects one computer.

Advantages and Disadvantages of Wiring Schemes

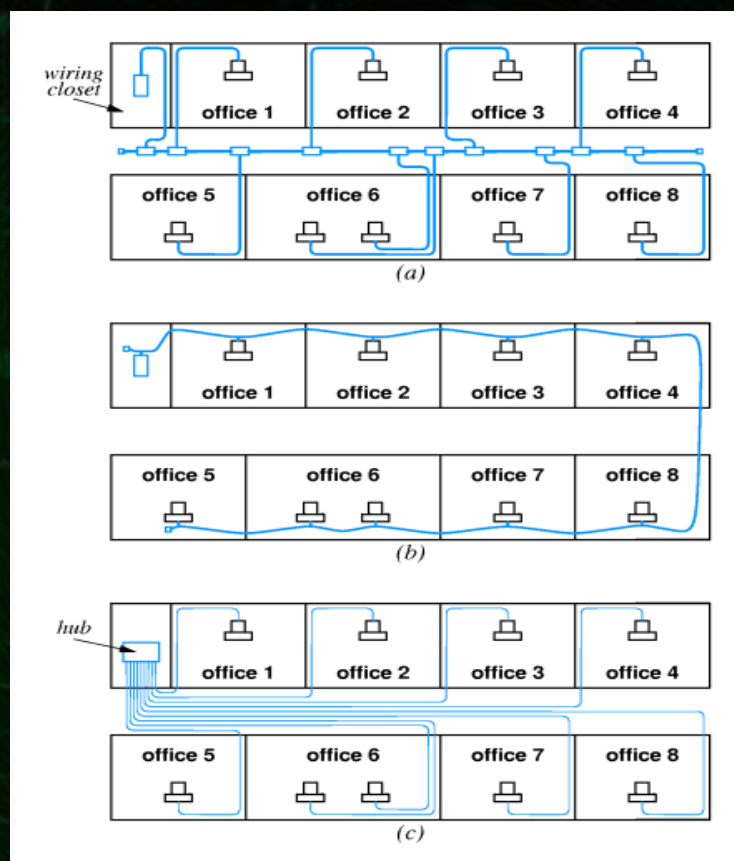
– Cost issues:

- Twisted pair Ethernet is the cheapest wiring that makes it so popular.
- Thicknet is the most costly wiring which is no longer used

♦ Example

- Eight offices wired with a) Thick Ethernet, b) Thin Ethernet, c) Twisted Pair Ethernet

Comparison of Wiring Schemes



The Topology Paradox

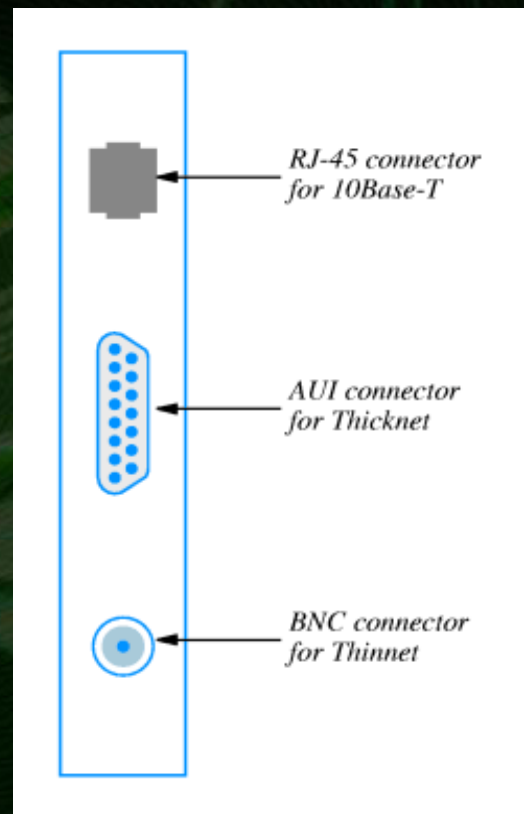
- ◆ Question: Is Ethernet a bus topology, or does the topology depend on the wiring?
- ◆ Answer: Both. Twisted pair Ethernet forms a classic star topology, however functions like a bus
- ◆ 10BaseT Ethernet is often called a star-shaped bus

The Topology Paradox

- ◆ Two different types of topologies:
 - Logical Topology: defined by the specific network technology
 - Physical Topology: depends on the wiring scheme

Network Interface Cards and Wiring Schemes

- ◆ To allow changing the wiring without changing the interface hardware, NICs support multiple wiring schemes



Network Interface Cards and Wiring Schemes



10/100 Network Interfaces and Autonegotiation

- ◆ 10 Base-T version of Twisted pair Ethernet operated at 10 Mbps
- ◆ 100 Base-T Twisted pair Ethernet operates at 100 Mbps
- ◆ 100 Base-T technology is backward compatible and allows the participants to negotiate a speed when connection is established
- ◆ Process is known as Autonegotiation

10/100 Ethernet NIC



Categories of Wires

- ◆ Cable used for wiring should match:
 - The intended data rate
 - The distance between the devices
 - The amount of electromagnetic noise
 - Anticipated future needs
 - COST

Categories of Wires

Category	Bandwidth	Typical Uses
3	16 MHz	older, low-speed networks; analog telephones
4	20 MHz	short distance 10Base-T
5	100 MHz	10Base-T Ethernet; some 100Base-T
5E	100 MHz	100Base-T (Fast Ethernet); some 1000Base-T
6	250 MHz	1000Base-T Gigabit Ethernet) or ATM
7	600 MHz	future (possibly 10 Gigabit Ethernet)

Summary

- ♦ Wiring Schemes
 - 10 Base-T
- ♦ Advantages and Disadvantages of Wiring Schemes
- ♦ The Topology Paradox
- ♦ NICs and Wiring Scheme
- ♦ Categories of Wires

COMPUTER NETWORKS

CS610

Lecture-13

Hammad Khalid Khan

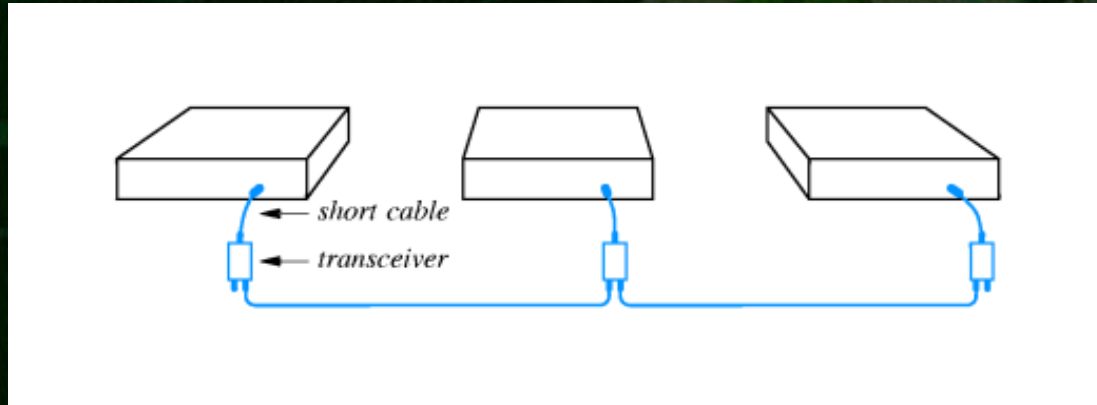
Review Lecture 12

- ◆ Wiring Schemes
 - 10 Base-T
- ◆ Advantages and Disadvantages of Wiring Schemes
- ◆ The Topology Paradox
- ◆ NICs and Wiring Scheme
- ◆ Categories of Wires

Wiring Schemes and Other Network Technologies

- ◆ Multiple wiring schemes are not limited to Ethernet technology. Almost all other network technologies use different wiring schemes
- ◆ Localtalk uses Hubs (Physical Star) to simulate a bus topology
- ◆ IBMs Token Ring also uses Hubs (Physically a Star Topology) to simulate a logical ring network

Wiring Schemes and Other Network Technologies



Chapter No 11

Extending LANs: Fiber Modems, Repeaters, Bridges, and Switches

Introduction

- ♦ LAN technologies are designed to operate within the same building
- ♦ However most companies or institutions have offices located far apart from each other

Distance Limitation And LAN Design

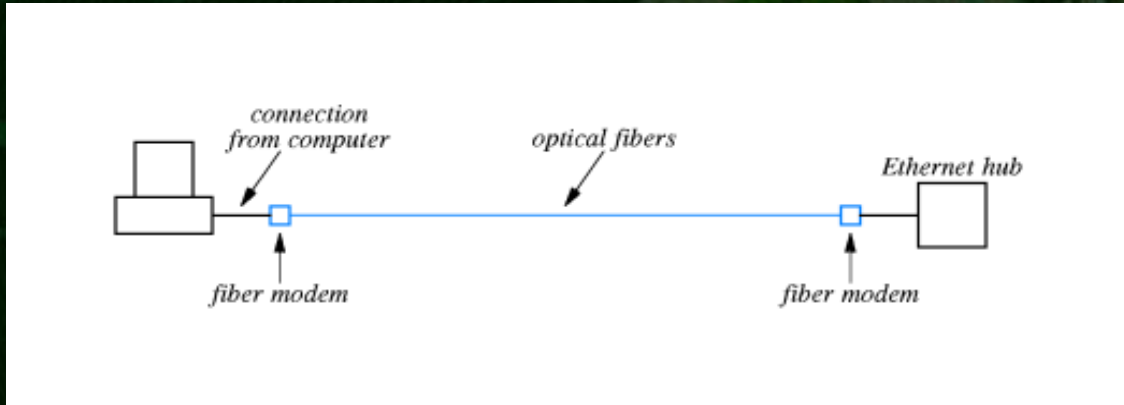
- ♦ The maximum cable length of a LAN is fixed, because:
 - The electrical signal level gets weaker as it travels
 - The delays must be short to allow access mechanisms (CSMA/CD, token passing), work properly

Distance Limitation And LAN Design

LAN Extensions

- ◆ Several techniques extend diameter of LAN medium
- ◆
- ◆ Most techniques use additional hardware
- ◆ LAN signals relayed between LAN segments
- ◆
- ◆ Resulting mixed technology stays within original engineering constraints while spanning greater distance

Fiber Optic Extensions



Fiber Optic Extensions

- ♦ The Fiber Modems:
 - Convert digital data into pulses of light
 - Transmit over the optical fiber
 - Receive light and convert into digital data
- ♦ Because
 - Delays on optical fiber is low and
 - Bandwidth is high
 - This mechanism will successfully extend the LAN across several kilometers

Fiber Optic Extensions



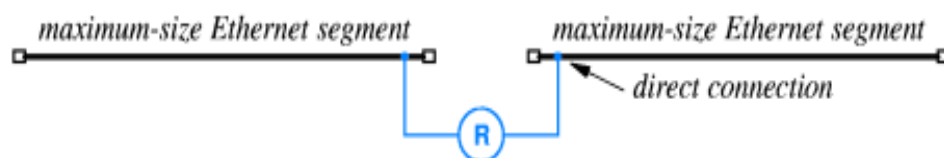
Fiber Optic Extensions



Repeaters

- ◆ Fact: Electrical signals gets weaker while travelling over copper
- ◆ A repeater (a hardware device)
 - Amplify the weakening signals received from one segment
 - And retransmit them on to another segment

Repeaters



Repeaters

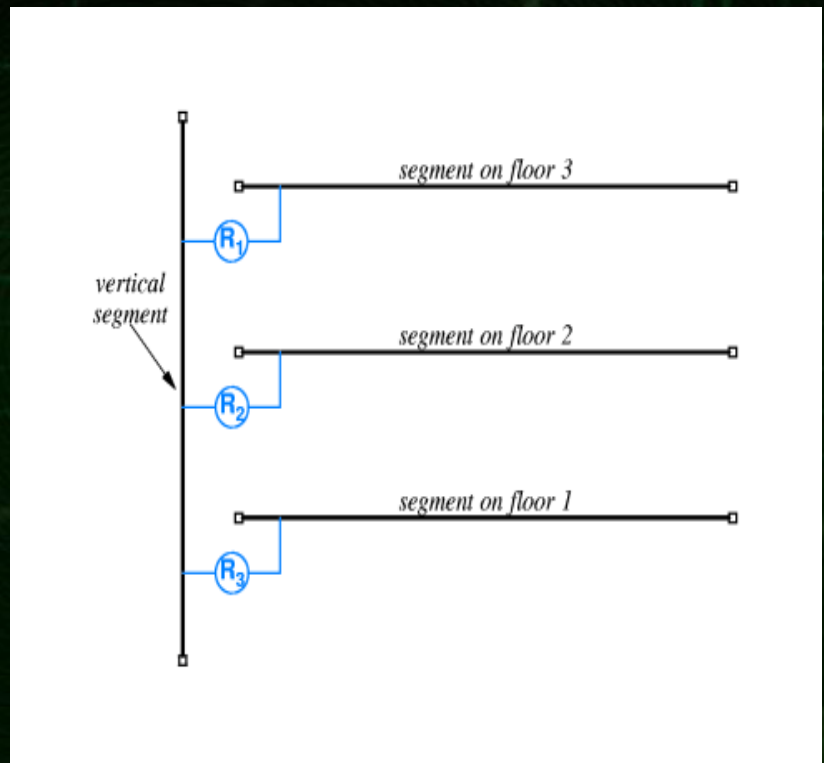
- ◆ One repeater doubles, two repeaters triples the maximum cable length limitation
- ◆ Computers attached to different segments communicate as if they are connected to the same cable

Repeaters

- ◆ Question: Can we increase the maximum cable length as many times as we wish by just adding repeaters?
- ◆ Answer: No
 - Every repeater introduces a delay
 - Access mechanisms such as CSMA/CD does not work with long delays
 - Ethernet standard specifies that any two stations cannot be separated by more than four repeaters

Repeaters

- ◆ Using a vertical segment:
 - Only two repeaters separate any two stations in this scheme



Repeaters

- ◆ Disadvantages:
 - Repeaters do not recognize frame formats, they just amplify and retransmit the electrical signals.
 - If a collision or error occurs in one segment,
 - Repeaters amplify and retransmits also the error onto the other segments

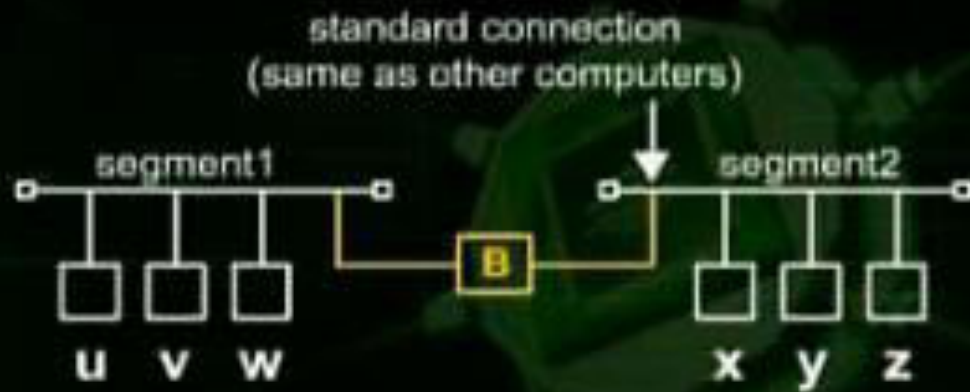
An Ethernet Repeater (Front)



An Ethernet Repeater (Back)



Bridges



Bridges

- ◆ A Bridge is a hardware device also used to connect two LAN segments to extend a LAN
- ◆ Unlike a repeater, a bridge:
 - Uses two NICs, to connect two segments
 - Listens to the all traffic
 - Recognizes frame format
 - Forwards only correct, complete frames
 - Discards the collided and errored frames

An Ethernet Bridge



Frame Filtering

- ◆ A typical bridge has two NICs, a CPU, a memory and a ROM
- ◆ It only runs the code stored in its ROM
- ◆ The most important task a bridge performs is frame filtering

Frame Filtering

- ◆ If both the source and destination are on the same segment, it does not forward the frame to the other segment
- ◆ A frame is forwarded to the other segment, if the frame is destined to the that segment
- ◆ Broadcast and multicast frames are also forwarded

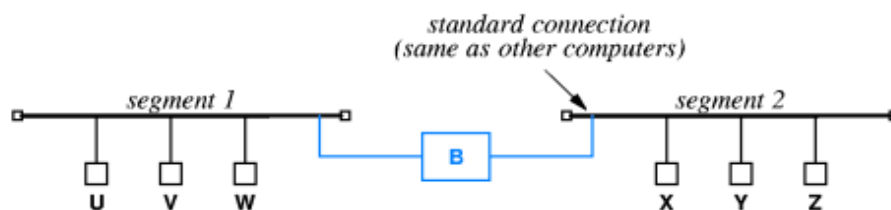
Frame Filtering

- ◆ Question: How does a bridge know on which segment a destination computer is attached?
- ◆ Answer: It keeps a list for each segment that consists of physical addresses of the computers attached to that segment

Frame Filtering

- ◆ Question: How does a bridge build up address lists?
- ◆ Answer: Most bridges are self learning bridges
 - As soon as a frame arrives to a bridge
 - It extracts the source address from its header and
 - Automatically adds it in the list for that segment

Frame Filtering



Event	Segment 1 List	Segment 2 List
Bridge boots	—	—
U sends to V	U	—
V sends to U	U, V	—
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

Summary

- ◆ Distance Limitation on LANs
- ◆ Fiber Optic Extensions
- ◆ Repeaters
- ◆ Bridges

COMPUTER NETWORKS

CS610

Lecture-14

Hammad Khalid Khan

Review Lecture 13

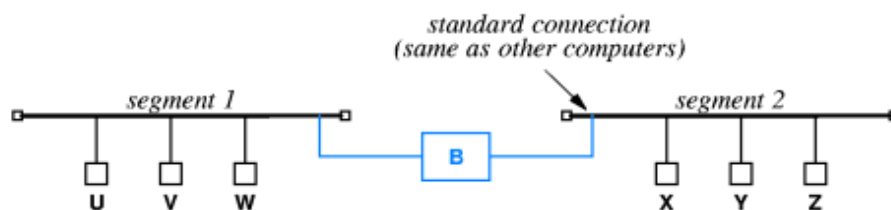
- ◆ Distance Limitation on LANs
- ◆ Fiber Optic Extensions
- ◆ Repeaters
- ◆ Bridges

Bridges

Frame Filtering

- ◆ Question: How does a bridge build up address lists?
- ◆ Answer: Most bridges are self learning bridges
 - As soon as a frame arrives to a bridge
 - It extracts the source address from its header and
 - Automatically adds it in the list for that segment

Frame Filtering



Event	Segment 1 List	Segment 2 List
Bridge boots	—	—
U sends to V	U	—
V sends to U	U, V	—
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

Startup And Steady State

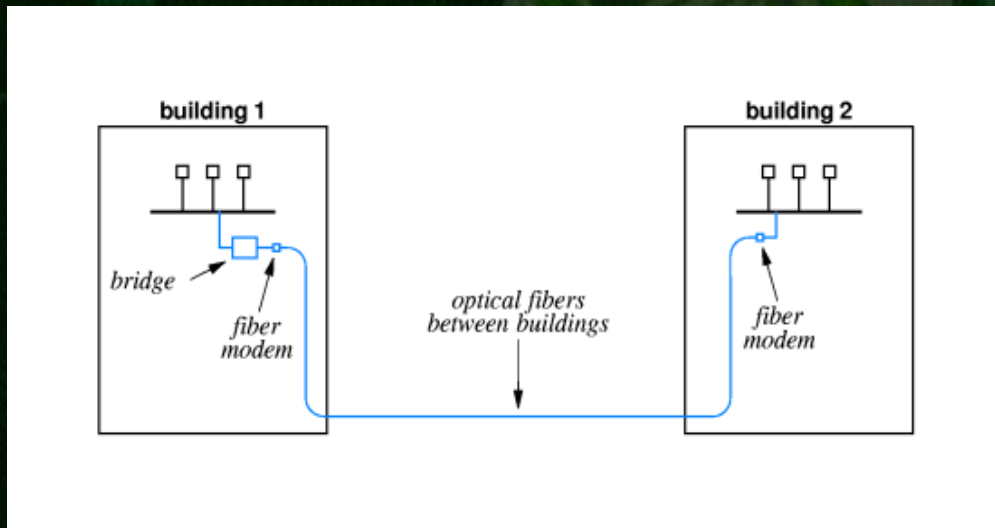
- ◆ When a bridge first boots, the address lists are empty (in startup state)
 - The bridge forwards frames to the other segment if it can not find its destination address in its lists
- ◆ After sometime, when the bridge has received at least one frame from every computer, it has the lists built (steady state), and
 - It forwards frames as far as it is necessary

Planning a Bridged Network

- ◆ In a steady state, a bridge allows simultaneous use of each segment
- ◆ When designing a LAN, bridges can be installed to divide the LAN into segments to improve performance
- ◆
- ◆ For example: Frequently contacting computers can be attached to the same segment
- ◆
- ◆ The frame traffic on one segment does not affect the other segment

Bridging Between Buildings

- ◆ If two buildings are located far from each other, a bridge, a pair of fiber modems and an optical fiber can be used to connect two LANs



Bridging Between Buildings

- ◆ Advantages:
 - Cost: An optical fiber and fiber modems are sufficient to connect many computers located on separate buildings
 - Maintenance: No need to change the wiring between the buildings when installing and removing a computer
 - Performance: The traffic on each building does not affect the other

Bridging Across Longer Distances

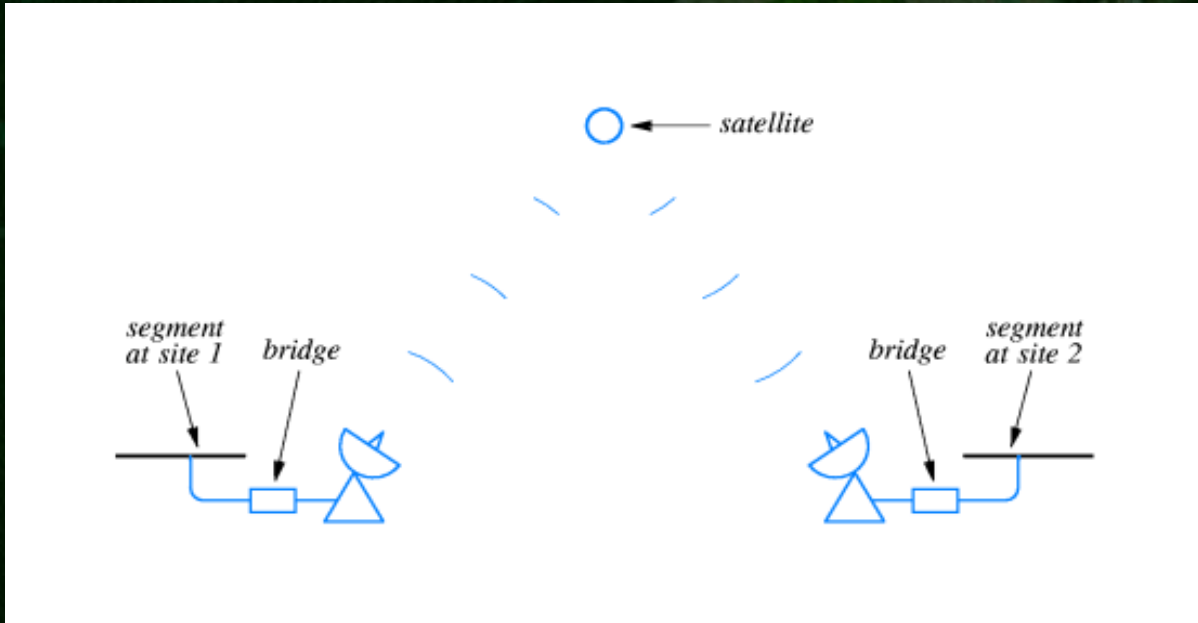
- ◆ Question: Is it always possible to connect two sites with optical fiber?
- ◆ Answer: No
 - The distance may be too long
 - It is usually not allowed to lay an optical fiber if the land does not belong to you

Bridging Across Longer Distances

- ◆ There are two common methods to connect two distant sites:
 - Leased serial line connection
 - Less expensive
 - Leased satellite channel
 - Can span arbitrarily long distance

Bridging Across Longer Distances

- ◆ Leased Satellite Connection:

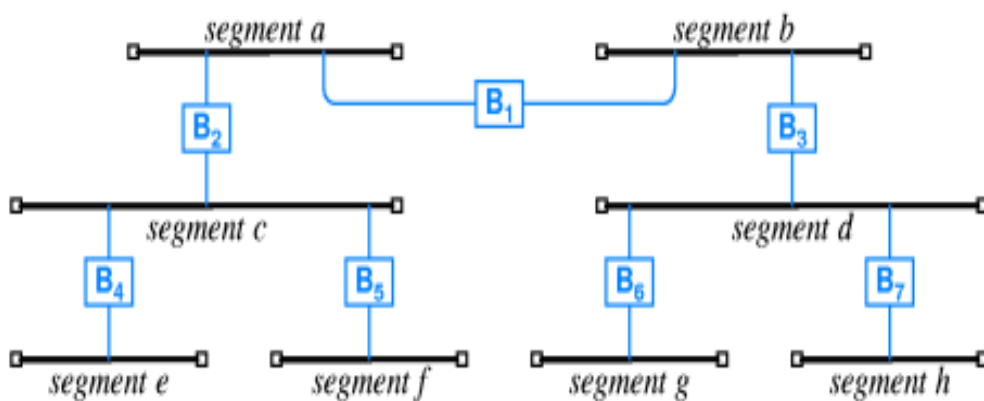


- ◆ Unlike optical fibers, satellite connections are low-bandwidth to save cost
- ◆ Because the frames arrive from local network much faster than they can be sent across a satellite link,
 - The bridge must use buffering(saving a copy of frame into memory until it can be sent)
 - The bridge may run out of memory
 - The communication software usually waits for a response after sending a few frames

A Cycle of Bridges

- ◆ A bridged network can connect many segments
- ◆ One bridge is needed to connect each segment to the rest of the bridged network

A Cycle of Bridges

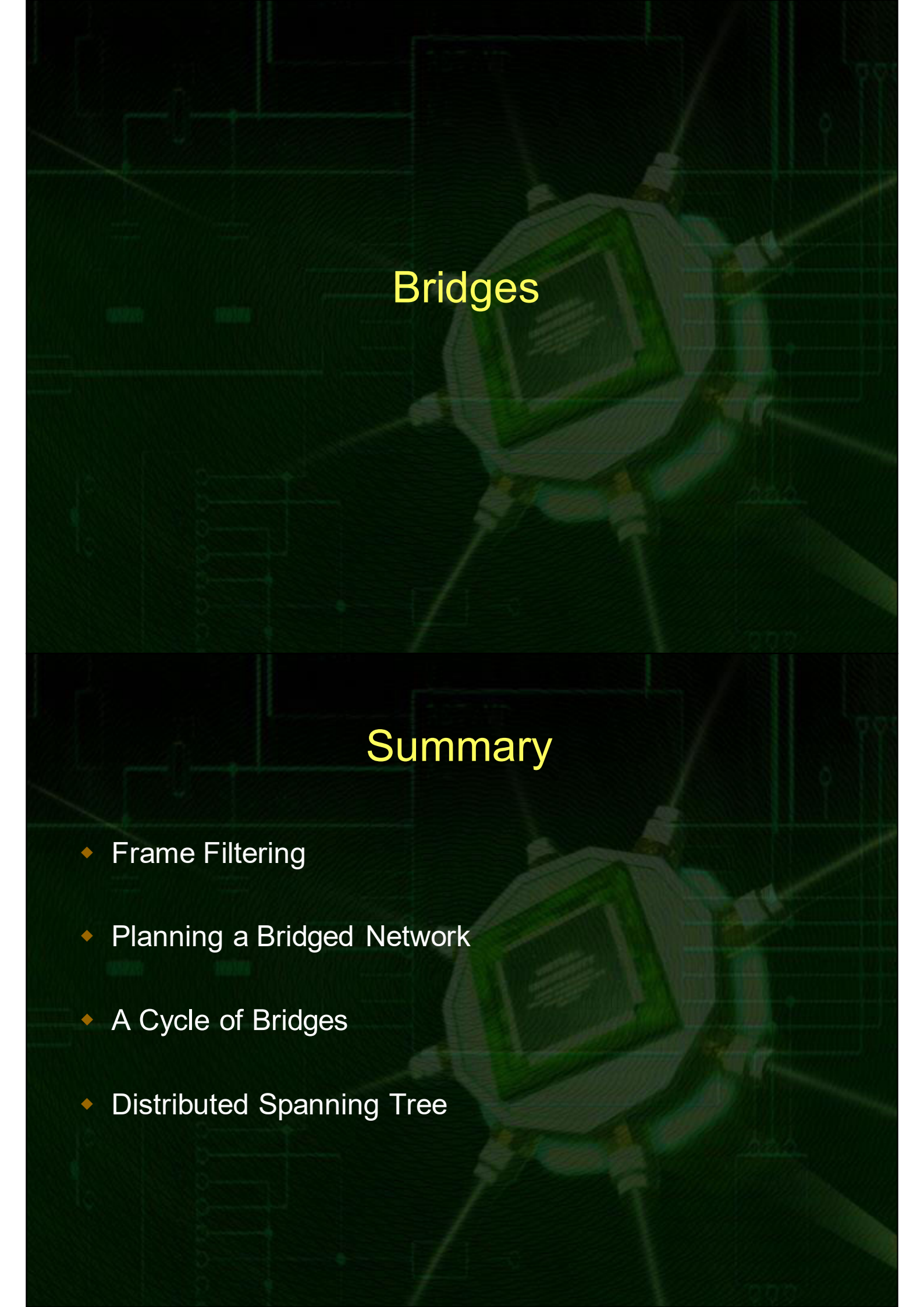


A Cycle of Bridges

- ◆ If the bridges on a large network form a cycle, then broadcasting frames introduce a problem
- ◆ Copies of a broadcast frame continuously flows around the cycle, each computer receiving an infinite number of copies

A Cycle of Bridges





Bridges

Summary

- ◆ Frame Filtering
- ◆ Planning a Bridged Network
- ◆ A Cycle of Bridges
- ◆ Distributed Spanning Tree

COMPUTER NETWORKS

CS610

Lecture-15

Hammad Khalid Khan

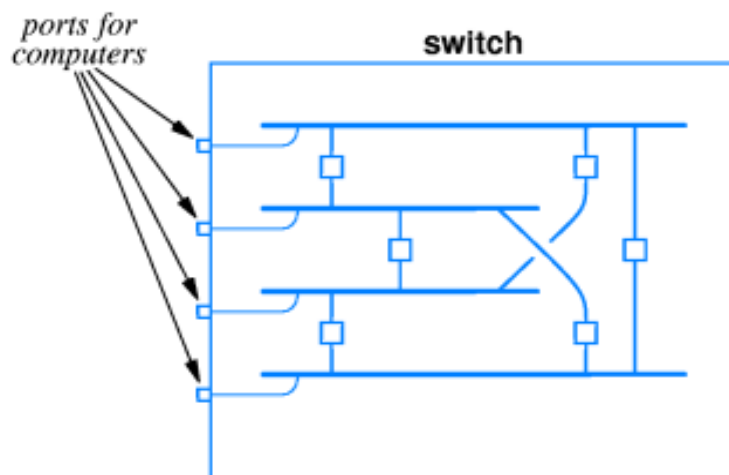
Review Lecture 14

- ◆ Start up and Stand by Modes of a Bridge
- ◆ Planning a Bridge
- ◆ Bridging between Buildings
- ◆ Bridging over Long Distance
- ◆ Cycle of Bridges and DST

Switching

- ♦ A switched LAN consists of a single electronic device that transfers frames among the connected computers
- ♦ A hub with multiple ports simulates a single shared medium
- ♦ However a switch simulates a bridged LAN with one computer per segment

Switching



Switching

- ◆ If a hub is used to connect many computers on a LAN, then only two computers can communicate at a given time
- ◆ However if a switch is used, the communication between two computers will not affect the others, pairs of computers can communicate at the same time

Combining Switches and Hubs

- ◆ To reduce costs, computers can be connected and distributed to a number of hubs, then the hubs can be connected to a switch
 - ◆ Hubs simulate single shared LAN segments
 - ◆ Switch simulates a bridged LAN connecting segments

Bridging And Switching With Other Technologies

- ◆ Hubs, bridges and switches are not limited to Ethernet logical bus topology
- ◆ They are available also for other networking technologies such as Token ring, FDDI etc.
 - ◆ FDDI hub
 - ◆ Token ring hub

Chapter 13

WAN Technologies and Routing

Introduction

- ♦ LANs can be extended using techniques in previous chapter
- ♦ Can not be extended arbitrarily far or to handle arbitrarily many computers
 - Distance limitations even with extensions
 - Broadcast a problem
- ♦ Need other technologies for larger networks

Characterization of Networks

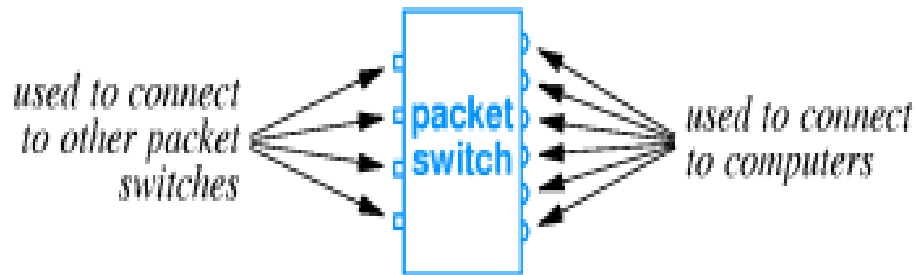
- ♦ Local Area Network (LAN)
 - Single building
- ♦ Metropolitan Area Network (MAN)
 - Single city
- ♦ Wide Area network (WAN)
 - Country
 - Continent

WAN Technology and Routing

Packet Switches

- ◆ To span long distances or many computers, network must replace shared medium with packet switches
- ◆
 - Each switch moves an entire packet from one connection to another
 - A small computer with network interfaces, memory and program dedicated to packet switching function

Packet Switches



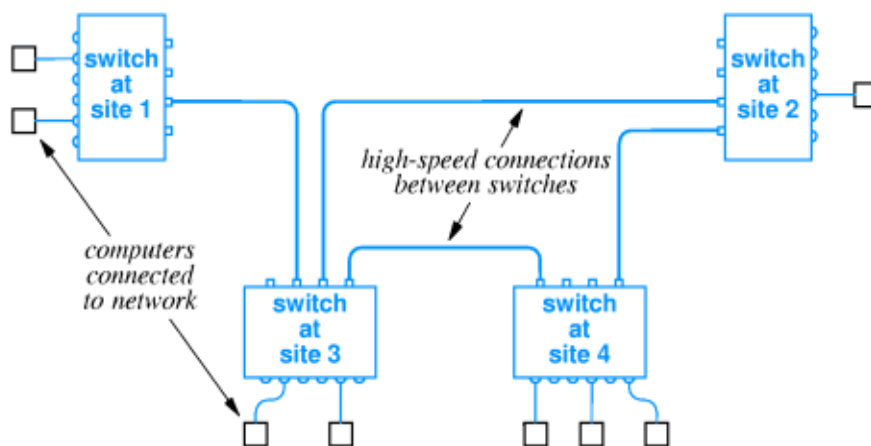
Connections to Packet Switches

- ◆ Packets switches may connect to computers and to other packet switches
- ◆ Typically high speed connections to other packets switches, lower speed to computers
- ◆ Technology details depend on desired speed

Packet Switches as Building Blocks

- ◆ Packet switches can be linked together to form WANs
- ◆ WANs need not be symmetric or have regular connections
- ◆
- ◆ Each switch may connect to one or more other switches and one or more computers

Packet Switches as Building Blocks



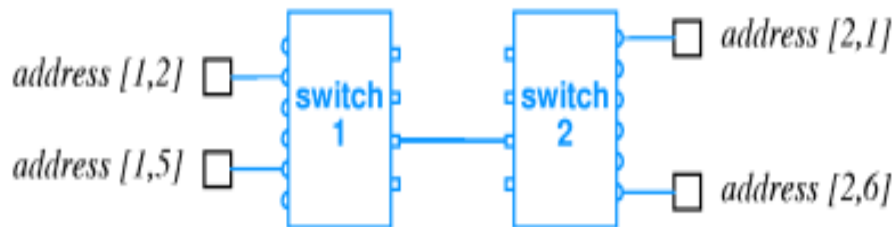
Store and Forward

- ◆ Data delivery from one computer to another is accomplished through store-and-forward technology
 - Packet switch stores incoming packet
 - ... and forwards the packet to another switch or computer
 -
- ◆ Packet switch has internal memory
 - Can hold packet if outgoing connection is busy
 - Packets for each connection held on queue

Physical Addressing in a WAN

- ◆ Similar to LAN
 - Data transmitted in packets (equivalent to frames)
 - Each packet has format with header
 - Packet header includes destination and source addresses
- ◆ Many WANs use hierarchical addressing for efficiency
 - One part of address identifies destination switch
 - Other part of address identifies port on switch

Physical Addressing in a WAN



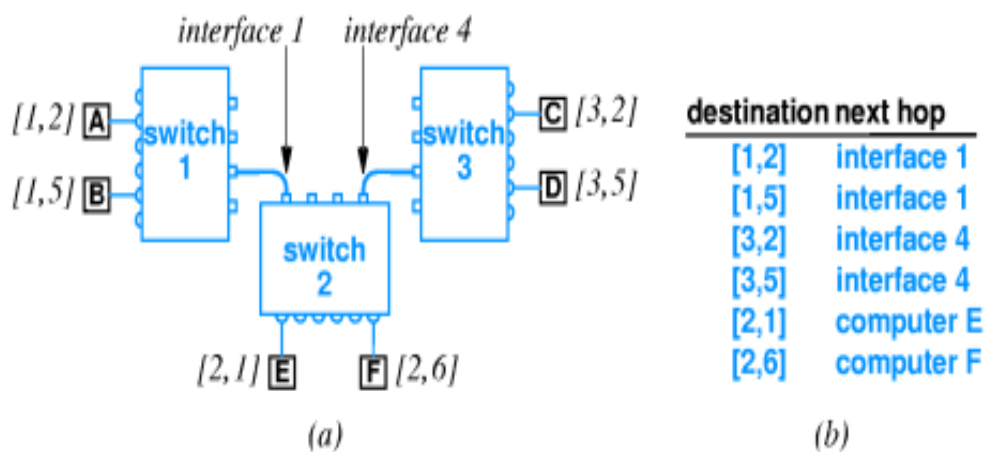
Next-Hop Forwarding

- ◆ Packet switch must choose outgoing connection for forwarding
- ◆
 - If destination is local computer, packet switch delivers computer port
 - If destination is attached another switch, this packet switch forwards to next hop through connection to another switch
- ◆ Choice based on destination address in packet

Choosing Next Hop

- ◆ Packet switch doesn't keep complete information about all possible destination
- ◆ Just keeps next hop
- ◆ So, for each packet, packet switch looks up destination in table and forwards through connection to next hop

Choosing Next Hop



Summary

- ♦ Wide Area Networks
- ♦ Packet Switches
- ♦ Physical Addressing in a WAN
- ♦ Store and Forward
- ♦ Next Hop Forwarding

COMPUTER NETWORKS

CS610

Lecture-16

Hammad Khalid Khan

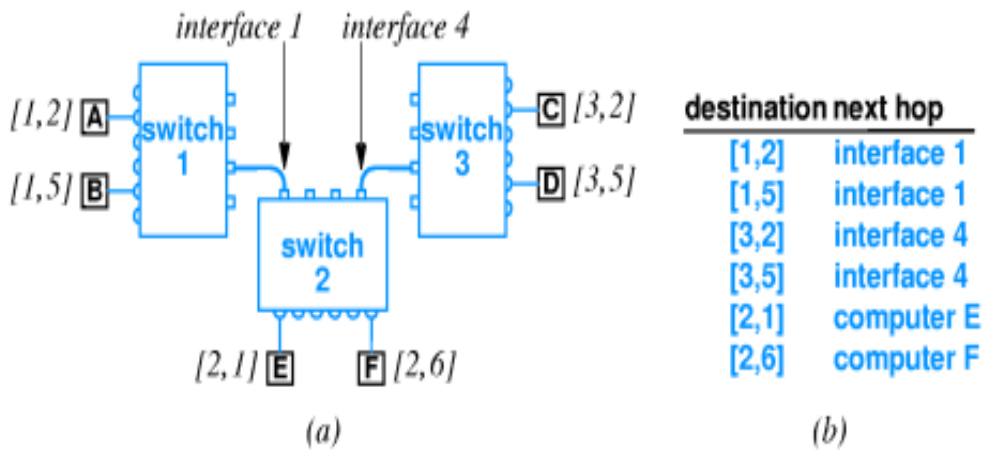
Review Lecture 15

- ♦ Wide Area Networks
- ♦ Packet Switches
- ♦ Physical Addressing in a WAN
- ♦ Store and Forward
- ♦ Next Hop Forwarding

Choosing Next Hop

- ♦ Packet switch doesn't keep complete information about all possible destination
- ♦ Just keeps next hop
- ♦ So, for each packet, packet switch looks up destination in table and forwards through connection to next hop

Choosing Next Hop



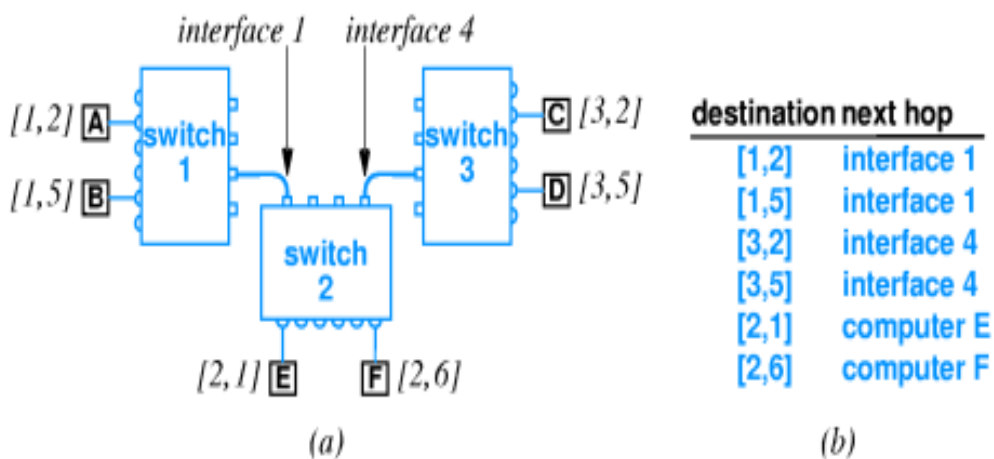
Source Independence

- ◆ Next hop to destination does not depend on source of packet, called Source Independence
- ◆ Allows fast, efficient routing
- ◆ Packet switch need not have complete information, just next hop
 - Reduces total information
 - Increases dynamic robustness - network can continue to function even if topology changes without notifying entire network

Hierarchical Addressing and Routing

The Process of forwarding the packets from one hop to the next is known as Routing

Hierarchical Addressing and Routing



Hierarchical Addressing and Routing

- ◆ In particular, all destinations on same switch have same next hop
- ◆ Thus, routing table can be collapsed:

Destination	Next Hop
(1, anything)	Interface 1
(3, anything)	Interface 4
(2, anything)	local computer

Routing in a WAN

- ◆ More computers == more traffic
- ◆ Can add capacity to WAN by adding more links and packet switches
- ◆ Packet switches need not have computers attached
- ◆ Interior switch - No attached computers
- ◆ Exterior switch - Attached computers

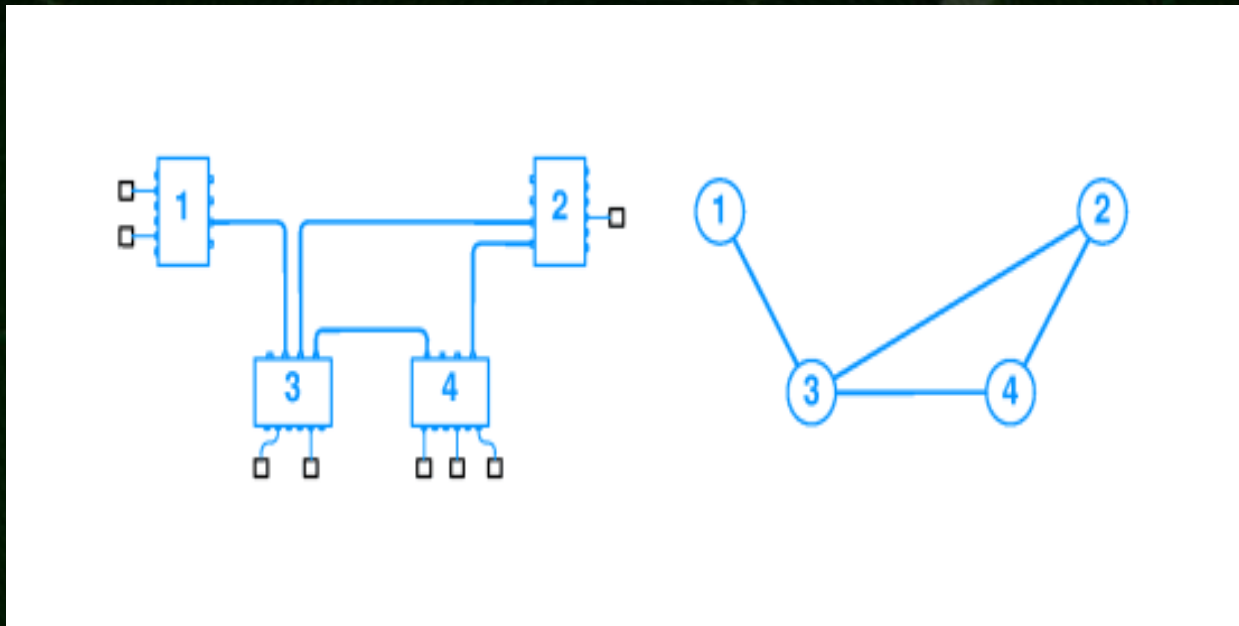
Routing in a WAN

- ◆ Both Interior and Exterior switches:
 - Forward Packets
 - Need Routing Tables
- ◆ Must have:
 - Universal Routing - Next hop for each possible destination
 - Optimal Routes - Next hop in table must be on shortest path to destination

Modeling a WAN

- ◆ Use a graph:
 - Nodes model switches
 - Edges model direct connections between switches
- ◆ Captures essence of network, ignoring attached computers

Modeling a WAN



Route Computation with a Graph

- Can represent routing table with edges:

destin- ation	next hop	destin- ation	next hop	destin- ation	next hop	destin- ation	next hop
1	-	1	(2,3)	1	(3,1)	1	(4,3)
2	(1,3)	2	-	2	(3,2)	2	(4,2)
3	(1,3)	3	(2,3)	3	-	3	(4,3)
4	(1,3)	4	(2,4)	4	(3,4)	4	-
<i>node 1</i>		<i>node 2</i>		<i>node 3</i>		<i>node 4</i>	

- Graph algorithms can be applied to find routes

Redundant Routing Information

- ◆ Notice duplication of information in routing table for node 1:

destin- ation	next hop	destin- ation	next hop	destin- ation	next hop	destin- ation	next hop
1	-	1	(2,3)	1	(3,1)	1	(4,3)
2	(1,3)	2	-	2	(3,2)	2	(4,2)
3	(1,3)	3	(2,3)	3	-	3	(4,3)
4	(1,3)	4	(2,4)	4	(3,4)	4	-
<i>node 1</i>		<i>node 2</i>		<i>node 3</i>		<i>node 4</i>	

- ◆ Switch 1 has only one outgoing connection; all traffic must traverse that connection

Default Routes

- ◆ Can collapse routing table entries with a Default Route
- ◆ If destination does not have an explicit routing table entry, use the default route:

Default Routes

destin- ation	next hop	destin- ation	next hop	destin- ation	next hop	destin- ation	next hop
1	-	2	-	1	(3,1)	2	(4,2)
*	(1,3)	4	(2,4)	2	(3,2)	4	-
		*	(2,3)	3	-	*	(4,3)
				4	(3,4)		
<i>node 1</i>		<i>node 2</i>		<i>node 3</i>		<i>node 4</i>	

Summary

- ◆ Source Independence
- ◆ Hierarchical Addressing and Routing
- ◆ Routing in a WAN
- ◆ Default Routes

COMPUTER NETWORKS

CS610

Lecture-17

Hammad Khalid Khan

Review Lecture 16

- ◆ Source Independence
- ◆ Hierarchical Addressing and Routing
- ◆ Routing in a WAN
- ◆ Modeling a WAN
- ◆ Route Computation and Default Routes

Building Routing Tables

- ♦ How to enter information into routing tables:
 - Manual entry
 - Software
- ♦ How to compute routing table information:
 - Static routing - At boot time
 - Dynamic routing - Allow automatic updates by a program

Building Routing Tables

- ♦ Static Routing
 - Simple
 - Low Network Overhead
 - Inflexible
- ♦ Dynamic Routing
 - Can work around network failures automatically

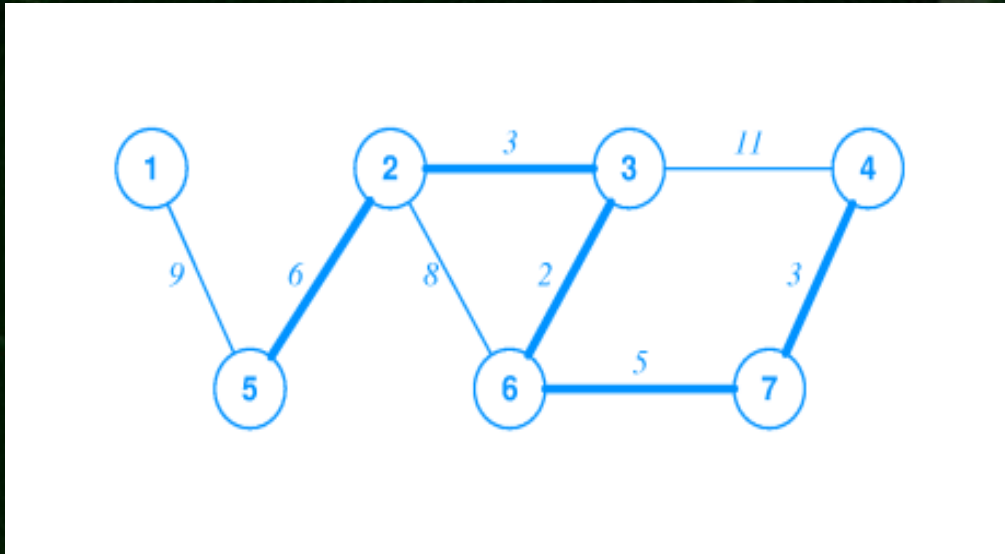
Computing Shortest Path in a Graph

- ◆ Assume graph representation of network at each node
- ◆ Use Dijkstra's algorithm to compute shortest path from each node to every other node
- ◆ Extract next-hop information from resulting path information
- ◆ Insert next-hop information into routing tables

Weighted Graph

- ◆ Dijkstra's algorithm can accommodate weights on edges in graph
- ◆ Shortest path is then the path with lowest total weight (sum of weights of all edges)
- ◆ Shortest path not necessarily fewest edges (or hops)

Weighted Graph



Distance Metrics

- ◆ Weights on graph edges reflect "cost" of traversing edge
 - Time
 - Dollars
 - Hop count (weight == 1)
- ◆ Resulting shortest path may not have fewest hops

Distributed Route Computation

- ◆ Each packet switch computes its routing table locally and sends messages to the neighbors
- ◆ Updates information periodically
- ◆ Network adapts if a link or a packet switch fails
- ◆ Packet switches modifies tables to avoid failed hardware

Distance Vector Routing

- ◆ Local information is next-hop routing table and distance from each switch
- ◆ Switches periodically broadcast topology information i.e. (*destination, distance*)
- ◆ Other switches update routing table based on received information

Vector-Distance Algorithm

- ◆ In more detail:

Wait for next update message

Iterate through entries in message

If entry has shorter path to destination:

- Insert source as next hop to destination

- Record distance as distance from next hop to destination

- PLUS distance from this switch to next hop

Link-State Routing (SPF)

Comparison

- ◆ Distance Vector Routing
 - Very simple to implement
 - Packet Switch updates its own routing table first
 - Used in RIP
- ◆ Link-State Algorithm
 - Much more complex
 - Switches perform independent computations
 - Used in OSPF

Examples-WAN Technology

- ◆ ARPANET
 - Began in 1960s
 - Funded by Advanced Research Projects Agency, an organization of the US Defense Department
 - Incubator for many of current ideas, algorithms and internet technologies

Examples-WAN Technology

- ◆ X.25
 - Early standard for connection-oriented networking
 - From ITU, which was originally CCITT
 - Predates computer connections, used for terminal/timesharing connection

Examples-WAN Technology

- ◆ Frame Relay
 - Telco service for delivering blocks of data
 - Connection-based service; must contract with telco for circuit between two endpoints
 - Typically 56Kbps or 1.5Mbps; can run to 100Mbps

Examples-WAN Technology

- ♦ SMDS - Switched Multi-megabit Data Service
 - Also a Telco service
 - Connectionless service; any SMDS station can send a frame to any other station on the same SMDS "cloud"
 - Typically 1.5-100Mbps

Examples-WAN Technology

- ♦ ATM - Asynchronous Transfer Mode
 - Designed as single technology for voice, video, data, ...
 - Low jitter (variance in delivery time) and high capacity
 - Uses fixed size, small cells - 48 octets data, 5 octets header
 - Can connect multiple ATM switches into a network

Chapter 14

Connection Oriented Networking & ATM

Summary (CH. 13)

- ◆ Packet Switch
- ◆ Next-Hope Forwarding
- ◆ Source Independence
- ◆ Hierarchical Addressing

Introduction

- ♦ LANs and WANs can both connect multiple computers, but they have different base technologies and meet different goals
- ♦ ATM is a single technology that is designed to meet the goals of both LANs and WANs
- ♦ ATM uses the concept of Connection-Oriented Networking

Summary

- ♦ Routing Table Computation
- ♦ Shortest Path Computation in a Graph
 - ♦ Dijkstra's Algorithm
- ♦ Distributed Route Computation
 - ♦ Distance Vector Routing
 - ♦ Link State Routing
- ♦ Example WAN Technologies

COMPUTER NETWORKS

CS610

Lecture-18

Hammad Khalid Khan

Review Lecture 17

- ♦ Routing Table Computation
- ♦ Shortest Path Computation in a Graph
 - Dijkstra's Algorithm
- ♦ Distributed Route Computation
 - Distance Vector Routing
 - Link State Routing
- ♦ Example WAN Technologies

Chapter 14

CONNECTION ORIENTED NETWORKING and ATM

Introduction

- ♦ LANs and WANs can both connect multiple computers, but they have different base technologies and meet different goals
- ♦ ATM is a single technology that is designed to meet the goals of both LANs and WANs
- ♦ ATM uses the concept of Connection-Oriented Networking

Asynchronous Transfer Mode

- ◆ Telephone companies (Telcos) introduced ATM to meet several goals:
 - Universal service – for all subscribers
 - Support for all uses – voice, video, and data
 - A single, unified infrastructure (no separate LANs & WANs)
 - Guaranteed service, when appropriate
 - Support for low-cost devices

Jitter

- ◆ Jitter is the term used for variance in transmission delays
- ◆ Jitter is significant for voice, video, and data
- ◆ Jitter in LANs can occur when a packet is delayed because the network is busy

Packet Sizes

- ◆ Large packets result in less overhead because a smaller fraction of the packet is used for header information
- ◆ Optimum networks use 4KB packets or larger
- ◆ Large packets can't easily be used for voice
 - 8 bit samples (at 125 usec per sample) would require half a second to fill a 4KB packet.
 - Echo cancellation can only be used with low transmission delays

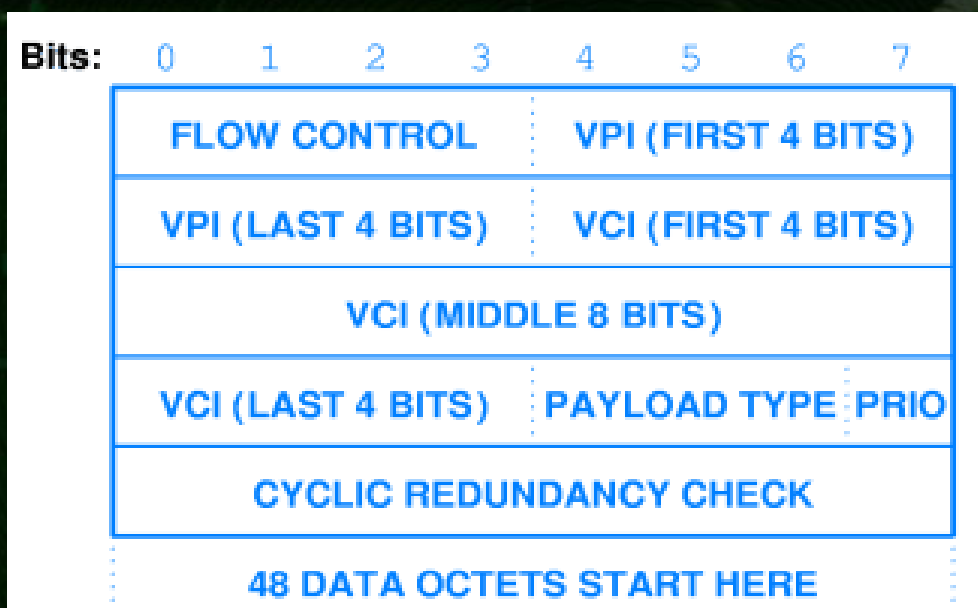
ATM Cells

- ◆ To meet its goals, ATM uses small, fixed-sized packets called cells
- ◆ Each cell has 53 octets
- ◆ VCI/VPI fields identify the cell's destination
- ◆ PRIO tell if cell can be discarded

ATM Cells

- ♦ CRC checks the header's bits only!
- ♦ ATM header is about 10 percent of the cell
- ♦ Ethernet can have overhead of only 1 %
- ♦ Engineers sometime call ATM overhead the Cell Tax

ATM Cells



Connection-Oriented Service

- ◆ The connection-oriented service paradigm for networking is similar to the manner in which telephones are used:
 - A caller dials the number of the destination
 - The telephone at the destination signals the arrival of a Connection Request
 - If the called person doesn't answer, the caller gives up after waiting for a Timeout
 - If the called person does answer, then the connection is established, and data is exchanged

Connection-Oriented Service

- ◆ In data communications, a binary connection identifier is given to each of the two parties to the connection to enable identification of the connection

Virtual Channels (or Circuits)

- ◆ Connections in ATM are called virtual channels (VC), or virtual circuits (a term preferred by some)
- ◆ These are called virtual, since connections are formed in ATM by storing values in memory locations (tables) in ATM switches, as opposed to making actual electrical connections

Virtual Channels (or Circuits)

- ◆ The VC is identified by a 24-bit value formed from:
 - The VPI, or virtual path indicator (8 bits), which identifies a particular path through the network; &
 - The VCI, or virtual channel indicator (16 bits), which identifies the channel in the virtual path is being used by the connection
- ◆ Most frequently, the 24-bit pair is treated as just a single connection identifier by computers

Summary

- ◆ Connection-Oriented Networking and ATM
- ◆ Asynchronous Transfer Mode
- ◆ ATM Design and Cells
- ◆ Connection-Oriented Services
- ◆ Virtual Channels

COMPUTER NETWORKS

CS610

Lecture-19

Hammad Khalid Khan

Review Lecture 18

- ◆ A single Global Technology
- ◆ ATM Design and Cells
- ◆ Connection Oriented Service
- ◆ VPI/VCI

Labels and Label Switching

- ◆ An ATM network is built from interconnected ATM switches
- ◆ Attachment points on switches, or ports, can be connected to computers or other ATM switches

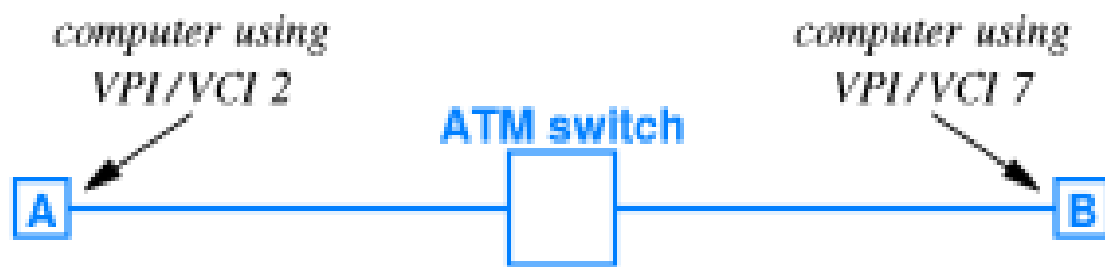
Labels and Label Switching

- ◆ As cells arrive at an ATM switch, their VPI/VCI is modified using a forwarding table which gives the new VPI/VCI for the next leg of the cell's trip
- ◆ The forwarding table is essentially indexed by the incoming cell's VPI/VCI, and the contents yield the new VPI/VCI

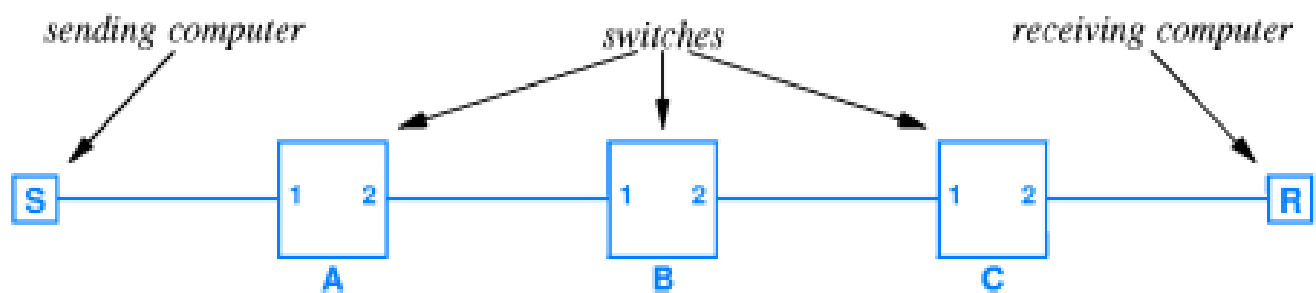
Label Rewriting

- ◆ The replacement of the incoming cell's VPI/VCI with a probably different VPI/VCI is called Rewriting
- ◆ ATM is thus called a Label Rewriting, or Label Switching system
- ◆ Thus two computers with a connection through an ATM network will likely have different VPI/VCI values for each end of the connection!

Label Switching



Example



old VPI/VCI	inter-face	new VPI/VCI
0		
1		
2		
3	2	4
4		
5		
6		

old VPI/VCI	inter-face	new VPI/VCI
0		
1		
2		
3		
4	2	1
5		
6		

old VPI/VCI	inter-face	new VPI/VCI
0		
1	2	6
2		
3		
4		
5		
6		

Example

- ◆ The sending computer, S, uses a VPI/VCI of 3 and sends a cell
- ◆ Switch A receives the cell and looks up 3, then rewrites the VPI/VCI as 4, and sends the cell out of its port 2
- ◆ Switch B receives the cell and looks up 4, then rewrites the VPI/VCI as 1, and sends the cell out of its port 2

Example

- ◆ Switch C receives the cell and looks up 1, then rewrites the VPI/VCI as 6, and sends the cell out of its port 2
- ◆ The receiving computer, R, receives the cell with a VPI/VCI of 6, which is the value it is using for the connection
- ◆ Forwarding tables in each switch must be coordinated to define meaningful “paths” through the network

Permanent Virtual Circuits

Permanent Virtual Circuits

- ◆ Provisioning requires two steps:
 - Determine a complete path (that is, identify the switches that will be used)
 - Choose appropriate VCI/VPI for each step in the path, and configure each adjacent pair of switches (easy, since each switch rewrites the VCI/VPI)

Switched Virtual Circuits

- ◆ Most networks offer dynamic connections which last for a relatively short time
- ◆ To handle this, ATM can dynamically establish a Switched Virtual Circuit (SVC), allow it last as long as necessary, and then terminate it
- ◆ The terminology comes from the telcos, where switching system normally refers to call switching

Establishing an SVC

- ◆ Computer sends a connection request to the switch to which it is attached
- ◆ Software in the switch finds a network path to the destination and sends along the connection request
- ◆ Each pair of switches in the path communicate to choose a VPI/VCI for their tables

Establishing an SVC

- ◆ Once the connection is accepted by the destination, a message is sent back to the originating computer to indicate the SVC is ready
- ◆ If any switch, or the destination computer, does not agree to setting up the VC, an error message is sent back and the SVC is not established

Signaling

- ◆ The term signaling is used to describe communication about the network, as opposed to communication that just uses the network
- ◆ A computer uses signaling, with reserved VCI/VPI values, to communicate with a switch to establish a connection or send other network control messages

Signaling

- ◆ These connection requests and network control messages are also sent in cells, and since the VPI/VCI used in these cells are reserved, there is no confusion between data and control cells

Quality of Service (QoS)

- ◆ Networks are more frequently being designed to allow specification of the quality of service required by users
- ◆ For example, a typical voice telephone call might give a QoS parameter for throughput of 64Kbps and delay less than 500 msec. A user sending video might require throughput of 2Mbps

Providing Desired QoS

- ◆ QoS desires are specified at connection setup time, and are never altered for the connection duration
- ◆ Switches along the path must reserve resources to guarantee the QoS
- ◆ If a switch cannot provide the resources, it rejects the connection request and an appropriate error message is returned

ATM QoS Specifications

- ◆ **Constant Bit Rate (CBR):** Used for uncompressed audio and video, since these have predefined maximum data rates
- ◆ **Variable Bit Rate (VBR):** Used for compressed audio and video, where the data rate depends on the level of compression that can be achieved

ATM QoS Specifications

- ◆ **Available Bit Rate (ABR)** is used for typical data applications (where the data rate may be unknown and bursty), and allows use of whatever bandwidth is available at a given time

Summary

- ◆ Label switching and Label Rewriting
- ◆ Permanent Virtual Circuits
- ◆ Switched Virtual Circuits
- ◆ Quality Of Service

COMPUTER NETWORKS

CS610

Lecture-20

Hammad Khalid Khan

Review Lecture 19

- ◆ Label Switching
- ◆ An Example ATM Network
- ◆ Permanent Virtual Circuits (PVC's)
- ◆ Switched Virtual Circuits (SVC's)
- ◆ Quality of Service (QoS)

Cells vs Packets

- ♦ ATM designers chose cells over packets because:
 - Cells aren't variable length, and memory management for them is simpler. Handling variable length packets leads to memory fragmentation
 - Variable length packets require hardware to accommodate the largest possible packet, and thus to detect the end of the packet. With cells, bits can just be counted as they arrive

Cells vs Packets

- The length of time required to send a variable length packet is variable, and requires complicated interrupt schemes to detect completion of transmission
- QoS can't be guaranteed with variable length packets as easily as it can with fixed length cells

ATM Speed

- ♦ ATM designers also chose cells to meet the need for speed, since it was designed to handle arbitrarily large numbers of users, each of which could be willing to pay for high throughput
- ♦ ATM is designed to work on fiber (but can be used with twisted pair). A typical port on an ATM switch operates at OC-3 speed (155 Mbps) or higher

ATM Critique

- ♦ ATM is far more expensive than typical LAN hardware
- ♦ Connection setup time may be excessive for short communications
- ♦ Cell tax consumes 10 % of network capacity
- ♦ QoS requirements might be unknown, leading to applications picking values that are too high or too low

ATM Critique

- ◆ Broadcast is inefficient, and has to be simulated by sending the same message to each computer separately
- ◆ ATM, as a single universal networking technology, has only minimal provision for interoperation with other technologies

Chapter 15

Network Characteristics: Ownership, Service Paradigm
and Performance

Network Ownership

- ◆ Private Network
 - Owned by single organization or company
- ◆ Public Network
 - Owned by common carrier e.g. Phone Company)

Private Network

- ◆ Often LAN Technology
- ◆ Multiple LANs in a building or campus linked together
- ◆ Sometimes called Intranet

Private Network Architecture

- ◆ Operates autonomously from other networks (e.g. Internet)
- ◆ Usually includes one or few closely managed external connections
- ◆ May restrict access at connections

Managing Private Networks

- ◆ Organization buys own equipment
- ◆ Hires staff to design, implement, maintain and upgrade network
- ◆ Responsible for all network management

Extending Private Networks

- ◆ Large organizations may have multiple buildings or campuses
- ◆ Can only install cables on own property
- ◆ May contract for leased lines from common carrier

Public Networks

- ◆ Operated by common carrier
- ◆ May be telephone company or other organization that builds network out of leased lines
- ◆ Multiple organizations subscribe and connect
- ◆ Data transits public network to other organizations

Advantages & Disadvantages

Private

♦ Advantages

- The owner has complete control over both the technical decision and policies

♦ Disadvantages

- Expensive to install and maintain

Public

♦ Advantages

- Flexibility

♦ Disadvantages

- No decision making power equipment or policies

Virtual Private Network

- ♦ VPN (Virtual Private Network) combines features of private and public networks
 - Limited to single organization
 - Uses public network for connectivity
- ♦ Connections, sometimes called Tunnels, connect sites
 - Each site sees tunnel as point-to-point link
 - No access for other users of public network

Service Paradigm

- ◆ Connection-Oriented
 - Similar to telephone system; endpoints establish and maintain a connection as long as they have data to exchange
- ◆ Connectionless
 - Similar to postal system; endpoint puts data to send into a packet and hands to network for delivery

Public and Private Networks

Summary

- ◆ Cells vs. Packets
- ◆ Label switching vs. Routing
- ◆ ATM Critique
- ◆ Network Characteristics (Chapter 15)
- ◆ Network Ownership
- ◆ Private and Public Networks

COMPUTER NETWORKS

CS610

Lecture-21

Hammad Khalid Khan

Review Lecture 20

- ◆ Cells vs Packets
- ◆ Label Switching vs Routing
- ◆ ATM Critique
- ◆ Network Ownership
 - Private vs Public Networks

Virtual Private Network

- ◆ VPN (Virtual Private Network) combines features of private and public networks.
 - Limited to single organization
 - Uses public network for connectivity
- ◆ Connections, sometimes called Tunnels, connect sites
 - Each site sees tunnel as point-to-point link
 - No access for other users of public network

Guaranteeing Absolute Privacy

- ◆ In addition to restricting packets, VPN systems use encryption to guarantee absolute privacy.
- ◆ Even if an outside does manage to obtain a copy of the packet, the outside will be unable to interpret the contents.

Service Paradigm

- ◆ At the lowest level, most networks transfer individual packets of data and the network requires each packet to follow an exact format dictates by the hardware.
- ◆ Other offer additional facilities the hide may of the details of the packets.
 - Interface Paradigms Or Service Paradigms

Service Paradigm

- ◆ Connection-Oriented
 - Similar to telephone system; endpoints establish and maintain a connection as long as they have data to exchange.
- ◆ Connectionless
 - Similar to postal system; endpoint puts data to send into a packet and hands to network for delivery.

Connection-Oriented Service

- ◆ One endpoint requests connection from network.
- ◆ Other endpoint agrees to connection.
- ◆ Computers exchange data through connection.
- ◆ One endpoint request network to break connection when transmission is complete.

Continuous and Bursty Traffic

- ◆ Networks handling voice or video are engineered to accept and deliver continuous data at fixed rate.
- ◆ Others are designed to handle burst traffic typical of computer networks.
- ◆ Connection does not disappear when no data is sent.

Simplex & Full Duplex Connections

- ◆ Some connection-oriented technologies provide full duplex while other allow on simplex connection.
 - To communicate using a simplex design a pair of computers must establish two connection; one from Computer A to Computer B and another from Computer B to A.

Connection Duration & Persistence

- ◆ Connections can be made on-demand or set up permanently.
 - Switched connection or switched virtual circuit.
 - Permanent connection or provisioned virtual circuit.
- ◆ Permanent connections
 - Originally hard-wired
 - Now configured at system unit time.

Connection Duration & Persistence

- ◆ Switched Connections
 - Computer maintains permanent connection to network
 - Network makes connection on demand
- ◆ Internal components are switches; network is a switched data network.

Service Guarantees

- ◆ Some connection-oriented networks provide guarantees about the service that computer will receive.
- ◆ They may guarantee a throughput rate or maximum packet loss rate.
- ◆ For example, ATM provides statistical guarantee about performance.

Stream or Message Interface

- ◆ Some connection-oriented networks provide stream interfaces
 - No boundaries are recorded; that receive may receive a single block of 60 characters even though the send sends three blocks of 20 characters.
- ◆ Others provide a message interface
 - Delivers data in the same size chunks that the sender transmitted.

Connectionless Service

- ◆ No connection necessary
- ◆ Source of data adds destination information to data and delivers to the network.
- ◆ Network delivers each data item individually.

Interior and Exterior Service Paradigms

- ◆ A network providing one service paradigm to the attached computers can use an entirely different service paradigm internally.
- ◆ For Example: ARPANET
 - Connection-Oriented Internally
 - Connection-less externally

Comparison

- ◆ Connection-Oriented
 - Accounting easier.
 - Application can learn of network problems immediately.
- ◆ Connectionless
 - Less overhead.
 - Easier to implement network.

Examples of Service Paradigms

Technology	Connection-Oriented	Connectionless	used for LAN	used for WAN
Ethernet		•	•	
Token Ring		•	•	
FDDI		•	•	
Frame Relay	•			•
SMDS		•		•
ATM	•		•	•
LocalTalk		•	•	

Addresses & Connection Identifiers

- ◆ Address is a complete, unique identifier.
- ◆ Connectionless delivery requires address on each packet.
- ◆ Connection-Oriented delivery can use a shorthand that identifies the connection rather than the destination.

Addresses & Connection Identifiers

- ◆ ATM - 160-bit address, 24-bit connection identifier
 - Connection identifier includes:
 - 8-bit virtual path identifier (VPI)
 - 16-bit virtual circuit identifier (VCI)
 - Connection identifier local to each computer.
 - May be different in different parts of the ATM switch.

Summary

- ◆ Virtual Private Networks
- ◆ Service Paradigm
- ◆ Connection-Oriented Service
- ◆ Connection-less Service

COMPUTER NETWORKS

CS610

Lecture-21

Hammad Khalid Khan

Review Lecture 21

- ♦ Virtual Private Networks (VPNs)
- ♦ Guaranteeing Absolute Privacy
- ♦ Service Paradigm
 - Connected-Oriented Service
 - Connectionless Service
- ♦ Address and Connection Identifiers

Network Performance Characteristics

Delay
Throughput

Delay

- ♦ Important quantitative property of networks.
- ♦ Delay is a measure of how long it takes for a bit of data to travel across the network from one computer to the other.
- ♦ Measured in seconds or fractions of seconds (milliseconds).
- ♦ Maximum and Average Delay.

Types of Delay

- ♦ Propagation delay - time to travel across medium.
- ♦ Switching delay - time for network component (hub, bridge, packet switch) to forward data.
- ♦ Access delay - time to get control of medium (CSMA/CD, token).
- ♦ Queuing delay - time enqueued in packet switches.

Throughput

- ◆ Throughput is a measure of the rate at which data can be sent through the network.
- ◆ The throughput capability of the underlying hardware is called bandwidth.

Throughput

- ◆ Because each frame contains headers the effective throughput is less than the hardware bandwidth.
- ◆ Networking professionals often use the term speed as a synonym for throughput.

Relationship between Delay and Throughput

- ◆ If a packet switch had a queue of packets waiting when a new packet arrives the new packet will be placed on the tail of the queue and will need to wait while the switch forwards the previous packets.

$$D = \frac{D_0}{(1-U)}$$

D = Effective Delay

D₀ = Delay when the network is idle

U = Value between 1 and 0 denoting the current utilization

Relationship between Delay and Throughput

- ◆ Throughput and delay are not completely independent.
- ◆ As traffic in a computer network increases, delays increase; a network that operates at close to 100% of its throughput capacity experiences severe delay.

Delay-Throughput Product

- ◆ Computed as delay time multiplied by effective throughput.
- ◆ Measures amount of data that can be present in the network.
- ◆ In fast networks with long delay times, sending computer can generate large amounts of data before destination receives first bit.

Jitter

- ◆ The amount of delay that a network introduces.
- ◆ A network with zero jitter takes exactly the same amount of time to transfer each packet.
- ◆ A network with high jitter takes much longer to deliver some packets than others.

Summary

- ◆ Delay
- ◆ Throughput
- ◆ Relationship between Delay and Throughput
- ◆ Delay-Throughput Product
- ◆ Jitter

COMPUTER NETWORKS

CS610

Lecture-22

Hammad Khalid Khan

Review Lecture 22

- ◆ Delay
- ◆ Throughput
- ◆ Relationship between Delay and Throughput
- ◆ Jitter

Chapter 17

Internetworking: Concepts, Architecture, and
Protocols

The Motivation For Internetworking

- ◆ No single networking technology is best for all needs.
- ◆ A large organization with diverse networking requirements needs multiple physical networks.
- ◆ If the organization chooses the type of network that is best for each task, the organization will need several types of networks.

The Motivation For Internetworking

- ◆ The interconnection of two or more networks, usually local area networks so that data can pass between hosts on the different networks as though they were one network.
- ◆ This requires some kind of Router or Gateway.

The Concept Of Universal Services

- ♦ The chief problem with multiple networks:
 - A computer attached to a given network can only communicate with other computers attached to the same network.
 - In the 1970s large organizations began to acquire multiple networks.
 - Each network in the organization formed an island.
 - Employees had to choose a computer appropriate for each task.
 - Multiple screens, keyboards, and computers.

The Concept Of Universal Services

- ♦ Universal Services
 - A communication system that supplies universal services allows arbitrary pairs of computers to communicate.
 - Universal service is desirable because it increases individual productivity.

The Concept of Universal Service

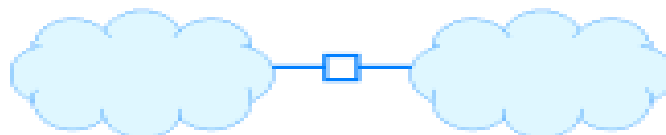
Internetworking

- ◆ Despite the incompatibilities among networks, researchers have devised a scheme that provides universal services among heterogeneous networks.
- ◆ Called INTERNETWORKING
 - Uses both hardware and software.

Physical Network Connection With Routers

- ♦ A router is a special-purpose system dedicated to the task of interconnecting networks.
- ♦ A router can interconnect networks that use different technologies, including different media, physical addressing schemes, or frame formats.

Physical Network Connection With Routers



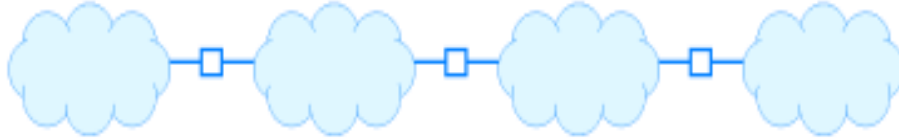
Internet Architecture

- ♦ Organization seldom use a single router to connect all its network for two reasons.
 - Because the router must forward each packet, the processor in a given router is insufficient to handle the traffic.
 - Redundancy improved internet reliability.

Internet Architecture

- ♦ An Internet consists of a set of networks interconnected by routers.
- ♦ The internet scheme allows each organization to choose the number and type of network, the number of routers to use to interconnect them, and the exact interconnection topology.

Internet Architecture



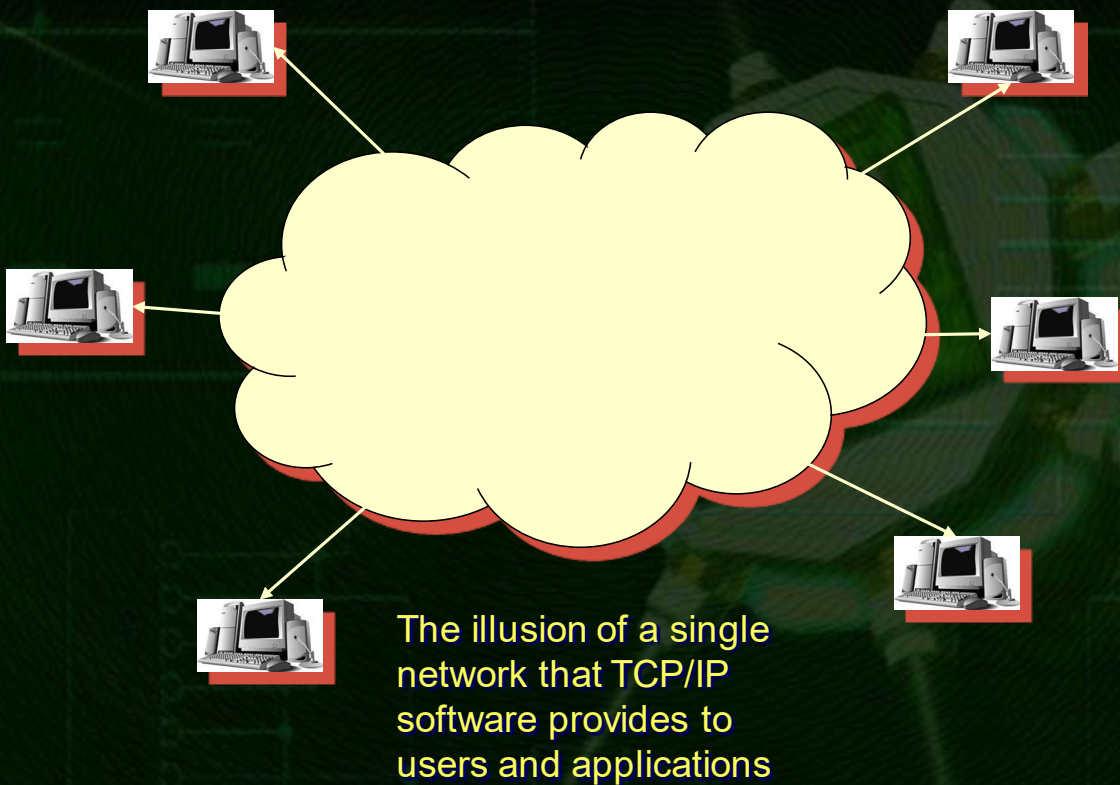
Achieving Universal Services

- ♦ The goal of internetworking is universal service across heterogeneous networks.
- ♦ To provide this service all computers, and routers must agree to forward information from a source on one network to a specified destination.

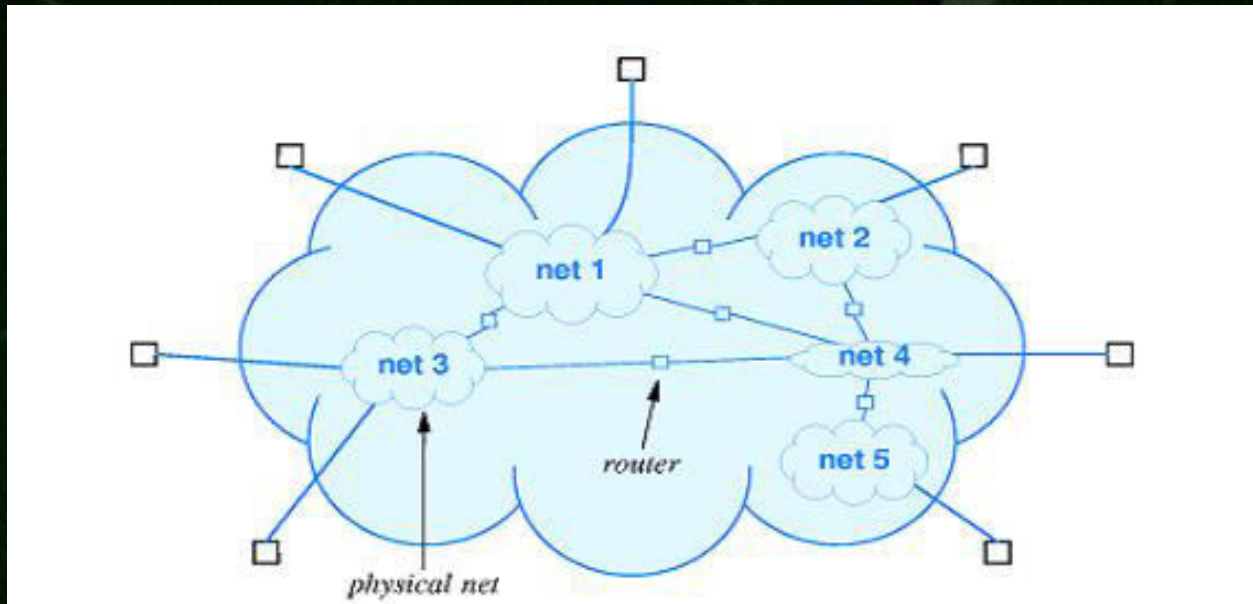
Achieving Universal Services

- ◆ The task is complicated as frame formats and addressing schemes may differ.
- ◆ The key is universal protocol software (TCP/IP).

A Virtual Network



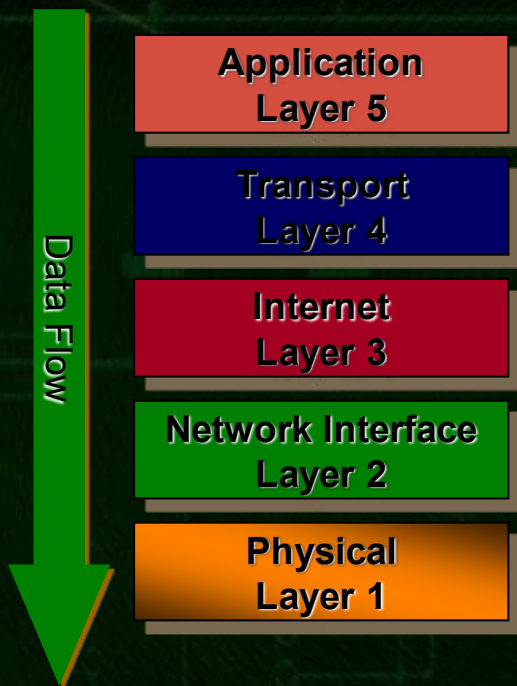
A Virtual Network



Layering And TCP/IP Protocols

- ◆ TCP/IP protocols are organized into five conceptual layers.
- ◆ Although some layers of the TCP/IP reference model correspond to layers of the ISO reference model, the ISO layers scheme does not have a layer that corresponds to TCP/IP Internet Layer.

Layering And TCP/IP Protocols



- ♦ Layer 1 Corresponds To Basic Network Hardware Layer In OSI..
- ♦ Layer 2 Specifies How To Organize Data Into Frames.
- ♦ Layer 3 Specifies The Format Of Packets Sent Across An Internet And Forward Packets.
- ♦ Layer 4 Specifies How To Ensure Reliable Transfer.
- ♦ Layer 5 Like 6 And 7 In OSI Species How One Application Uses An Internet.

Host Computers, Routers, and Protocol Layers

- ♦ TCP/IP defines the term **host computer** to refer to any computer system that connect to an internet and runs applications.
- ♦ TCP/IP protocols makes it possible for any pair of host to communicate despite hardware differences.
- ♦ Both host and routers need TCP/IP protocol software.
 - Routers do not need Layer 5 protocols for applications as they do not run applications.

Summary

- ◆ Motivation for internetworking
- ◆ Concept of Universal Services
- ◆ Internet Architecture
- ◆ A Virtual Network
- ◆ Layering and TCP/IP Protocols
- ◆ Host Computers, Routers and Protocol Layers

COMPUTER NETWORKS

CS610

Lecture-23

Hammad Khalid Khan

Review Lecture 23

- ◆ Motivation for Internetworking
- ◆ The concept of Universal Service
- ◆ Internetworking
- ◆ Physical Connections using Routers
- ◆ Internet Architecture
- ◆ The Virtual Network
- ◆ TCP/IP Protocol Suite and Layering

Address for the Virtual Internet

- ◆ To provide uniform addressing in an internet protocol software defines an abstract addressing scheme that assigns each host a unique protocol address.
- ◆ Users, application programs, and higher layers of protocol software use the abstract protocol addresses to communicate.

The IP Addressing Scheme

- ◆ An Internet Address (IP Address) is a unique 32-bit binary number assigned to a host and used for all communication with the host.
- ◆ Each packet sent across an internet contains the 32-bit IP address of the sender (source) as well as the intended recipient (destination).

The IP Address Hierarchy

- ◆ Each 32-bit IP address is divided into two parts:
 - Prefix: identifies the physical network to which the computers are attached.
 - Suffix: identifies an individual computer on the network.

The IP Address Hierarchy

- ◆ The physical network in an internet is assigned a unique value known as a network number.
- ◆ No two networks can be assigned the same network number and no two computers on the same network can be assigned the same suffix.
- ◆ A suffix value can be used on more than one network.

The IP Address Hierarchy

- ◆ The IP address hierarchy guarantees two important principles:
 - Each computer is assigned a unique address.
 - Although network number assignment must be coordinated globally, suffices can be assigned locally.

Original Classes Of IP Addresses

- ♦ The original IP address scheme divides host addresses into three primary classes.
- ♦ The class of an address determines the boundary between the network prefix and suffix.

Original Classes Of IP Addresses

	bits	0	1	2	3	4	8	16	24	31
Class A		0					prefix			suffix
Class B		1	0				prefix			suffix
Class C		1	1	0			prefix			suffix
Class D		1	1	1	0					multicast address
Class E		1	1	1	1					reserved for future use

Summary

- ◆ Addresses for Virtual Internet
- ◆ The IP addressing Scheme
- ◆ The Address Hierarchy
- ◆ Original Classes of IP Addresses

COMPUTER NETWORKS

CS610

Lecture-25

Hammad Khalid Khan

Review Lecture 24

- ◆ Addresses for Virtual Internet
- ◆ The IP addressing Scheme
- ◆ The IP Address Hierarchy
- ◆ Original Classes of IP Addresses

Computing The Class Of An Address

- ◆ Whenever it handles a packet, IP software needs to separate the destination address into a prefix and suffix.
- ◆ Classful IP addresses are self-identifying because the class of an address can be computed from the address itself.

Computing The Class Of An Address

First Four Bits Of Address	Table Index (in decimal)	Class of Address
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Dotted Decimal Notation

- ◆ Dotted decimal notation is a syntactic form, the IP software uses to express 32-bit binary values when interacting with humans.
- ◆ Dotted decimal represent each octet in decimal and uses a dot to separate octets.

Dotted Decimal Notation

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

Classes And Dotted Decimal Notation

- ◆ In class A the last three octets correspond to a host suffix.
- ◆ In Class B the last two octets are the host octets.
- ◆ Class C only has one octet to represent the host.

Classes And Dotted Decimal Notation

- ♦ The range of decimal values found in the first octet of each address class.

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

Division Of The Address Space

- ♦ The IP class scheme does not divide the 32-bit address space into equal size class and the classes do not contain the same number of networks.

$$2^n$$

$$2^n$$

Division Of The Address Space

- ♦ A prefix of n bits allows unique network numbers, while a suffix of n bits allows host numbers to be assigned on a given network.

Division Of The Address Space

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

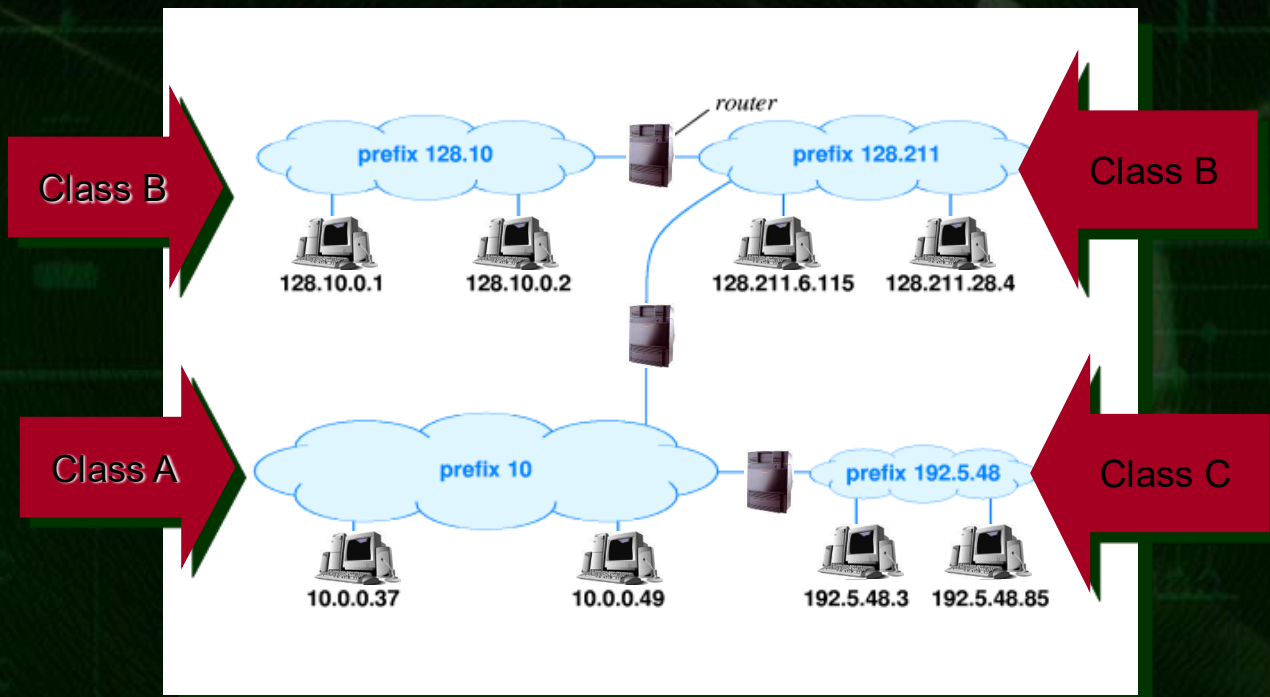
Authority For Addresses

- ◆ Throughout the internet, each network prefix is unique.
- ◆ Networks obtain their network numbers from their Internet Service Provider (ISP).
- ◆ The Internet service providers coordinate with The Internet Assigned Number Authority to obtain their network numbers.

Classful Addressing Example

- ◆ Here we have a private TCP/IP network which consists of four physical networks.
- ◆ The first step is to assign IP addresses.
 - Usually assigned class C addressed.
- ◆ Network administrator computes the ultimate size of each physical network and assigns a prefix.

Classful Addressing Example



Summary

- ◆ Computing the Class of an IP Address
- ◆ Dotted Decimal Notation
- ◆ Classes & Dotted Decimal Notation
- ◆ Division of the Address Space
- ◆ Authority For Address
- ◆ A Classful Addressing Example

COMPUTER NETWORKS

CS610

Lecture-26

Hammad Khalid Khan

Review Lecture 25

- ◆ Computing The Class of An Address
- ◆ Dotted Decimal Notation
- ◆ Division of Address Space
- ◆ A Classful Addressing Example

Subnets and Classless Addressing

- ♦ As the Internet grew, the original classful addressing scheme became a limitation.
 - The IP address space was being exhausted.
 - Because all networks had to choose one of three possible sizes, many addresses were unused.

Subnets and Classless Addressing

- ♦ Two new mechanisms were invented to overcome the limitations:
 - Subnet addressing
 - Classless addressing

Subnets and Classless Addressing

- ◆ Instead of having three distinct address classes, allow the division between prefix and suffix to occur on an arbitrary boundary.
- ◆ The classless addressing scheme solves the problem by allowing an ISP to assign a prefix that is 28 bits long (allowing the host to have up to 14 hosts).

Subnet/Address Mask

- ◆ D = Destination Address
- ◆ (A,M) = (32-bit IP Address, 32-bit Address Mask)
 - $A == (D \& M)$
 - Example:- 32-bit mask
 - 11111111 11111111 00000000 00000000
 - Denoted in dotted decimal as 255.255.0.0

Subnet and Classless Addresses

Subnet/Address Mask

- 32-bit network prefix

10000000 00001010 00000000 00000000

Denoted in dotted decimal value as 128.10.0.0

32-bit destination address 128.10.2.3

Binary equivalent:

10000000 00001010 00000010 00000011

Subnet/Address Mask

A logical 'and' between D and M produces the binary result

10000000 00001010 00000000 00000000

Which is equal to prefix 128.10.0.0

Subnet/Address Mask

- ◆ How can an IP address be divided at an arbitrary boundary?
- ◆ To use a classless or subnet address, table inside host and routers that contain address must keep two pieces of information with each address: the 32-bit address itself and another 32-bit value that specifies the boundary.
- ◆ Known as the Address Mask or Subnet Mask.

CIDR Notation

- ◆ Inside a computer, each address mask is stored as a 32-bit value.
- ◆ When we enter a prefix and an address mask they use a modified form of dotted decimal addressing called CIDR addressing.
- ◆ Known as CIDR notation

128.10.0.0/16

CIDR Notation

- ◆ As an example of how CIDR adds flexibility, suppose a single class B prefix (e.g. 128.211.0.0) i.e. 2^{16} host addresses
- ◆ 16-bit CIDR mask denoted as:

128.211.0.0 / 16

That is, by making CIDR mask correspond exactly to the old classful interpretation.

CIDR Notation

- ◆ It will be fine if 2^{16} hosts are attached. If it does have two customers with only twelve computers each, the ISP can use CIDR to partition the address into three pieces,
 - Two of them each big enough for one of the customers.
 - Remainder available for future customers.

CIDR Notation

- ◆ For example:-
 - One customer can be assigned
128.211.0.16 /28
 - And the other customer can be assigned
128.211.0.32 /28Both customers have same mask size, the prefix differs.
i.e. each customer has a unique prefix.

CIDR Host Addresses

0 **Network Prefix 128.211.0.16 /28** 28 31
1 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

0 **Address Mask 255.255.255.240** 28 31
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0

0 **Lowest Host Address 128.211.0.17** 28 31
1 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1

0 **Highest Host Address 128.211.0.30** 28 31
1 0 0 0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0

Summary Of Special IP Addresses

Prefix	Suffix	Type Of Address	Purpose
all-0s	all-0s	this computer	used during bootstrap
network	all-0s	network	identifies a network
network	all-1s	directed broadcast	broadcast on specified net
all-1s	all-1s	limited broadcast	broadcast on local net
127	any	loopback	testing

Summary

- ◆ Subnet and Classless Addressing
- ◆ Subnet/Address Mask
- ◆ CIDR Notation
- ◆ Special IP Addresses

COMPUTER NETWORKS

CS610

Lecture-27

Hammad Khalid Khan

Review Lecture 26

- ◆ Subnet and Classless Addressing
- ◆ Subnet/Address Mask
- ◆ CIDR Notation
- ◆ Special IP Addresses

Chapter 19

Binding Protocol Addresses

Protocol Addresses and Packet Delivery

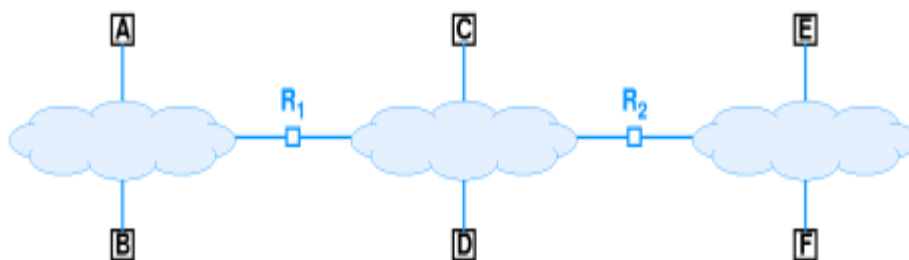
- ◆ Protocol addresses are abstractions provided by software.
- ◆ Physical network hardware does not know how to locate a computer from its protocol address.
- ◆ The protocol address of the next hop must be translated to an equivalent hardware address before a packet can be sent.

Protocol Addresses and Packet Delivery

Address Resolution

- ◆ Mapping between a protocol address and a hardware address is called Address Resolution.
- ◆ A host or router uses address resolution when it needs to send a packet to another computer on the same physical network.
- ◆ A computer never resolves the address of a computer that attaches to a remote network.

Address Resolution



Address Resolution

- ◆ A resolves protocol address for B for protocol messages from an application on A sent to an application on B.
- ◆
- ◆ A does not resolve a protocol address for F.
 - Through the internet layer, A delivers to F by routing through R1 and R2.
 - A resolves R1 hardware address.
 -
- ◆ Network layer on A passes packet containing destination protocol address F for delivery to R1.

Address Resolution Techniques

- ◆ Address resolution algorithms can be grouped into three basic categories:
 - Table lookup
 - Closed-form computation
 - Message Exchange

Address Resolution Techniques

- ◆ Table lookup
 - Binding or mapping are stored in a table in memory, which the software searches when it needs to resolve an address.
- ◆ Closed-form computation
 - The protocol address assigned to a computer is chosen carefully so that computer's hardware can be computed from the protocol address using basic Boolean and arithmetic operations.

Address Resolution Techniques

- ◆ Message Exchange
 - Computers exchange messages across a network to resolve an address.
 - One computer sends a message that requests an address binding (translation) and another computer sends a reply that contains the requested information.

Address Resolution with Table Lookup

- ◆ Resolution requires a data structure that contains information about address binding.
- ◆ A separate address binding table is used for each physical network.
- ◆ The chief advantage of the table look up approach is generality, a table can store the address bindings for an arbitrary set of computers.

Address Resolution with Table Lookup

- ◆ For less than a dozen hosts, a sequential search can suffice.
- ◆ For large networks the sequential approach uses too much CPU time.

Address Resolution with Table Lookup

<u>IP Address</u>	<u>Hardware Address</u>
197.15.3.2	0A:07:4B:12:82:36
197.15.3.3	0A:9C:28:71:32:8D
197.15.3.4	0A:11:C3:68:01:99
197.15.3.5	0A:74:59:32:CC:1F
197.15.3.6	0A:04:BC:00:03:28
197.15.3.7	0A:77:81:0E:52:FA

Address Resolution with Table Lookup

- ◆ Two standard implementations to improve computational efficiency:
 - Hashing
 - Direct Indexing

Address Resolution with Table Lookup

- ◆ Hashing

- Hashing is the transformation of a string of characters into a usually shorter fixed-length value or a key that represents the original string.
- Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value.
- It is also used in many encryption algorithms.

Address Resolution with Table Lookup

- ◆ Direct Indexing

- Less generally known technique.
- Possible only in cases where protocols addresses are assigned from a compact range.

Address Resolution with Table Lookup



Address Resolution with Closed-Form Computation

- ◆ For networks use configurable addressing it is possible to choose an address that make closed-form address resolution possible.
- ◆ A resolver is used to compute a mathematical function that maps an IP address to a hardware address.

Address Resolution with Closed-Form Computation

- ◆ When a computer connects to a network that uses configurable address, the local network administrator must choose a hardware address as well as an IP address.
- ◆ The two values can be chosen to make address resolution trivial.

Address Resolution with Closed-Form Computation

- ◆ Example:- Suppose a configurable network number:
220.123.5.0 / 24
 - The IP address of first host = 220.123.5.1
Hardware Address = 1
 - The IP address of second host = 220.123.5.2
Hardware Address = 2

Address Resolution with Closed-Form Computation

Hardware Address = 101

The IP address of router = 220.123.5.101

A single Boolean 'and' operation can compute the computer's hardware address i.e.

Hardware address = ip_address & 0xff

Address Resolution with Message Exchange

- ◆ An alternative to local computations is a distributed approach.
- ◆ A computer that needs to resolve an address, sends a message across a network and receives a reply.
- ◆ The message carries a request that species the protocol address, and reply carries the corresponding hardware address.

Address Resolution with Message Exchange

- ◆ Two possible designs:
 - Centralized
 - Distributed

Address Resolution with Message Exchange

- ◆ CENTRALIZED
 - A network includes one or more servers that are assigned the task of answering address resolution requests.
 - Advantage: Resolution easier to configure, manage and control.

Address Resolution with Message Exchange

◆ DISTRIBUTED

- Each computer on the network participates in address resolution by agreeing to answer resolution request for its address.
- Advantage: Address resolution servers can become a bottleneck and reduce cost.

Address Resolution Summary

Feature	Type Of Resolution
Useful with any hardware	T
Address change affects all hosts	T
Protocol address independent of hardware address	T, D
Hardware address must be smaller than protocol address	C
Protocol address determined by hardware address	C
Requires hardware broadcast	D
Adds traffic to a network	D
Produces resolution with minimum delay	T, C
Implementation is more difficult	D

Address Resolution Protocol

- ◆ TCP/IP can use any of the three address resolution method depending on the addressing scheme used by the underlying hardware.
- ◆ To guarantee that all computers agree on the exact format and meaning of message used to resolve addresses, the TCP/IP protocol suite includes an Address Resolution Protocol (ARP).

Address Resolution Protocol

- ◆ The ARP standard defines two basic message types:
- ◆ Request
 - Contains an IP address and requests the corresponding hardware address.
- ◆ Response
 - Contains both the IP address sent in the request and the hardware address.

Summary

- ◆ Address Resolution
- ◆ Address Resolution with Table Lookup
- ◆ Address Resolution with Closed-Form Computation
- ◆ Address Resolution with Message Exchange

COMPUTER NETWORKS

CS610

Lecture-28

Hammad Khalid Khan

Review Lecture 27

- ◆ Protocol Addresses and Packet Delivery
- ◆ Address Resolution
- ◆ Address Resolution Techniques
 - Table Lookup
 - Closed-Form Computation
 - Dynamic Message Exchange

Address Resolution Techniques

Feature	Type Of Resolution
Useful with any hardware	T
Address change affects all hosts	T
Protocol address independent of hardware address	T, D
Hardware address must be smaller than protocol address	C
Protocol address determined by hardware address	C
Requires hardware broadcast	D
Adds traffic to a network	D
Produces resolution with minimum delay	T, C
Implementation is more difficult	D

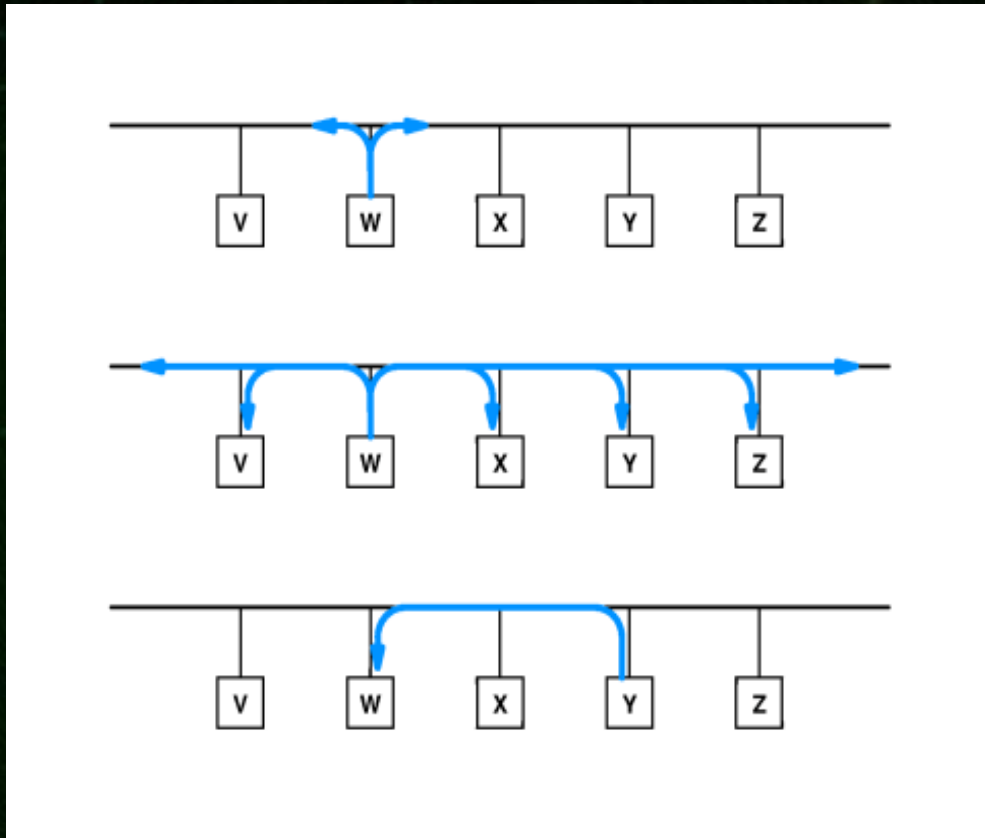
Address Resolution Protocol

- ◆ TCP/IP can use any of the three address resolution method depending on the addressing scheme used by the underlying hardware
- ◆ To guarantee that all computers agree on the exact format and meaning of message used to resolve addresses, the TCP/IP protocol suite includes an Address Resolution Protocol (ARP)

Address Resolution Protocol

- ◆ The ARP standard defines two basic message types:
- ◆ Request
 - Contains an IP address and requests the corresponding hardware address
- ◆ Response
 - Contains both the IP address sent in the request and the hardware address

ARP Message Delivery



ARP Message Format

- ◆ Although the ARP message format is sufficiently general to allow arbitrary protocol and hardware addresses:
 - ARP almost always used to bind a 32-bit IP address to a 48-bit Ethernet address

ARP Message Format

0	8	16	24	31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE		
HADDR LEN	PADDR LEN	OPERATION		
SENDER HADDR (first 4 octets)				
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)		
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)		
TARGET HADDR (last 4 octets)				
TARGET PADDR (all 4 octets)				

Sending An ARP Message

- ◆ When one computer sends an ARP message to another, the message travels inside the hardware frame.
- ◆ Technically, placing a message inside a frame for transport is called encapsulation.

Sending An ARP Message



Identifying ARP responses

- ◆ How does a computer know whether an incoming frame contains an ARP message?
- ◆ The type field in the frame header specifies that the frame contains an ARP message.
- ◆ The Ethernet standard specifies that the type field in an Ethernet frame carrying an ARP message must contain the hexadecimal value 0x806.

Identifying ARP responses

Dest. Address	Source Address	Frame Type	Data In Frame
		806	complete ARP message

Caching ARP Responses

- ◆ Although message exchange can be used to bind addresses, sending a request for each binding is hopelessly inefficient.
- ◆ To reduce network traffic, ARP software extracts and saves the information from a response so it can be used for subsequent packets.
- ◆ ARP manages the Table as a cache short term storage.

Processing an incoming ARP Message

- ◆ When an ARP message arrives, the protocol specifies that the receiver must perform two basic steps:
- ◆ First, the receiver extracts the sender's address binding and checks to see if it is present in the cache.
- ◆ If not, it updates the cache.

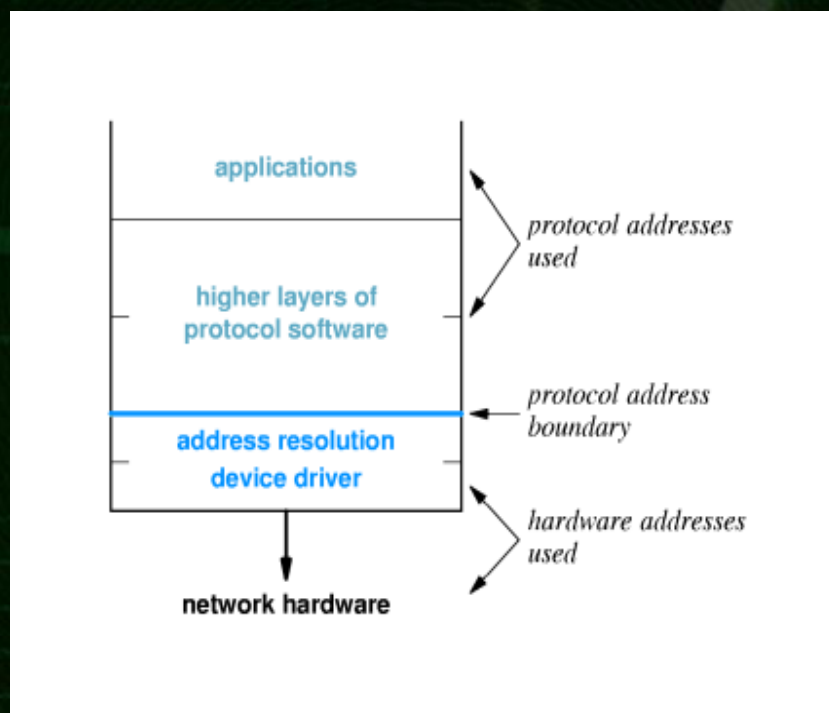
Processing an incoming ARP Message

- ◆ The receiver examines the operation field of the message to determine whether the message is a request or a response.
 - If the message is a request, the receiver compares the field TARGET PADDR with the local protocol address.
 - If the two are identical, the computer is the target of the request and must send an ARP response.

Layering, Address Resolution, Protocol Addresses

- ◆ Address resolution (ARP) is a network interface layer function.
- ◆ Protocol addresses used in all higher layers.
- ◆ Hides ugly details and allows generality in upper layers.

Layering, Address Resolution, Protocol Addresses



Summary

- ◆ Address Resolution Protocol
- ◆ ARP Message Delivery & Format
- ◆ Identifying and Caching ARP Responses
- ◆ Layering, Address Resolution, Protocol Addresses

COMPUTER NETWORKS

CS610

Lecture-29

Hammad Khalid Khan

Review Lecture 28

- ◆ Address Resolution Protocol (ARP)
- ◆ ARP Message Delivery & Format
- ◆ Sending an ARP Message
- ◆ Identifying ARP Responses
- ◆ Caching ARP Responses
- ◆ Processing an Incoming ARP Message
- ◆ Layering, Address Resolution and Protocol Addresses

Chapter 20

IP Datagrams and Datagram Forwarding

Introduction

- ◆ Fundamental Internet communication service
- ◆ Format of packets
- ◆ Processing of packets by Routers
 - Forwarding
 - Delivery

Connectionless service

- ◆ End-to-end delivery service is connectionless
- ◆ Extension of LAN abstraction
 - Universal addressing
 - Data delivered in packets (frames), each with a header
- ◆ Combines collection of physical networks into single, virtual network.

Connectionless service

- ◆ Transport protocols use this connectionless service to provide:
 - Connectionless data delivery (UDP)
- and
- Connection-oriented data delivery (TCP)

Virtual Packets

- ◆ Packets serve same purpose in internet as frames on LAN.
- ◆ Each has a header.
- ◆ Routers (formerly gateways) forward between physical networks.

Virtual Packets

- ♦ Packets have a uniform, hardware-independent format.
 - Includes header and data.
 - Can't use format from any particular hardware.
- ♦ Encapsulated in hardware frames for delivery across each physical network.

IP Datagram Format

- ♦ Formally, the unit of IP data delivery is called a Datagram.
- ♦ Includes header area and data area.

Header

Data Area



IP Datagram Size

- ◆ Datagrams can have different sizes:
 - Header area usually fixed (20 octets) but can have options.
 - Data area can contain between 1 octet and 65,535 octets ($2^{16} - 1$).
 - Usually, data area is much larger than header.

Forwarding Datagrams

- ◆ Header contains all information needed to deliver datagram to the destination computer.
 - Destination address
 - Source address
 - Identifier
 - Other delivery information
- ◆ Router examines header of each datagram and forwards datagram along path to destination.

Routing Table

- ◆ For efficiency, information about forwarding is stored in a routing table.
 - Initialized at system initialization.
 - Must be updated as network topology changes.
- ◆ Contains list of destination networks and next hop for each destination.

Routing Table



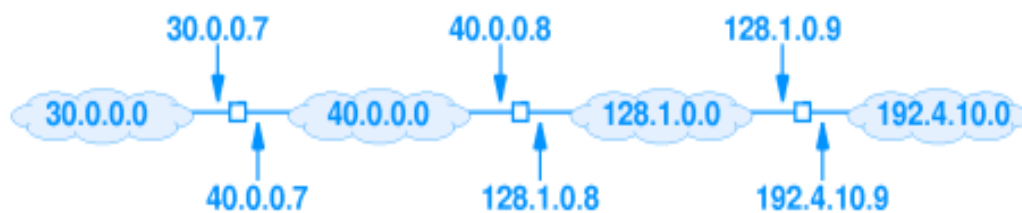
Destination	Next Hop
net 1	R_1
net 2	deliver direct
net 3	deliver direct
net 4	R_3

(b)

Routing Tables & Address Masks

- ◆ In practice, additional information is kept in routing table.
- ◆ Destination stored as network address.
- ◆ Next hop stored as IP address of router.
- ◆ Address mask defines how many bits of address are in prefix.
 - Prefix defines how much of address used to identify network.
 - E.g., class A mask is 255.0.0.0.
 - Used for subnetting.

Routing Tables & Address Masks



(a)

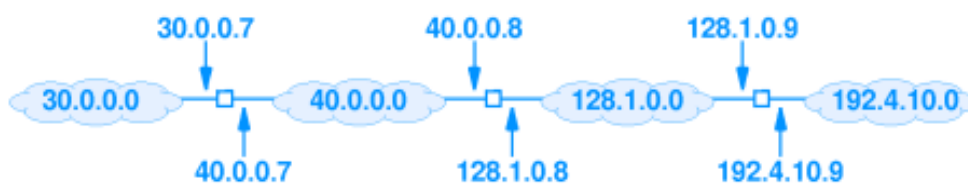
Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

Address Masks

- ◆ To identify destination network, apply address mask to destination address and compare to network address in routing table.
- ◆ Can use Boolean and
- ◆ if $((\text{Mask}[i] \& D) == \text{Dest}[i])$ forward to $\text{NextHop}[i]$.

Address Masks



(a)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

Forwarding, Destination Address and Next-hop

- ◆ Destination address in IP datagram is always ultimate destination.
- ◆ Router looks up next-hop address and forwards datagram.
- ◆ Network interface layer takes two parameters:
 - IP datagram
 - Next-hop address
- ◆ Next-hop address never appears in IP datagram.

Best-Effort Delivery

- ◆ IP provides service equivalent to LAN.
- ◆ Does not guarantee to prevent:
 - Duplicate datagrams
 - Delayed or out-of-order delivery
 - Corruption of data
 - Datagram loss

Best-Effort Delivery

- ◆ Reliable delivery provided by Transport layer
- ◆ Network layer - IP - can detect and report errors without actually fixing them.
 - Network layer focuses on datagram delivery.
 - Application layer not is interested in differentiating among delivery problems at intermediate routers.

Summary

- ◆ IP Datagram and Datagram Forwarding
- ◆ Connectionless service
- ◆ Virtual Packets
- ◆ IP Datagram Format and Size
- ◆ Routing Table and Address Masks
- ◆ Best Effort Delivery

COMPUTER NETWORKS

CS610

Lecture-30

Hammad Khalid Khan

Review Lecture 29

- ◆ IP Datagram and Datagram Forwarding
- ◆ Connectionless service
- ◆ Virtual Packets
- ◆ IP Datagram Format and Size
- ◆ Routing Table and Address Masks
- ◆ Best Effort Delivery

IP Datagram Header Format

0	4	8	16	19	24	31
VERS	H. LEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		TYPE	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (MAY BE OMITTED)					PADDING	
BEGINNING OF DATA ⋮						

IP Datagram Header Format

- ♦ VERS - version of IP (currently 4)
- ♦ H. LEN - header length (in units of 32 bits)
- ♦ SERVICE TYPE - sender's preference for low latency, high reliability (rarely used)
- ♦ TOTAL LENGTH - total octets in datagram
- ♦ IDENT, FLAGS, FRAGMENT OFFSET - used with fragmentation

IP Datagram Header Format

- ◆ TTL - time to live; decremented in each router; datagram discarded when $TTL = 0$
- ◆ TYPE - type of protocol carried in datagram; e.g., TCP, UDP.
- ◆ HEADER CHECKSUM - 1s complement of 1s complement sum.
- ◆ SOURCE, DEST ,IP ADDRESS - IP addresses of original source and ultimate destination.

IP Datagram Options

- ◆ Several options can be added to IP header:
 - Record route
 - Source route
 - Time stamp
- ◆ Header with no options has H. LEN field value 5; data begins immediately after DESTINATION IP ADDRESS.
- ◆ Options added between DESTINATION IP ADDRESS and data in multiples of 32 bits.
- ◆ Header with 96 bits of options has H. LEN field value 8.

Chapter 21

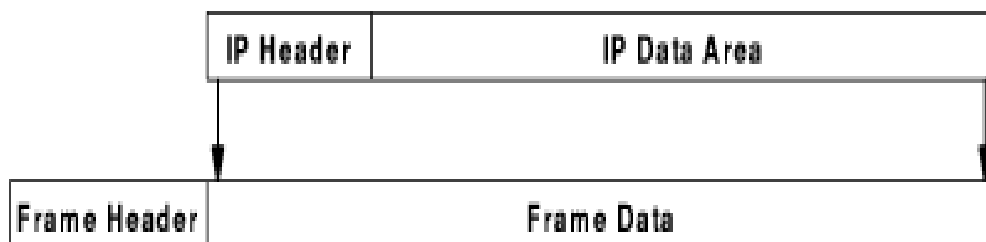
IP Encapsulation, Fragmentation and Reassembly

Datagram Transmission and Frames

Encapsulation

- ♦ Network interface layer encapsulates IP datagram as data area in hardware frame.
 - Hardware ignores IP datagram format
 - Standards for encapsulation describe details.
- ♦ Standard defines data type for IP datagram, as well as others (e.g., ARP).
- ♦ Receiving protocol stack interprets data area based on frame type.

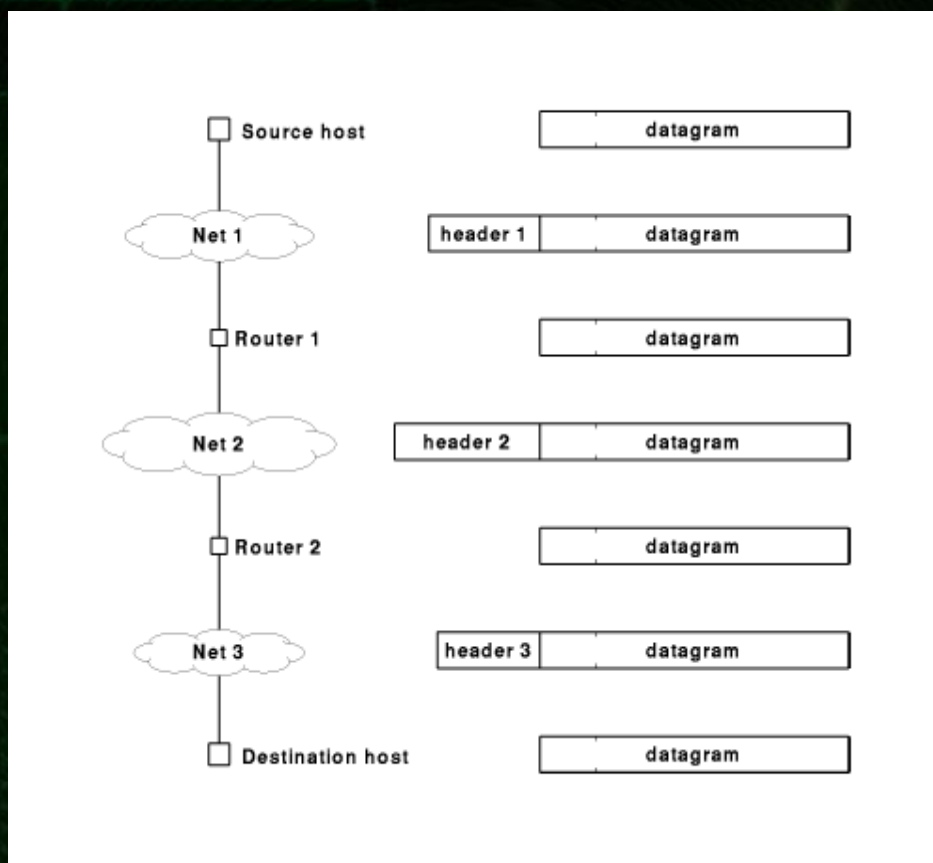
Encapsulation



Encapsulation across Multiple Hops

- ◆ Each router in the path from the source to the destination:
 - Unencapsulates incoming datagram from frame.
 - Processes datagram - determines next hop.
 - Encapsulates datagram in outgoing frame.
- ◆ Datagram may be encapsulated in different hardware format at each hop.
- ◆ Datagram itself is (almost!) unchanged.

Encapsulation across Multiple Hops



MTU

- ◆ Every hardware technology specification includes the definition of the maximum size of the frame data area.
- ◆ Called the Maximum Transmission Unit (MTU).
- ◆ Any datagram encapsulated in a hardware frame must be smaller than the MTU for that hardware.

MTU and Heterogeneous Networks

- ◆ An internet may have networks with different MTUs.
- ◆ Suppose downstream network has smaller MTU than local network?



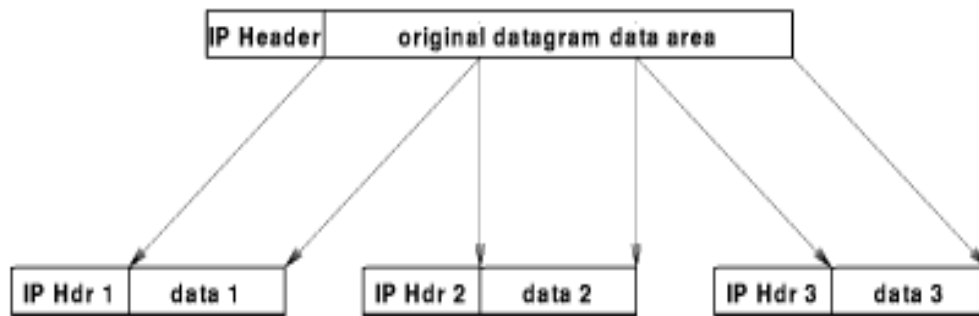
Fragmentation

- ◆ One technique - limits datagram size to smallest MTU of any network.
- ◆ IP uses fragmentation - datagrams can be split into pieces to fit in network with small MTU.
- ◆ Router detects datagram larger than network MTU.
 - Splits into pieces.
 - Each piece smaller than outbound network MTU.

Fragmentation

- ◆ Each fragment is an independent datagram
 - Includes all header fields.
 - Bit in header indicates datagram is a fragment.
 - Other fields have information for reconstructing original datagram.
 - FRAGMENT OFFSET gives original location of fragment.
- ◆ Router uses local MTU to compute size of each fragment.
- ◆ Puts part of data from original datagram in each fragment.
- ◆ Puts other information into header.

Fragmentation



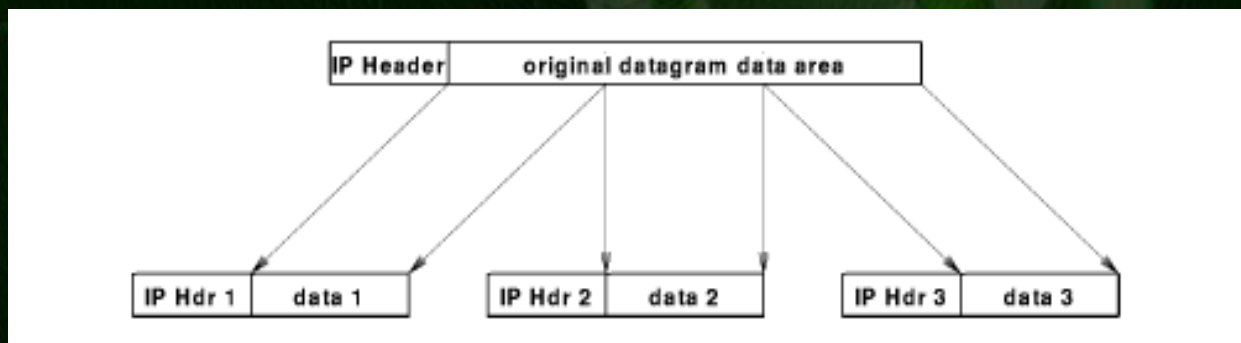
Datagram Reassembly

- ◆ Reconstruction of original datagram is called Reassembly.
- ◆ Ultimate destination performs reassembly.



Datagram Reassembly

- ◆ Fragments may arrive out of order; header bit identifies fragment containing end of data from original datagram.
- ◆ Fragment 3 identified as last fragment.



Identifying a Datagram & Fragment Loss

Fragment Loss

- ◆ IP may drop fragment.
- ◆ What happens to original datagram?
 - Destination drops entire original datagram.
- ◆ How does destination identify lost fragment?
 - Sets timer with each fragment.
 - If timer expires before all fragments arrive, fragment assumed lost.
 - Datagram dropped.
- ◆ Source (application layer protocol) assumed to retransmit.

Fragmenting a Fragment

- ◆ Fragment may encounter subsequent network with even smaller MTU.
- ◆ Router fragments the fragment to fit.
- ◆ Resulting sub-fragments look just like original fragments (except for size).
- ◆ No need to reassemble hierarchically; sub-fragments include position in original datagram.

Summary

- ◆ IP Datagram Header Format
- ◆ Datagram Transmission and Frames
- ◆ Encapsulation
- ◆ Transmission across an Internet
- ◆ MTU
- ◆ Reassembly
- ◆ Identifying a Datagram
- ◆ Fragmentation Loss
- ◆ Fragmenting a Fragment

COMPUTER NETWORKS

CS610

Lecture-31

Hammad Khalid Khan

Review Lecture 30

- ◆ IP Datagram Header Format
- ◆ Datagram Transmission and Frames
- ◆ Encapsulation
- ◆ Transmission across an Internet
- ◆ MTU
- ◆ Reassembly
- ◆ Identifying a Datagram
- ◆ Fragmentation Loss
- ◆ Fragmenting a Fragment

Chapter 22

The Future IP (IPV6)

Introduction - The Future of IP

- ◆ Current version of IP - Version 4 (IPv4) - is 20 years old
- ◆ IPv4 has shown remarkable ability to move to new technologies
- ◆ IETF has proposed entirely new version to address some specific problems
- ◆

Success of IP

Motivation for Change

- ◆ Address space
 - ◆ 32 bit address space allows for over a million networks
 - ◆ But...most are Class C and too small for many organizations
 - ◆ 214 Class B network addresses already almost exhausted (and exhaustion was first predicted to occur a couple of years ago)

Motivation for Change

- ◆ Type of service
 - ◆ Different applications have different requirements for delivery reliability and speed
 - ◆ Current IP has type of service that's not often implemented
- ◆ Multicast

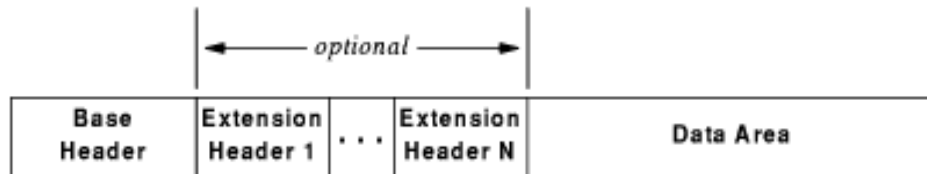
Name and Version Number

- ◆ Preliminary versions called IP - Next Generation (IPng)
- ◆ Several proposals all called IPng
- ◆ One was selected and uses next available version number (6)
- ◆ Result is IP version 6 (IPv6)

New Features

- ◆ Address size - IPv6 addresses are 128bits
- ◆ Header format - entirely different
- ◆ Extension headers - Additional information stored in optional extension headers, followed by data
- ◆ Support for audio and video - flow labels and quality of service allow audio and video applications to establish appropriate connections
- ◆ Extensible - new features can be added more easily

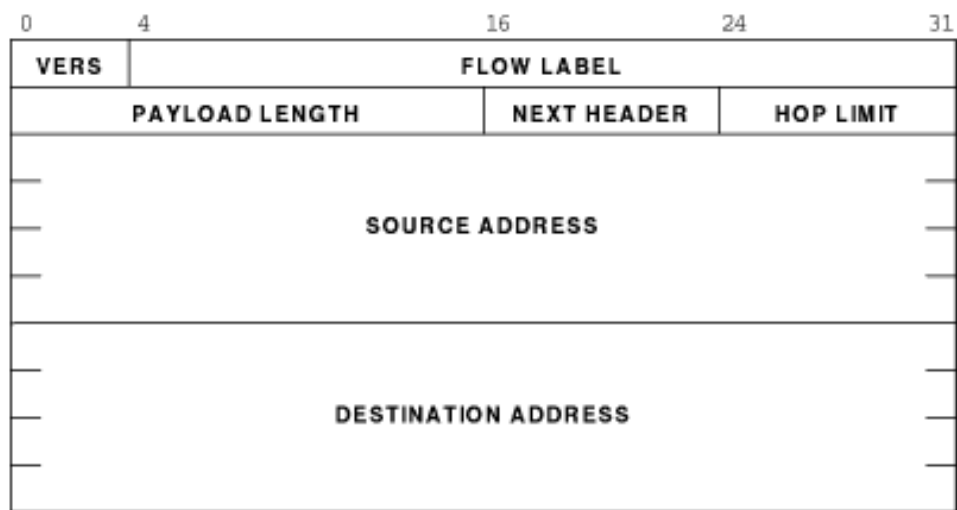
IPv6 Datagram Format



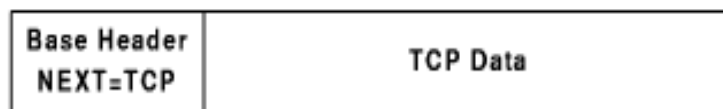
IPv6 Base Header Format

- ◆ Contains less information than IPv4 header
- ◆ NEXT HEADER points to first extension header
- ◆ FLOW LABEL used to associate datagrams belonging to a flow or communication between two applications
 - ◆ Traffic class
 - ◆ Specific path
 - ◆ Routers use FLOW LABEL to forward datagrams along prearranged path

IPv6 Base Header Format



IPv6 NEXT HEADER



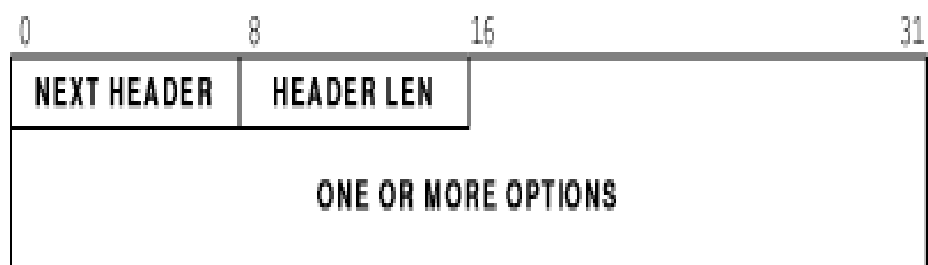
(a)



(b)

How IPVS Handles Multiple Headers

Parsing IPv6 Headers



Summary

- ◆ Success of IP
- ◆ Motivation for Change
- ◆ IPV6 Features
- ◆ IPV6 Datagram Format
- ◆ IPV6 Base Header Format
- ◆ Parsing IPV6 Headers

COMPUTER NETWORKS

CS610

Lecture-32

Hammad Khalid Khan

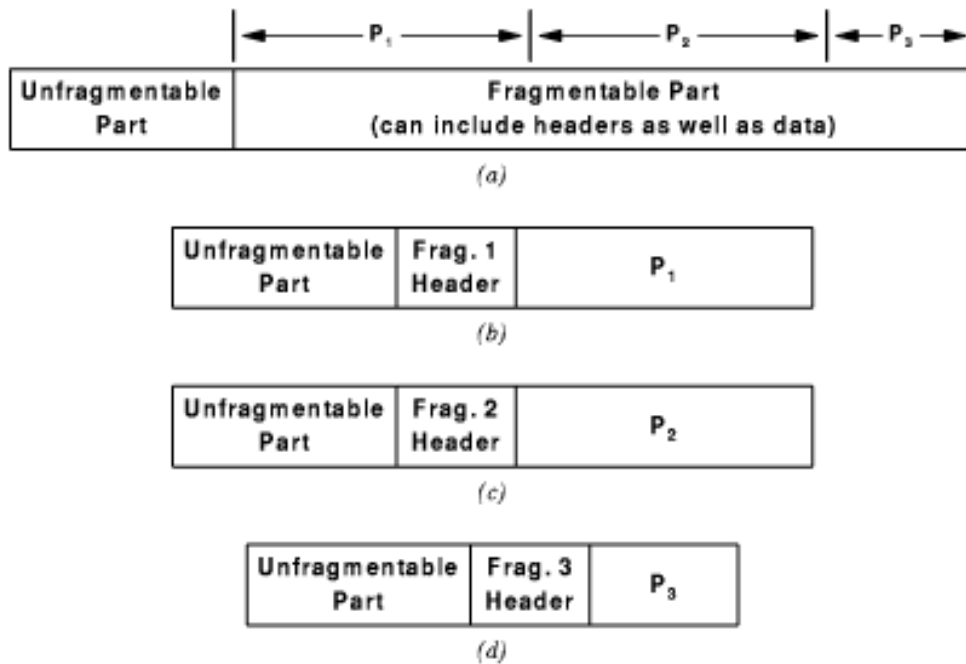
Review Lecture 31

- ◆ Success of IP
- ◆ Motivation for Change
- ◆ IPV6 Features
- ◆ IPV6 Datagram Format
- ◆ IPV6 Base Header Format
- ◆ Parsing IPV6 Headers

Fragmentation

- ◆ Fragmentation information kept in separate extension header
- ◆ Each fragment has base header and (inserted) fragmentation header
- ◆ Entire datagram, including original header may be fragmented

Fragmentation



Fragmentation and Path MTU

- ◆ IPv6 source (not intermediate routers) responsible for fragmentation
 - Routers simply drop datagrams larger than network MTU
 - Source must fragment datagram to reach destination
- ◆ Source determines path MTU
 - Smallest MTU on any network between source and destination
 - Fragments datagram to fit within that MTU

Fragmentation and Path MTU

- ◆ Uses path MTU discovery
 - Source sends probe message of various sizes until destination reached
 - Must be dynamic - path may change during transmission of datagrams

Use of Multiple Headers

- ◆ Efficiency - header only as large as necessary
- ◆
- ◆ Flexibility - can add new headers for new features
- ◆ Incremental development - can add processing for new features to testbed; other routers will skip those headers

IPv6 Addressing

- ◆ 128-bit addresses
- ◆ Includes network prefix and host suffix
- ◆ No address classes - prefix/suffix boundary can fall anywhere

IPv6 Addressing

- ◆ Special types of addresses:
 - Unicast - single destination computer
 - Multicast - multiple destinations; possibly not at same site
 - Cluster - collection of computers with same prefix; datagram is delivered to one out of cluster

IPv6 Address Notation

- ◆ 128-bit addresses unwidely in dotted decimal; requires 16 numbers
- ◆ 105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255
- ◆ Groups of 16-bit numbers in hex separated by colons - colon hexadecimal (or colon hex)
- ◆ 69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF
- ◆ Zero-compression - series of zeroes indicated by two colons
FF0C:0:0:0:0:0:0:B1
- ◆ FF0C::B1
- ◆ IPv6 address with 96 leading zeros is interpreted to hold an IPv4 address

Chapter 23

An Error Reporting Mechanism (ICMP)

Introduction

- ◆ IP provides best-effort delivery
- ◆
- ◆ Delivery problems can be ignored; datagrams can be "dropped" on the floor
- ◆ Internet Control Message Protocol (ICMP) provides error-reporting mechanism
- ◆

Best-Effort Semantics and Error Detection

- ◆ Internet layer can detect a variety of errors:
 - Checksum (header only!)
 - TTL expires
 - No route to destination network
 - Can't deliver to destination host (e.g., no ARP reply)
- ◆ Internet layer discards datagrams with problems
- ◆ Some - e.g., checksum error - can't trigger error messages

Internet Control Message Protocol

- ◆ Some errors can be reported
 - Router sends message back to source in datagram
 - Message contains information about problem
- ◆ Encapsulated in IP datagram

Types of Messages

- ◆ Internet Control Message Protocol (ICMP) defines Error and Informational messages
- ◆ Error messages:
 - Source quench
 - Time exceeded
 - Destination unreachable
 - Redirect
 - Fragmentation required

Types of Messages

- ◆ Informational messages:
 - Echo request/reply
 - Address mask request/reply
 - Router discovery

Summary

- ◆ Fragmentation in IPV6
- ◆ Use of Multiple Headers
- ◆ IPV6 Addressing
- ◆ ICMP
- ◆ Best Effort Semantics and Error Detection
- ◆ Types of ICMP Messages

COMPUTER NETWORKS

CS610

Lecture-33

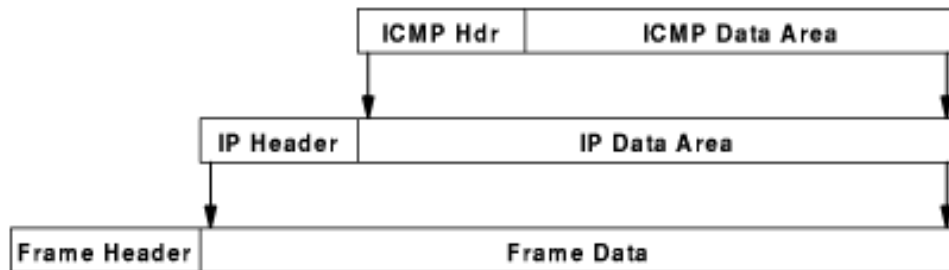
Hammad Khalid Khan

Review Lecture 32

- ◆ Fragmentation in IPV6
- ◆ Use of Multiple Headers
- ◆ IPV6 Addressing
- ◆ ICMP
- ◆ Best Effort Semantics and Error Detection
- ◆ Types of ICMP Messages

ICMP Message Transport

- ◆ ICMP encapsulated in IP



ICMP Message Transport

- ◆ How it Works?
- ◆ ICMP messages sent in response to incoming datagrams with problems
- ◆ ICMP message not sent for ICMP message

Using ICMP to Test Reachability

- ◆ An internet host, A, is reachable from another host, B, if datagrams can be delivered from A to B
- ◆ Ping program tests reachability - sends datagram from B to A that A echoes back to B
- ◆ Uses ICMP echo request and echo reply messages
- ◆ Internet layer includes code to reply to incoming ICMP echo request messages

Using ICMP to Trace a Route

- ◆ List of all routers on path from A to B is called the route from A to B
- ◆ Intermediate routers send ICMP time exceeded message to the source
- ◆ destination sends an ICMP destination unreachable message to the source

Using ICMP to Trace a Route

- ♦ `tracert` (Windows version) Sends ICMP echo messages with increasing TTL
 - Router that decrements TTL to 0 sends ICMP time exceeded message, with router's address as source address
 - First, with TTL 1, gets to first router, which discards and sends time exceeded message
 - Next, with TTL 2, gets through first router to second router
 - Continue until an ICMP echo reply message from destination received

The Last Address printed by Traceroute

- ♦ There are two possibilities used to detect the destination:
 - Send an ICMP echo request, destination host will generate an ICMP echo reply
 - Send a datagram to a non-existent application, destination host will generate an ICMP destination unreachable message

Using ICMP for Path MTU Discovery

- ◆ Fragmentation should be avoided
- ◆ How can source configure outgoing datagrams to avoid fragmentation?
- ◆ Source determines path MTU - smallest network MTU on path from source to destination
- ◆ Source probes path using IP datagrams with don't fragment flag
- ◆ Router responds with ICMP fragmentation required message
- ◆ Source sends smaller probes until destination reached

Summary

- ◆ ICMP Message Transport
- ◆ Using ICMP to Test Reachability
- ◆ Using ICMP to Trace a Route
- ◆ The Address Printed by Trace-route
- ◆ Using ICMP for Path MTU Discovery

COMPUTER NETWORKS

CS610

Lecture-34

Hammad Khalid Khan

Review Lecture 33

- ◆ ICMP Message Transport
- ◆ Using ICMP to Test Reachability
- ◆ Using ICMP to Trace a Route
- ◆ The Address Printed by Trace-route
- ◆ Using ICMP for Path MTU Discovery

Chapter 24

UDP: Datagram Transport Service

Terminology

- ♦ IP
 - Provides computer-to-computer communication
 - Source and destination addresses are computers
 - Called machine-to-machine
- ♦ Transport protocols
 - Provide application-to-application communication
 - Need extended addressing mechanisms to identify applications
 - Called end-to-end

Introduction

- ◆ UDP: The first of the Transport Protocols in TCP/IP protocol suite
- ◆ UDP protocol allows applications on the computers to send and receive datagrams.
- ◆ UDP Packet Format
- ◆ UDP uses best effort delivery service.

The Need for Transport Protocols

- ◆ Internet Protocol cannot distinguish between application programs running on the same computer.
- ◆ Fields in the IP datagram header refer to computers, not applications.
- ◆ A protocol that allows an application program to serve as the end point of communication is known as a Transport Protocol or an End-to-end protocol.

The User Datagram Protocol

- ◆ TCP/IP contains two transport protocols:
 - UDP
 - TCP
- ◆ UDP- Less Complex and easier to understand
- ◆ UDP- Does not provide the type of service a typical application expects

Characteristics of UDP

- ◆ End-to-end
- ◆ Connectionless
- ◆ Message-Oriented
- ◆ Best Effort Delivery
- ◆ Arbitrary Interaction
- ◆ Operating System Independent

The Connectionless Paradigm

- ◆ Connectionless:
 - UDP does not need to pre-establish communication
 - No need to terminate communication
- ◆ UDP allows an application to delay long intervals between two messages:
 - No Control Messages; Only Data Messages
 - Very Low Overhead

Message-Oriented Interface

- ◆ UDP offers application programs a Message-Oriented Interface.
- ◆ Does not divide messages into packets for Transmission.
- ◆ Does not combine messages for delivery.

Message-Oriented Interface

- ♦ Advantages:

- Applications can depend on protocol to preserve data boundaries.

- ♦ Disadvantage:

- Each UDP message must fit into a single IP Datagram.
- Can result to an inefficient use of the underlying network.

UDP Communication Semantics

- ♦ UDP uses IP for all delivery

- Same best-effort delivery semantics as IP

- ♦ To use UDP:

- An application must either be immune to the problems OR
- Programmer must take additional steps to detect and correct problems.

- ♦ Examples:

- Audio Transmission
- On-Line Shopping Application

Arbitrary Interaction

- ◆ UDP follows four types of interaction:
 - 1-to-1
 - 1-to-many
 - Many-to-1
 - Many-to-many

Support for Unicast, Multicast, and Broadcast

- ◆ UDP allows multicast 1-to-many interaction using multicast or a broadcast.
- ◆ Sender uses a broadcast address as the destination address to interact with MANY applications.
- ◆ Especially useful for Ethernet Networks.

Endpoint Identification with Protocol Port Numbers

- ◆ How should UDP identify an application as an endpoint?
- ◆ Mechanism cannot be the same as of the operating system.
 - No common mechanism exists
 - Multiple identifiers
 - Protocol Identifiers
 - Job Names
 - Task Identifiers

Endpoint Identification with Protocol Port Numbers

- ◆ UDP defines a set of identifiers called “Protocol Ports”.
- ◆ Independent of the underlying operating system.
- ◆ Each computer using UDP provides a mapping between the protocol port number and the program identifiers of its operating system.

Endpoint Identification with Protocol Port Numbers

- ◆ The address and protocol port specifications of an application define the type of communication.
 - To engage in a 1-to-1 communication, the application specifies:
 - The Local Port Number
 - Remote IP Address
 - The Remote Port Number

Summary

- ◆ The need for End –to-End Protocols
- ◆ User Datagram Protocol
- ◆ Characteristics of UDP
- ◆ The Connectionless Paradigm
- ◆ Message-Oriented Interface
- ◆ UDP Communication Semantics
- ◆ Arbitrary Interaction
- ◆ Support for Multicast and Broadcast
- ◆ Endpoint Identification

COMPUTER NETWORKS

CS610

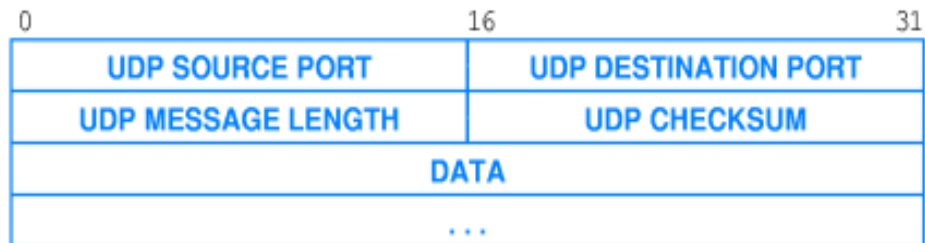
Lecture-35

Hammad Khalid Khan

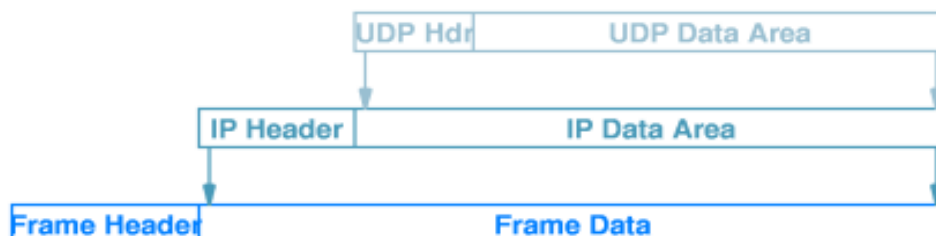
Review Lecture 34

- ◆ The need for End –to-End Protocols
- ◆ User Datagram Protocol
- ◆ Characteristics of UDP
- ◆ The Connectionless Paradigm
- ◆ Message-Oriented Interface
- ◆ UDP Communication Semantics
- ◆ Arbitrary Interaction
- ◆ Support for Multicast and Broadcast
- ◆ Endpoint Identification

UDP Datagram Format



UDP Encapsulation



Chapter 25

TCP: Reliable Transport Service

Introduction

- ◆ TCP: Major Transport Protocol in the TCP/IP suite
- ◆ Uses unreliable datagram service offered by IP when sending data to another computer
- ◆ Provides reliable data delivery service to applications

The Need for Reliable Transport

- ◆ Reliability is fundamental in a computer system
- ◆ Software in the internet must provide the same level of reliability as a computer system
- ◆ Software must guarantee prompt and reliable communication without any loss, duplication, and change in the order

Transmission Control Protocol

- ◆ Reliability is the responsibility of the Transport Layer
- ◆ In TCP/IP, TCP provides reliable transport service
- ◆ Most internet applications use TCP as no other protocol has proved to work better

Service provided by TCP

- ◆ Connection-Oriented service
- ◆ Point-to-point
- ◆ Complete Reliability
- ◆ Full-duplex communication
- ◆ Stream interface
- ◆ Reliable Connection Startup
- ◆ Graceful Connection Shutdown

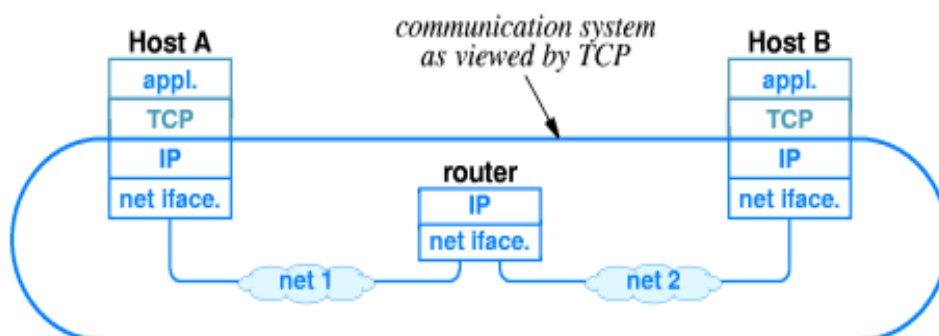
End-to-End Service and Datagrams

- ◆ Applications can request a connection
- ◆ TCP connections are called Virtual Connections
 - ◆ Created by Software only
 - ◆ Internet does not provide software or hardware support for the connections
 - ◆ TCP software modules on two computers create an illusion of a connection

End-to-End Service and Datagrams

- ◆ TCP uses IP to carry messages
- ◆ TCP message encapsulated in IP datagram and sent to the destination
- ◆ On the destination host, IP passes the contents to TCP

End-to-End Service and Datagrams



Achieving Reliability

- ◆ The major problems in the reliable delivery are:
 - ◆ Unreliable delivery by the underlying communication system
 - ◆ System reboot

Summary

- ◆ UDP datagram Format
- ◆ UDP Encapsulation
- ◆ TCP: Reliable Transport Service
- ◆ The Need For Reliable Transport
- ◆ Service Provided by TCP
- ◆ End-to-End Service and Datagrams
- ◆ Achieving Reliability

COMPUTER NETWORKS

CS610

Lecture-36

Hammad Khalid Khan

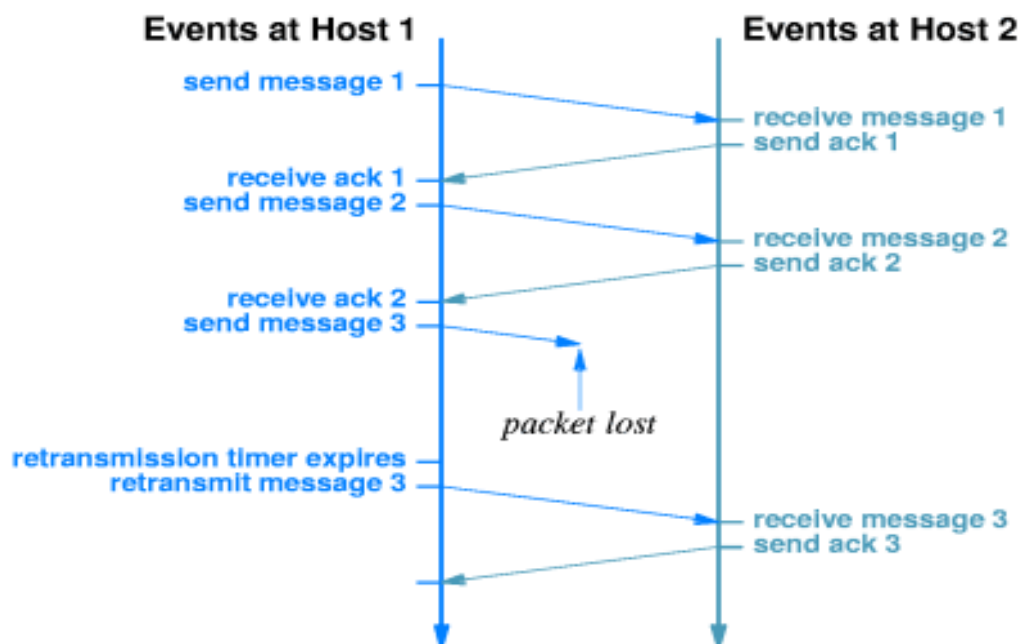
Review Lecture 35

- ◆ UDP datagram Format
- ◆ UDP Encapsulation
- ◆ TCP: Reliable Transport Service
- ◆ The Need For Reliable Transport
- ◆ Service Provided by TCP
- ◆ End-to-End Service and Datagrams
- ◆ Achieving Reliability

Packet Loss and Retransmission

- ◆ How does TCP achieve Reliability?
- ◆ Retransmission
 - An Acknowledgement is used to verify that data has arrived successfully.
 - If Acknowledgement does not arrive, the previous data is retransmitted.

Packet Loss and Retransmission



How Long Should TCP Wait Before Retransmitting?

- ◆ Time for acknowledgement to arrive depends on
 - Distance to destination
 - Current traffic conditions
- ◆ Multiple connections can be opened simultaneously.
- ◆ Traffic conditions change rapidly.

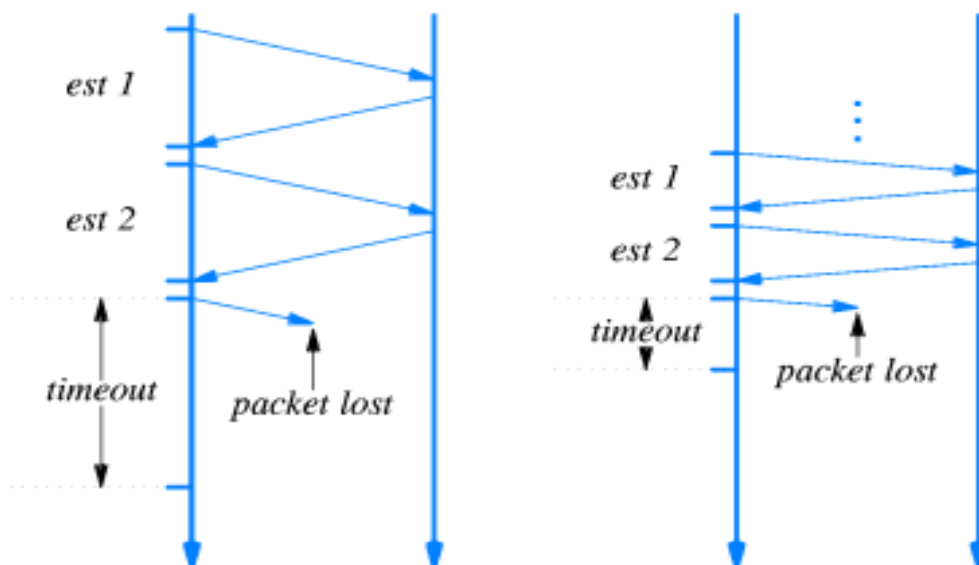
Adaptive Retransmission

- ◆ Set a timer. It sounds so easy, but ...What time interval?
 - Too long?
 - You are spending time waiting for something that is just not going to happen.
 - Too short?
 - You will resend needlessly.

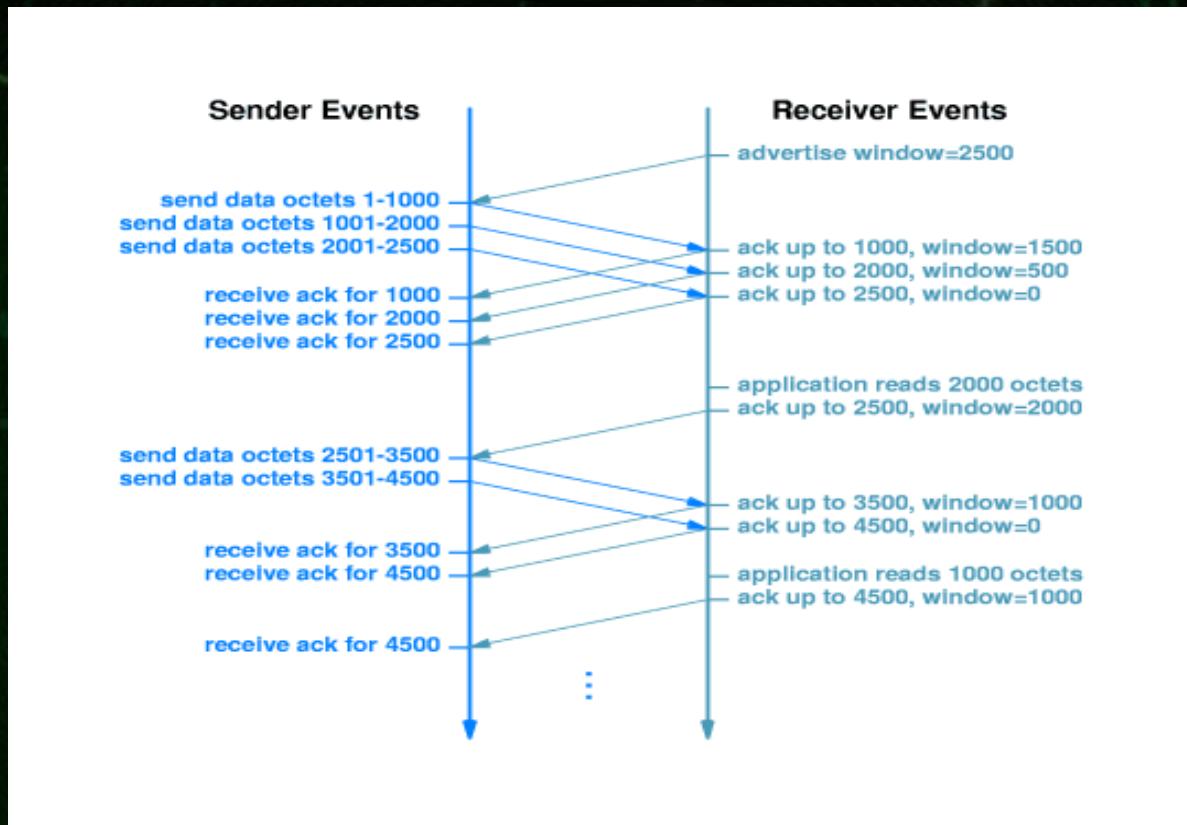
Adaptive Retransmission

- ◆ Keep estimate of round trip time on each connection
- ◆ Use current estimate to set transmission timer
- ◆ Known as Adaptive Retransmission
- ◆ Key to TCP's success

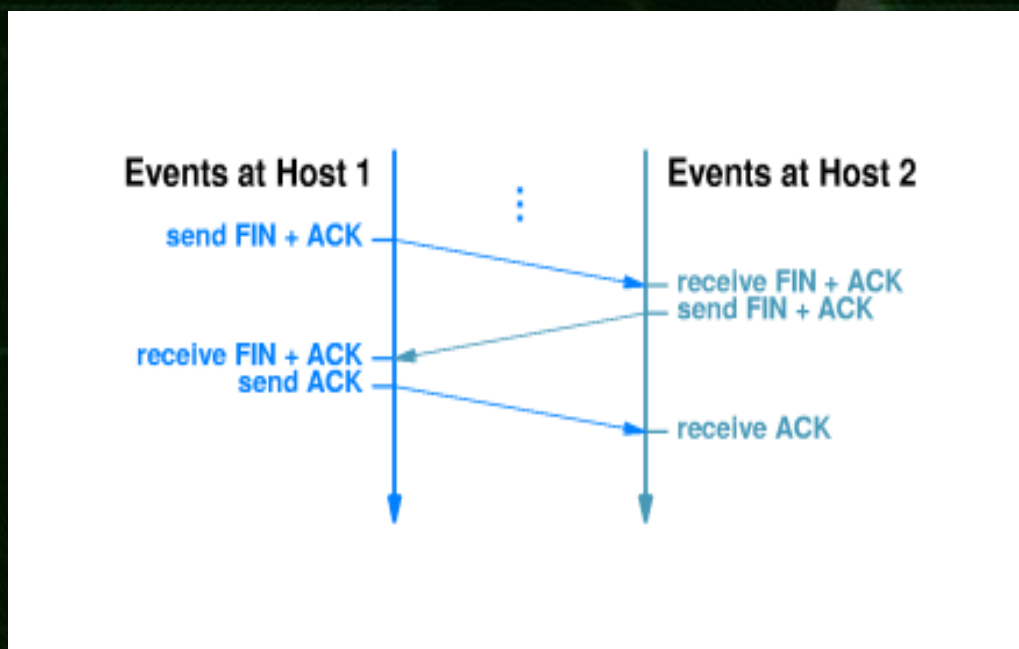
Comparison of Retransmission Times



Buffers, Flow Control & Windows



Three-Way Handshake to Close a Connection



Three-way Handshake to Begin a Connection

- ◆ This will not mean much until you look at the packets, but
 - SYN
 - Randomly chosen sequence number, $S1:0$
 - SYN + ACK
 - $S2:S1+1$
 - ACK
 - $S1+1:S2+1$

Summary

- ◆ Packet Loss and Retransmission
- ◆ Adaptive Retransmission
- ◆ Buffers, Flow Control & Windows
- ◆ Three-Way Handshake

COMPUTER NETWORKS

CS610

Lecture-37

Hammad Khalid Khan

Review Lecture 36

- ◆ Achieving Reliability
- ◆ Packet Loss and Retransmission
- ◆ Adaptive Transmission
- ◆ Buffers, Flow Control, and Windows
- ◆ Three Way Handshake

Congestion Control

- ◆ The goal is to avoid adding retransmissions to an already congested network
- ◆ Reduce window size quickly in response to lost messages
 - Assumption: loss is due to congestion
- ◆ Resume carefully. Otherwise the network will swing wildly between congestion and under utilization

TCP Segment Format

0	4	10	16	24	31
SOURCE PORT			DESTINATION PORT		
SEQUENCE NUMBER					
ACKNOWLEDGEMENT NUMBER					
HLEN	NOT USED	CODE BITS	WINDOW		
CHECKSUM			URGENT POINTER		
OPTIONS (if any)					
BEGINNING OF DATA					
⋮					

Chapter 26

Network Address Translation (NAT)

Network Address Translation (NAT)

- ◆ Extension of original addressing scheme
- ◆ Motivated by exhaustion of IP address space
- ◆ Allows multiple computers to share a single address

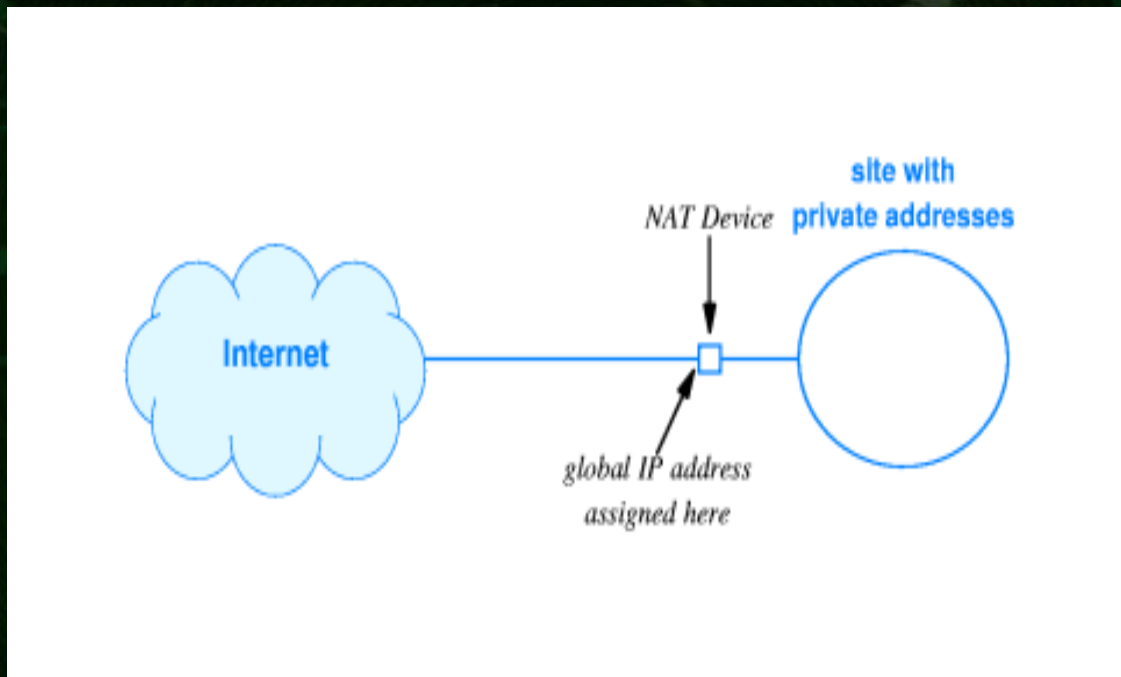
Network Address Translation (NAT)

- ◆ Requires device to perform packet translation
- ◆ Implementations available
 - Stand-alone hardware device
 - IP router with NAT functionality embedded

NAT Details

- ◆ Site
 - Obtains a single valid IP address
 - Assigns a private address to each computer
 - Uses NAT box to connect to the internet
- ◆ NAT
 - Translates address in IP datagrams

Illustration of NAT



NAT Example

- ◆ Site uses private network 10.0.0.0/8 internally
 - First computer assigned 10.0.0.1
 - Second computer assigned 10.0.0.2
 - And so on . . .
 - Site obtains a valid IP address (e.g. 128.210.24.6)
 - Assume computer 10.0.0.1 sends to 128.211.134.4

NAT Example

- ♦ NAT translates the IP source address of the outgoing datagram
- ♦ NAT translates the destination address of incoming datagram

Illustration of NAT Translation

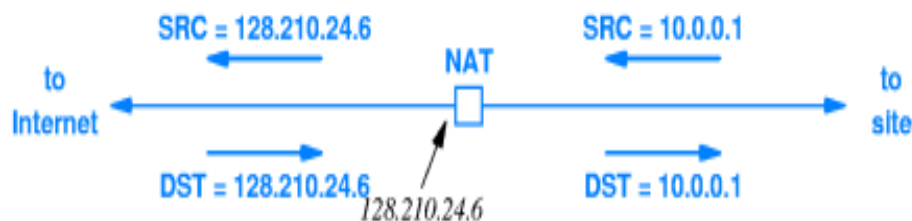


Illustration of NAT Translation

- ♦ Transparent to each end
 - Computer at site sends and receives datagrams normally
 - Computer in Internet receives datagrams from NAT box

Implementation of NAT

Direction	Field	Old Value	New Value
out	IP Source	10.0.0.1	128.10.24.6
in	IP Destination	128.10.24.6	10.0.0.1

Implementation of NAT

- ◆ NAT device stores state information in table
- ◆ Value is entered in table when NAT box receives outgoing datagram for new destination

Summary

- ◆ Congestion Control
- ◆ TCP Segment Format
- ◆ Network Address Translation
- ◆ NAT Technology
- ◆ Implementation of NAT
- ◆ Basic Address Translation

COMPUTER NETWORKS

CS610

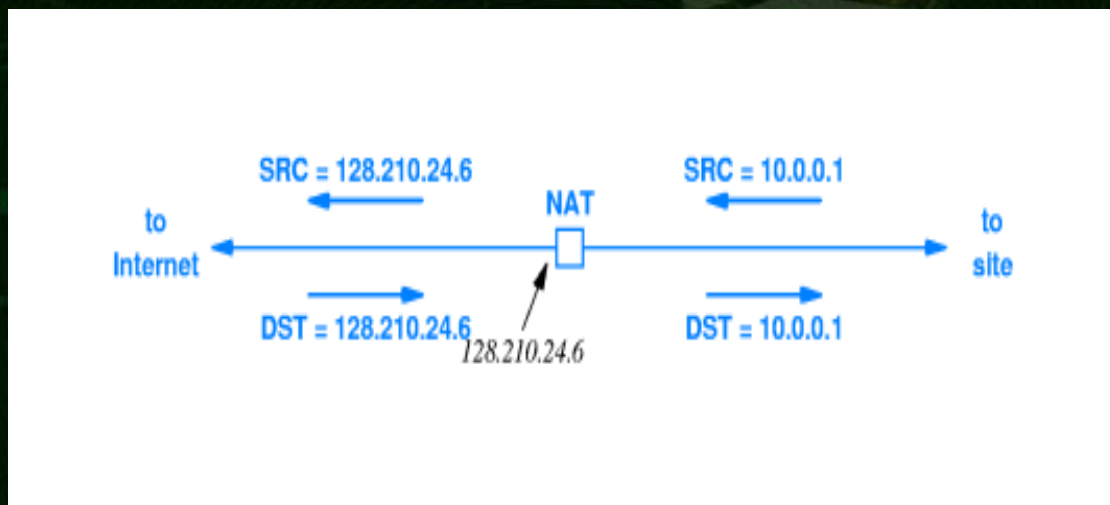
Lecture-38

Hammad Khalid Khan

Review Lecture 37

- ◆ Congestion Control
- ◆ TCP Segment Format
- ◆ Network Address Translation (NAT)
- ◆ NAT Technology
- ◆ NAT Topology
- ◆ NAT Implementations
- ◆ NAT Translation

Illustration of NAT Translation



NAT Translation Table

Direction	Field	Old Value	New Value
out	IP Source	10.0.0.1	128.10.24.6
in	IP Destination	128.10.24.6	10.0.0.1

Variants of NAT

- ◆ Basic NAT
 - Changes IP addresses
- ◆ Network Address and Port Translation
 - Changes IP addresses and protocol port numbers
 - Most popular form
- ◆ Twice NAT
 - Used with site that runs server
 - NAT box connected to Domain Name System (DNS) server

Network Address and Port Translation (NAPT)

- ◆ By far the most popular form of NAT
- ◆ Can change TCP or IP protocol port numbers as well as IP addresses
- ◆ Allows
 - Multiple computers at site to communicate with single destination
 - Multiple users on given computer to communicate with same destination

Example NAT Translation Table

Direction	Fields	Old Value	New Value
out	IP SRC:TCP SRC	10.0.0.1:30000	128.10.19.20:40001
out	IP SRC:TCP SRC	10.0.0.2:30000	128.10.19.20:40002
in	IP DEST:TCP DEST	128.10.19.20:40001	10.0.0.1:30000
in	IP DEST:TCP DEST	128.10.19.20:40002	10.0.0.2:30000

Example NAT Translation Table

- ◆ Entry in table records protocol port numbers as well as IP address
- ◆ Port numbers reassigned to avoid conflicts

TCP Splicing

- ◆ Popular use of NAT
- ◆ Interconnects two independent TCP connections
- ◆ Performs segment rewriting
- ◆ Extremely efficient: avoids overhead of extracting data from one connection and sending to the other
- ◆ Uses extended translation table

Twice NAT

- ◆ Basic NAT does not work well for communication initiated from the Internet
- ◆ Twice NAT allows a site to run servers
- ◆ Twice NAT requires the DNS to interact with the NAT device
- ◆ Twice NAT fails if an application uses the IP-Address instead of Domain Name

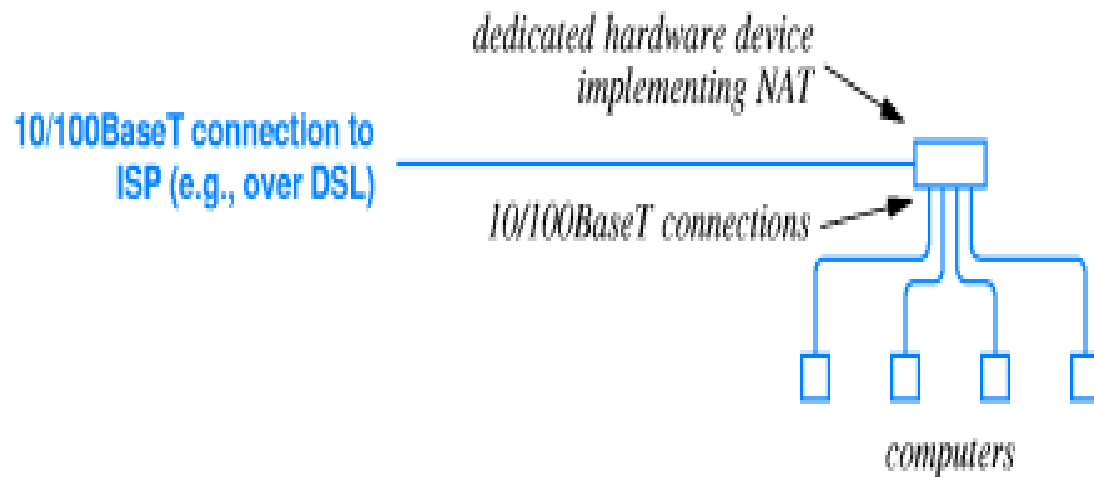
CAT

- ◆ Proposed by Cable TV providers offering Internet services through Cable Modems
- ◆ Includes NAPT plus additional functionality
- ◆ The additional functionality allows the cable operator to:
 - Communicate with the CAT device
 - Inspect Values
 - Control Network Access

NAT at Home

- ◆ NAT is useful at a residence with a Cable Modem or DSL Connectivity
- ◆ Allows the customer to have multiple computers at home without requiring an IP Address for each of them
- ◆ NAT software allows a PC to connect with the Internet and act as a NAT device at the same time

NAT at Home



Summary

- ◆ NAT Translation Table
- ◆ NAPT and TCP Splicing
- ◆ Twice NAT
- ◆ CAT
- ◆ NAT at Home

COMPUTER NETWORKS

CS610

Lecture-39

Hammad Khalid Khan

Review Lecture 38

- ♦ NAT Translation Table
- ♦ NAPT
- ♦ TCP Splicing
- ♦ Twice NAT
- ♦ CAT
- ♦ NAT at Home

Chapter 27

IP ROUTING

Terminology

- ◆ Forwarding
 - Refers to datagram transfer
 - Performed by host or router
 - Uses routing table
- ◆ Routing
 - Refers to propagation of routing information
 - Performed by routers
 - Inserts / changes values in routing table

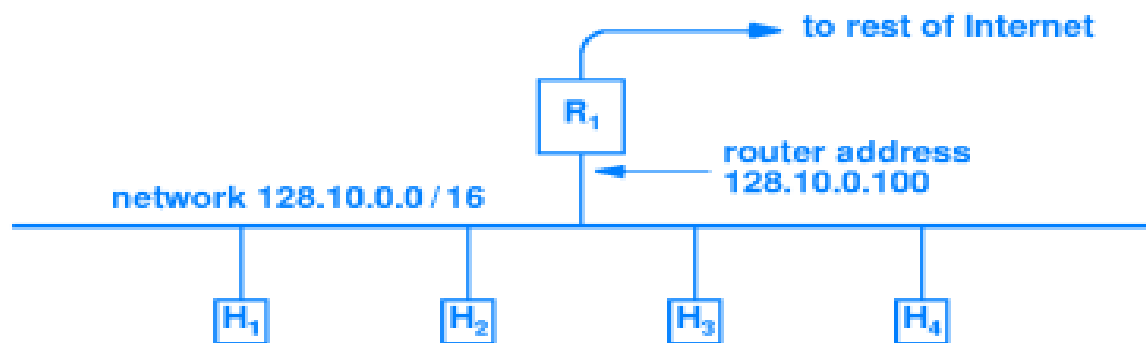
Two Forms of Internet Routing

- ◆ Static Routing
 - Table initialized when system boots
 - No further changes
- ◆ Dynamic Routing
 - Table initialized when system boots
 - Routing software learns routes and updates table
 - Continuous changes possible

Static Routing

- ◆ Used by most Internet hosts
- ◆ Typical routing table has two entries:
 - Local network → direct delivery
 - Default → nearest router

Example of Static Routing



(a)

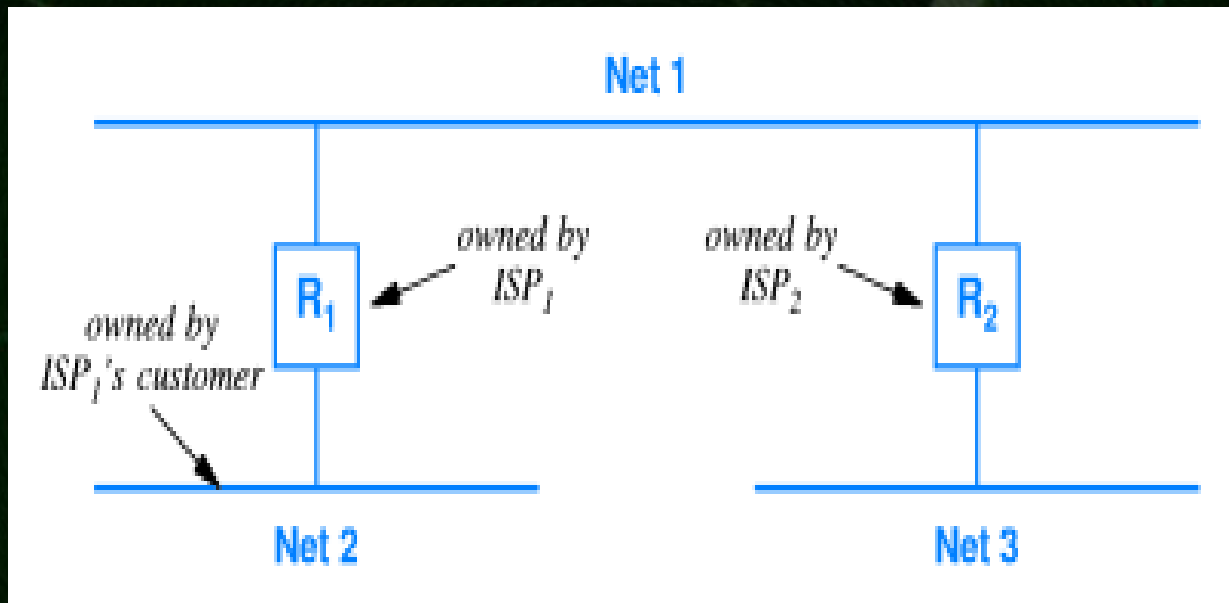
<i>Net</i>	<i>Mask</i>	<i>Next hop</i>
128.10.0.0	255.255.0.0	direct
default	0.0.0.0	128.10.0.100

(b)

Dynamic Routing

- ◆ Used by IP routers
- ◆ Requires special software
- ◆ Each router communicates with neighbors
- ◆ Pass routing information
- ◆ Uses Route Propagation Protocol

Example of Route Propagation



Summary

- ◆ IP Routing (Ch. 27)
- ◆ Static Routing Vs. Dynamic Routing
- ◆ Static Routing in Hosts and a Default Route
- ◆ Dynamic Routing and Routers

COMPUTER NETWORKS

CS610

Lecture-40

Hammad Khalid Khan

Review Lecture 39

- ◆ IP Routing (Ch. 27)
- ◆ Static Routing Vs. Dynamic Routing
- ◆ Static Routing in Hosts and a Default Route
- ◆ Dynamic Routing and Routers

Routing in the Global Internet

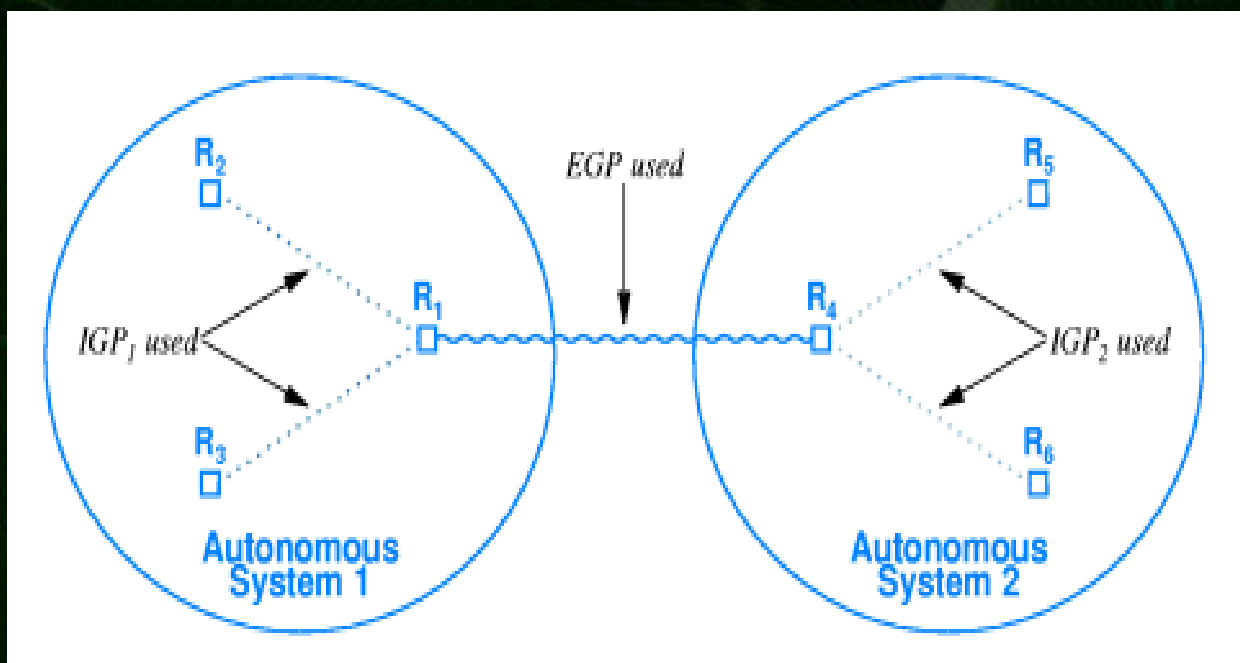
Autonomous System Concept

- ◆ Set of networks and routers under one administrative authority
- ◆ Flexible, soft definition
- ◆ Intuition: a single corporation
- ◆ Needed because no routing protocol can scale to entire Internet
- ◆ Each AS chooses a routing protocol

Classification of Internet Routing Protocols

- ♦ Two broad classes:
 - Interior Gateway Protocols (IGPs)
 - Used among routers within an autonomous system
 - Destinations lie within IGP
 - Exterior Gateway Protocols (EGPs)
 - Used among autonomous systems
 - Destinations lie throughout Internet

Illustration of IGP / EGP Use



Routes and Data Traffic

- ◆ Each ISP is an autonomous system that uses an Exterior Gateway Protocol to advertise its customers' networks to other ISPs
- ◆ After an ISP advertises destination D, datagrams destined for D can begin to arrive

Summary

- ◆ Routing in The Global Internet
- ◆ Autonomous System Concept
- ◆ Classification of Internet Routing Protocols
- ◆ Optimal Routes

COMPUTER NETWORKS

CS610

Lecture-41

Hammad Khalid Khan

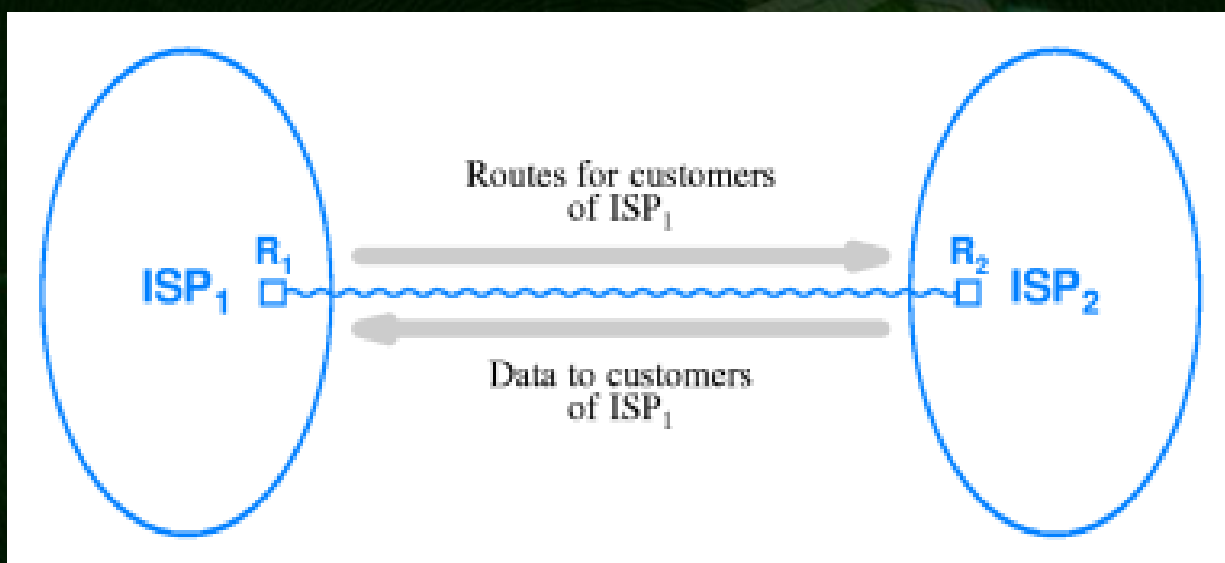
Review Lecture 40

- ♦ Routing in The Global Internet
- ♦ Autonomous System Concepts
- ♦ IGP & EGP
- ♦ Optimal Routes

Routes and Data Traffic

- ◆ Each ISP is an autonomous system that uses an Exterior Gateway Protocol to advertise its customers' networks to other ISPs
- ◆ After an ISP advertises destination D, datagrams destined for D can begin to arrive

Routes and Data Traffic



Internet Routing Protocols

- ◆ Border Gateway Protocol (BGP)
- ◆ Routing Information Protocol (RIP)
- ◆ Open Shortest Path First Protocol (OSPF)

Border Gateway Protocol (BGP)

- ◆ Provides routing among autonomous systems (EGP)
- ◆ Policies to control routes advertised
- ◆ Uses reliable transport (TCP)
- ◆ Gives path of autonomous systems for each destination
- ◆ Currently the EGP of choice in the Internet
- ◆ Current version is four (BGP-4)
- ◆ Facilities for Transit Routing

The Routing Information Protocol (RIP)

- ◆ Routing within an autonomous system (IGP)
- ◆ Hop count metric
- ◆ Unreliable transport (uses UDP)
- ◆ Broadcast or multicast delivery
- ◆ Default Route Propagation
- ◆ Distance vector algorithm
- ◆ Passive version for host

Summary

- ◆ Routes and Data Traffic
- ◆ Border Gateway Protocol
- ◆ Routing Information Protocol

COMPUTER NETWORKS

CS610

Lecture-42

Hammad Khalid Khan

Review Lecture 41

- ◆ Routes and Data Traffic
- ◆ Border Gateway Protocol (BGP)
- ◆ Routing Information Protocol (RIP)

RIP Packet Format

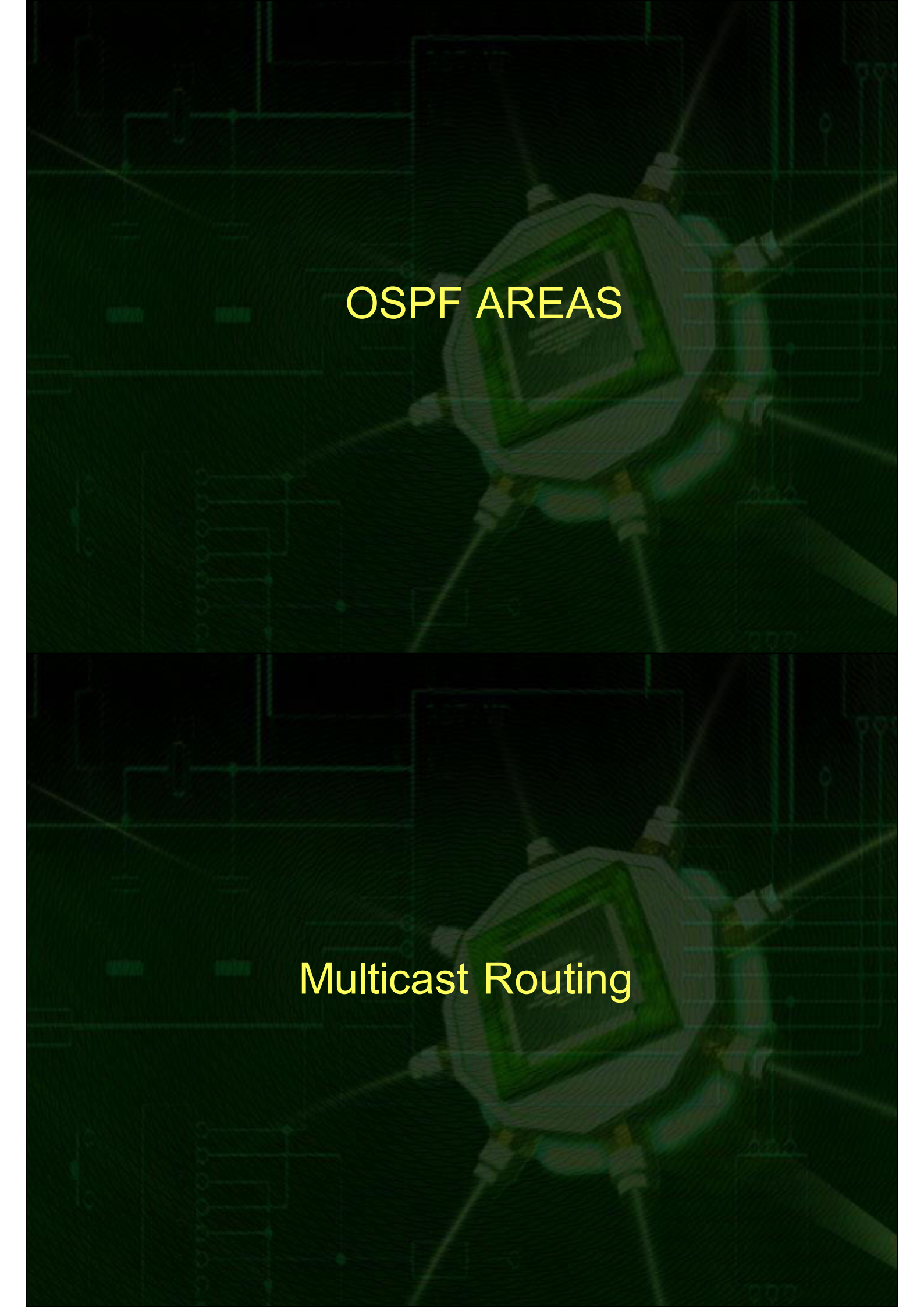
Illustration of RIP Packet Format

0	8	16	24	31
COMMAND (1-5)		VERSION (2)		MUST BE ZERO
FAMILY OF NET 1			ROUTE TAG FOR NET 1	
IP ADDRESS OF NET 1				
SUBNET MASK FOR NET 1				
NEXT HOP FOR NET 1				
DISTANCE TO NET 1				
FAMILY OF NET 2			ROUTE TAG FOR NET 2	
IP ADDRESS OF NET 2				
SUBNET MASK FOR NET 2				
NEXT HOP FOR NET 2				
DISTANCE TO NET 2				
...				

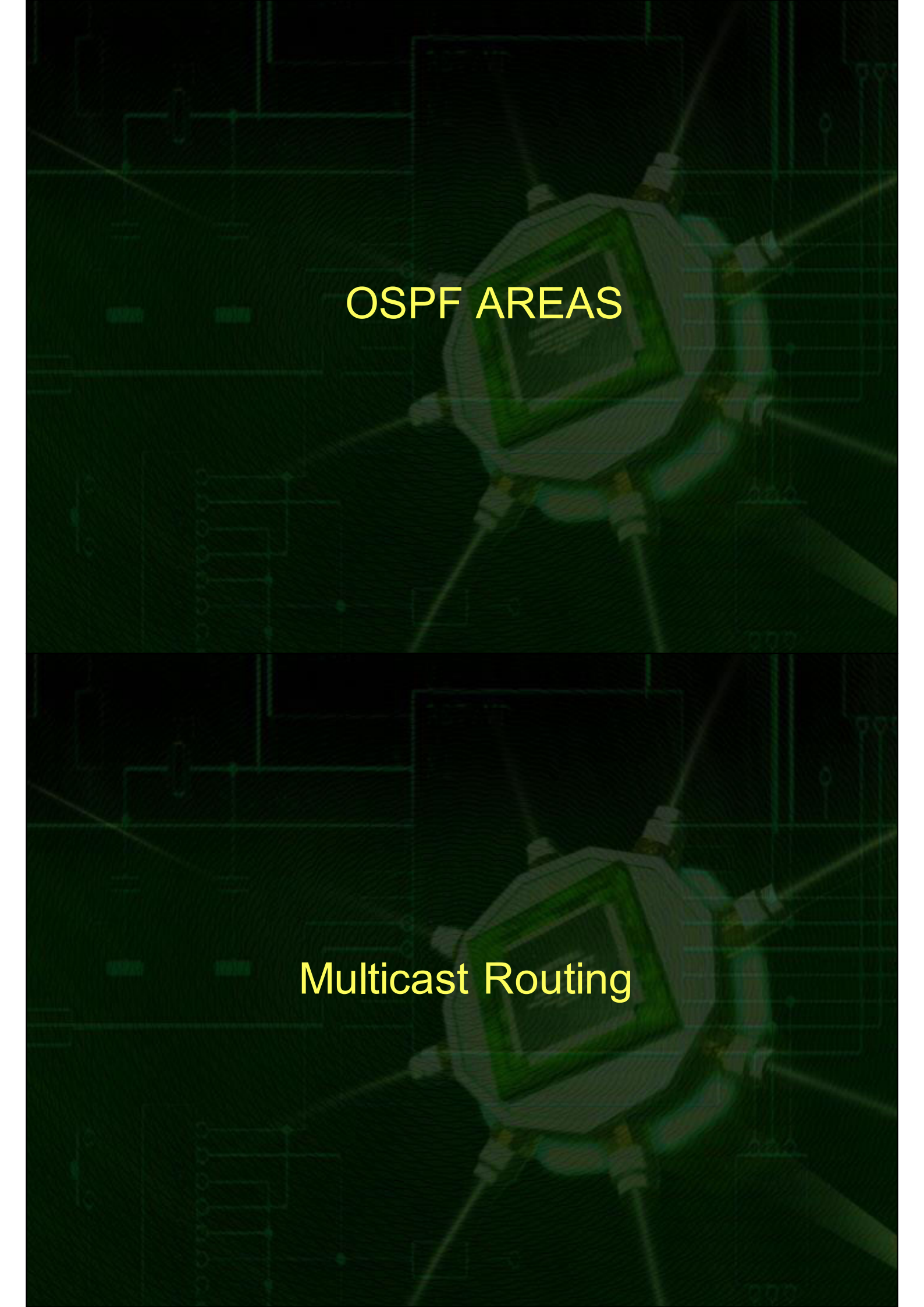
The Open Shortest Path

OSPF Characteristics

- ◆ Routing Within An Autonomous System
- ◆ Full CIDR and Subnet Support
- ◆ Authenticated Message Exchange
- ◆ Imported Routes
- ◆ Link-State Algorithm
- ◆ Support For Multi-access Networks

The background of the slide features a dark green, textured surface. Overlaid on this is a faint, glowing green circuit board pattern. In the center, there is a detailed image of a network switch or router, which is a white, multi-ported device with several cables connected to its ports. The text "OSPF AREAS" is centered over the image in a bright yellow, sans-serif font.

OSPF AREAS

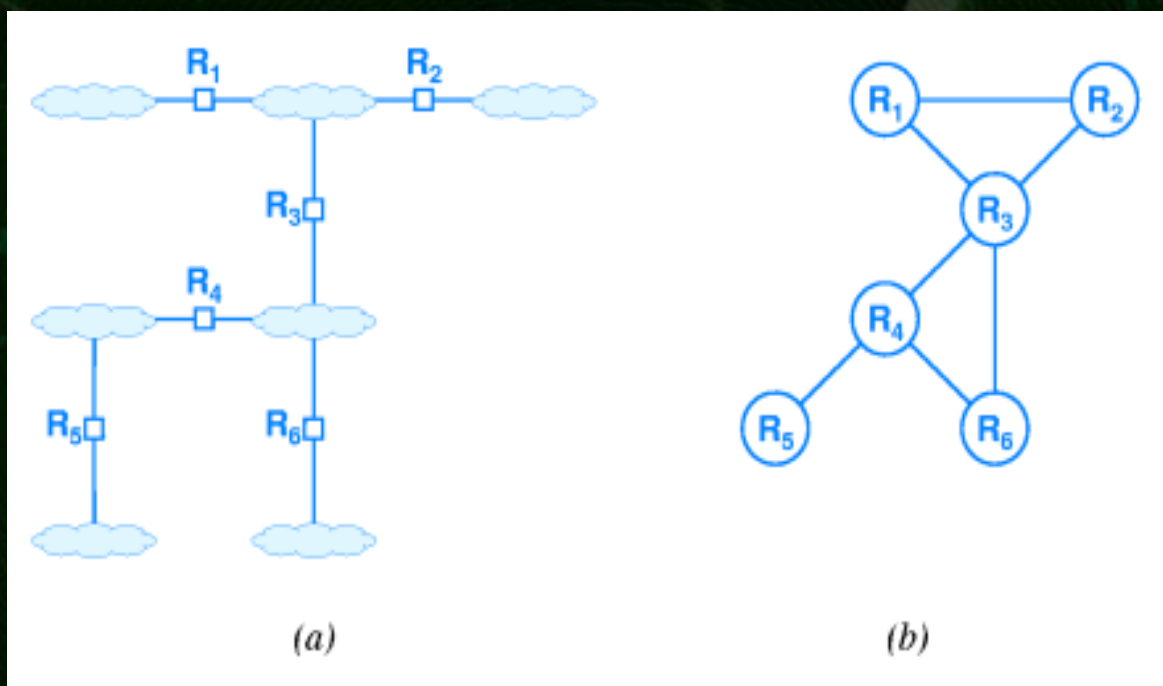
The background of the slide features a dark green, textured surface. Overlaid on this is a faint, glowing green circuit board pattern. In the center, there is a detailed image of a network switch or router, which is a white, multi-ported device with several cables connected to its ports. The text "Multicast Routing" is centered over the image in a bright yellow, sans-serif font.

Multicast Routing

Link-Status in the Internet

- ♦ Router corresponds to node in graph
- ♦ Network corresponds to edge
- ♦ Adjacent pair of routers periodically
 - Test connectivity
 - Broadcast link-status information to area
- ♦ Each router uses link-status messages to compute shortest paths

Illustration of OSPF Graph



OSPF and Scale

- ◆ Because it allows a manager to partition the routers and networks in an autonomous system into multiple areas, OSPF can scale to handle a much larger number of routers than other IGPs

Summary

- ◆ RIP Packet Format
- ◆
- ◆ Open Shortest Path First (OSPF) Protocol
- ◆ OSPF Graph
- ◆ OSPF Areas

COMPUTER NETWORKS

CS610

Lecture-43

Hammad Khalid Khan

Review Lecture 42

- ◆ RIP Packet Format
- ◆ Open Shortest Path First (OSPF) Protocol
- ◆ OSPF Graph
- ◆ OSPF Areas

Internet Multicast Routing

- ◆ Difficult because Internet multicast allows
 - Arbitrary computer to join multicast group at any time
 - Arbitrary member to leave multicast group at any time
 - Arbitrary computer to send message to a group (even if not a member)

IP Multicast Semantics

- ◆ IP Multicast group is anonymous in two ways.
 - Neither a sender nor a receiver knows the identity or the number of group members.
 - Routers and hosts do not know which applications will send a datagram to a group

IGMP

- ◆ A standard protocol exists that allows a host to inform a nearby router whenever the host needs to join or leave a particular multicast group known as Internet Group Multicast Protocol
- ◆ The computer uses IGMP to inform the local router about the last application when it leaves.

Forwarding and Discovery Techniques

- ◆ Routers, not hosts have responsibility for the propagation of multicast routing information.
- ◆ The size and topology of groups may vary e.g.,
 - teleconferencing often creates small groups
 - Web casting can create a large group

Approaches for Datagram Forwarding

- ◆ Flood-And-Prune
- ◆ Configuration-And-Tunneling
- ◆ Core-Based Discovery

Summary

- ◆ Multicast Routing
- ◆ IP Multicast Semantics
- ◆ IGMP
- ◆ Forwarding And Discovery Techniques

COMPUTER NETWORKS

CS610

Lecture-44

Hammad Khalid Khan

Review Lecture 43

- ◆ IP Multicast Semantics
- ◆ IGMP
- ◆ Forwarding and Discovery Techniques
 - Flood-And-Prune
 - Configuration-And-Tunneling
 - Core-Based Discovery

Multicast Protocols (BAR)

- ◆ Several protocols exist
 - Distance Vector Multicast Routing Protocol (DVMRP)
 - Core Based Trees (CBT)
 - Protocol Independent Multicast – Sparse Mode (PIM-SM)
 - Protocol Independent Multicast – Dense Mode (PIM-DM)
 - Multicast extensions to the Open Shortest Path First (MOSPF)
- ◆ None best in all circumstances

Client-Server Interaction

Initial Thought

- ◆ Although an internet system provides basic communication service, the protocol software cannot initiate contact with, or accept contact from a remote computer
- ◆ Instead, two application programs must participate in any communication:
 - one application initiates communication and the other accepts it.

How Two Application Programs Make Contact?

- ◆ One application
 - Actively begins execution first
- ◆ Another application
 - Waits passively at prearranged location
- ◆ Called client-server interaction

Client-Server Paradigm

- ◆ Used by all network applications
- ◆ Passive program called a server
- ◆ Active program called a client

Characteristics of a Client

- ◆ Arbitrary application program
- ◆ Becomes client temporarily
- ◆ Can also perform other computations
- ◆ Invoked directly by the user
- ◆ Runs locally on the user's computer
- ◆ Actively initiates contact with a server
- ◆ Contacts one server at a time

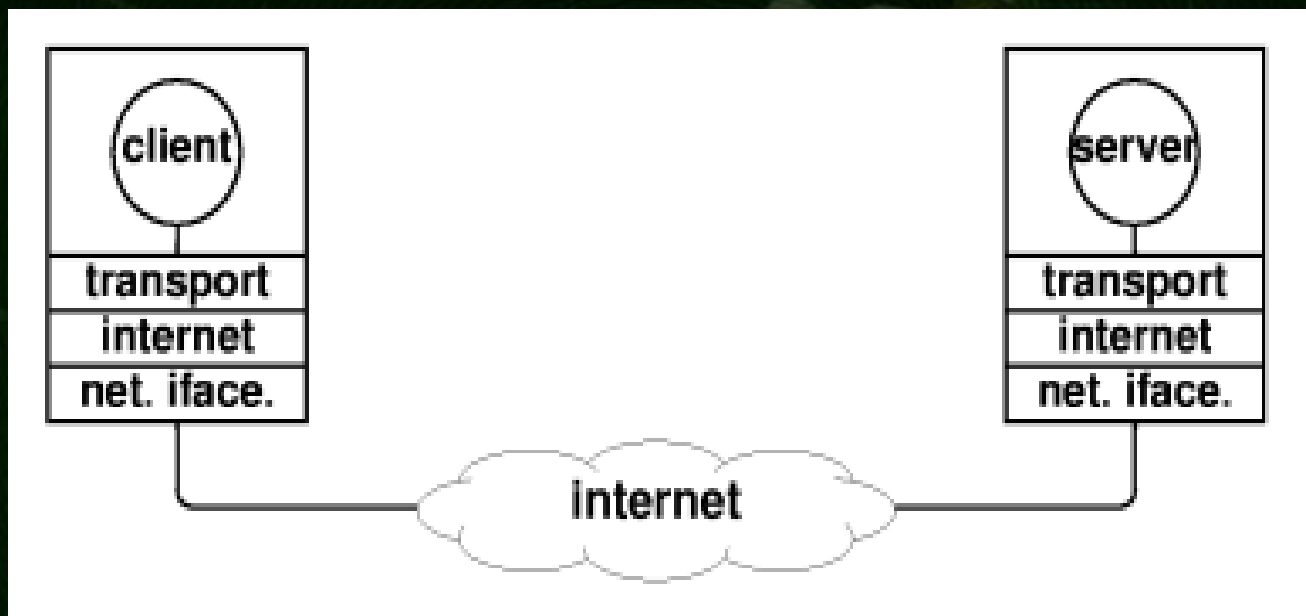
Characteristics of a Server

- ◆ Special-purpose, privileged program
- ◆ Dedicated to providing one service
- ◆ Can handle multiple remote clients simultaneously
- ◆ Invoked automatically when system boots
- ◆ Executes forever
- ◆ Needs powerful computer and operating system

Characteristics of a Server

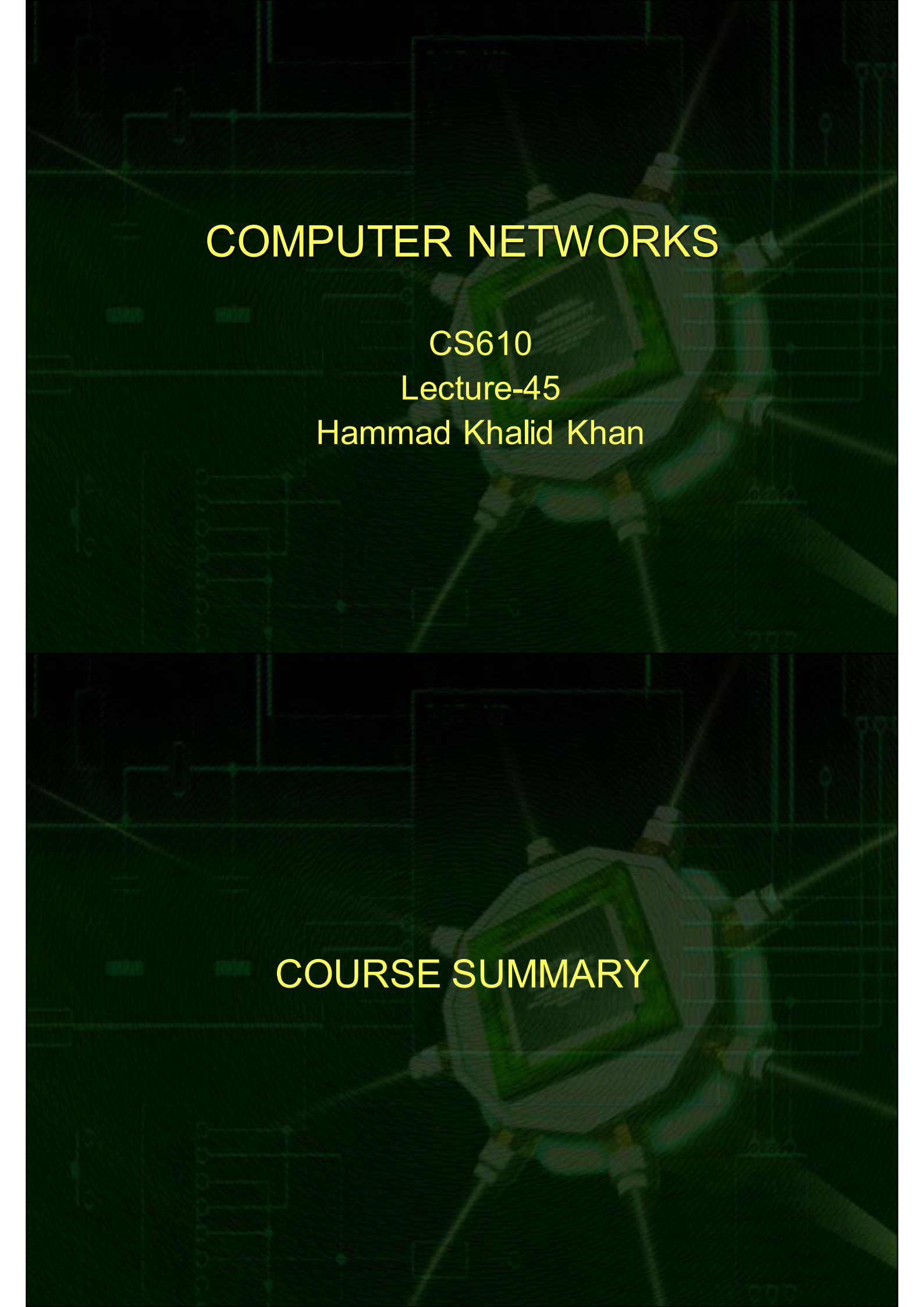
- ◆ Waits passively for client contact
- ◆ Accepts requests from arbitrary clients

Clients, Servers, and Other Protocols



Summary

- ◆ Multicast Protocols
- ◆ Client-Server Interaction
- ◆ Application Software Functionality
- ◆ Characteristics of Clients And Servers
- ◆ Transport Protocol and Client-Server Interaction



COMPUTER NETWORKS

CS610

Lecture-45

Hammad Khalid Khan

COURSE SUMMARY

Course Summary

- ◆ Part I Introduction
- ◆ Part II Data Transmission
- ◆ Part III Packet Transmission
- ◆ Part IV Internetworking

Syllabus for Finals

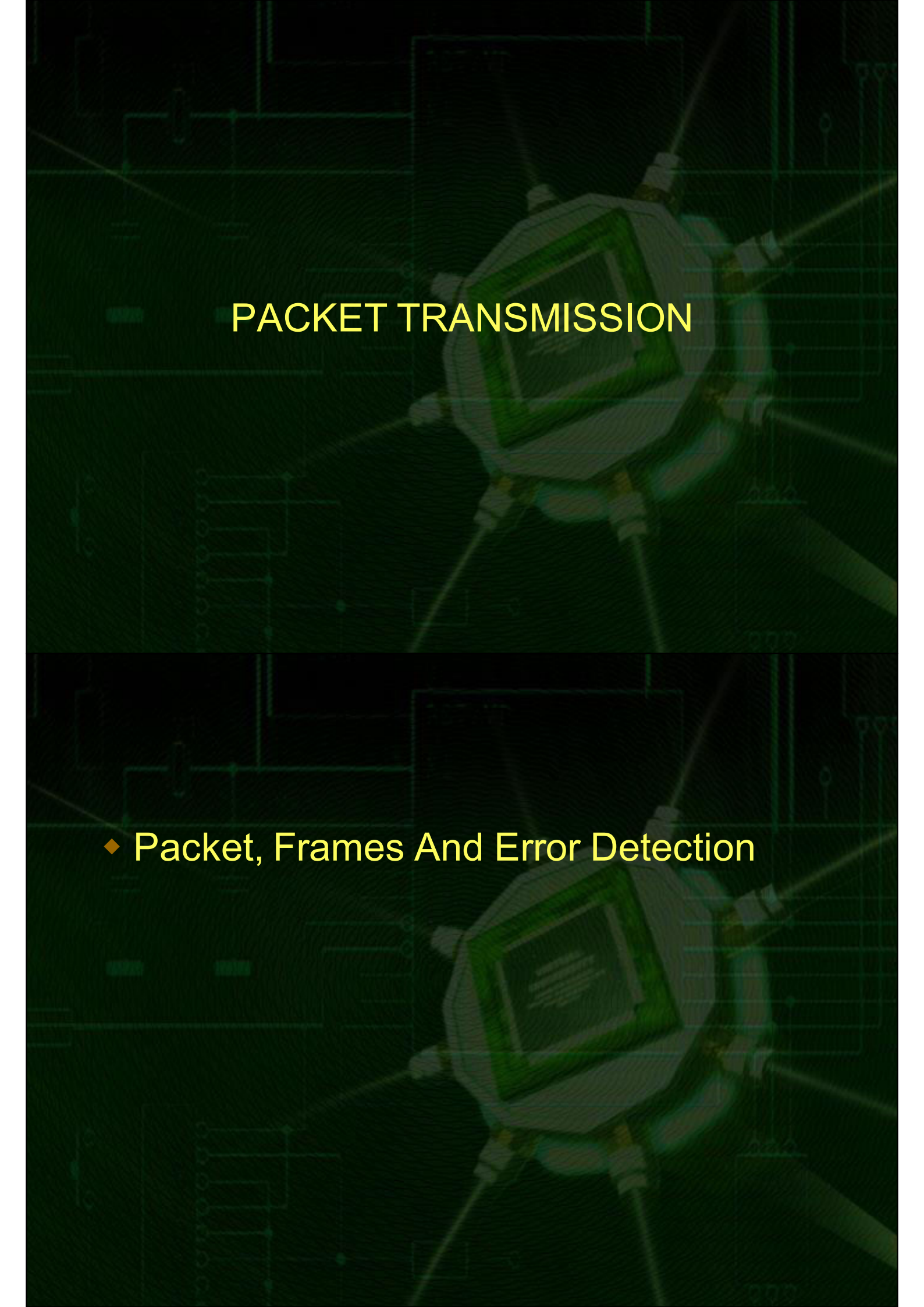
- ◆ Packet Transmission
 - Packets, Frames and Error Detection
 - LAN Technologies and Network Topologies
 - Hardware Addressing and Frame Type Identification
 - LAN Wiring, Physical Topology, And Interface Hardware
 - Extending LANs
 - WAN Technologies and Routing
 - Connection-Oriented Networking and ATM

Syllabus for Finals

- ◆ Packet Transmission (Cont'd)
 - Network Characteristics
- ◆ Internetworking
 - Internetworking Concepts, Architecture and Protocols
 - IP Addressing
 - Binding Protocol Addresses (ARP)

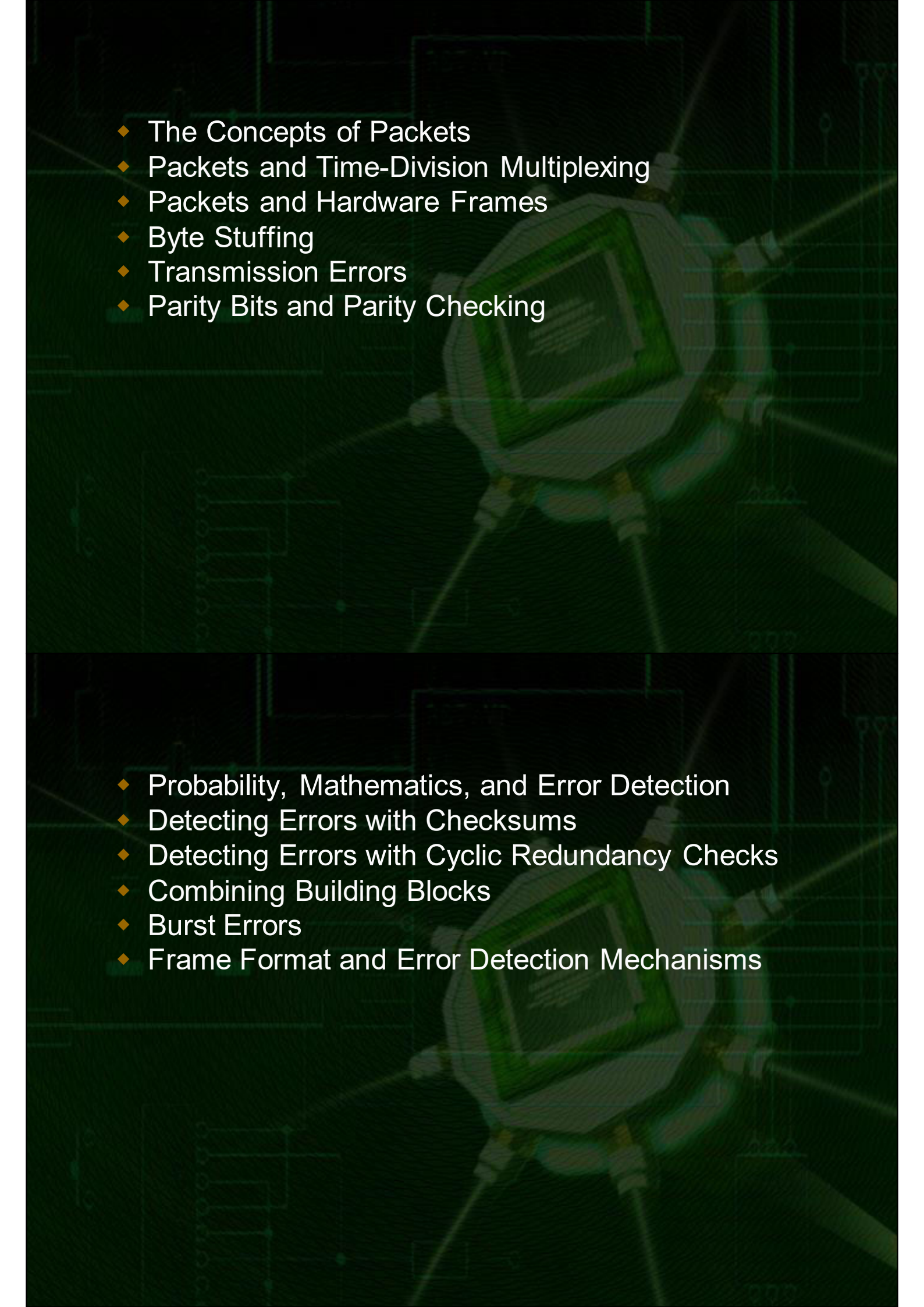
Syllabus for Finals

- ◆ Internetworking
 - IP Datagrams and Datagrams Forwarding
 - IP Encapsulation, Fragmentation and Reassembly
 - UDP: Datagram Transport Service
 - TCP: Reliable Transport Service
 - Internet Routing

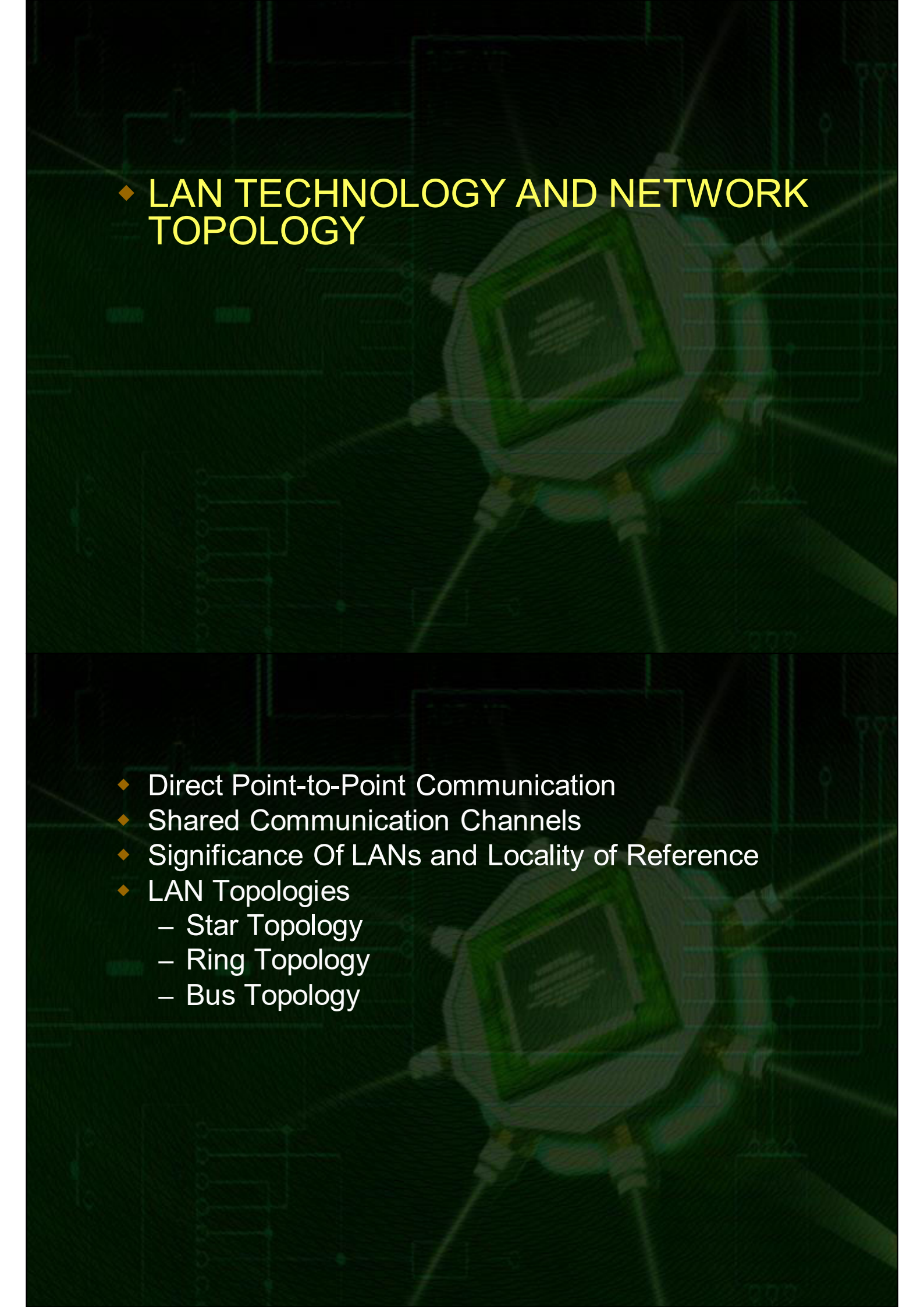
The background of the slide features a dark green, textured image of a satellite in space, with its solar panels and various instruments visible. Overlaid on this is a faint, light green circuit board pattern with various electronic symbols and lines.

PACKET TRANSMISSION

- ◆ Packet, Frames And Error Detection

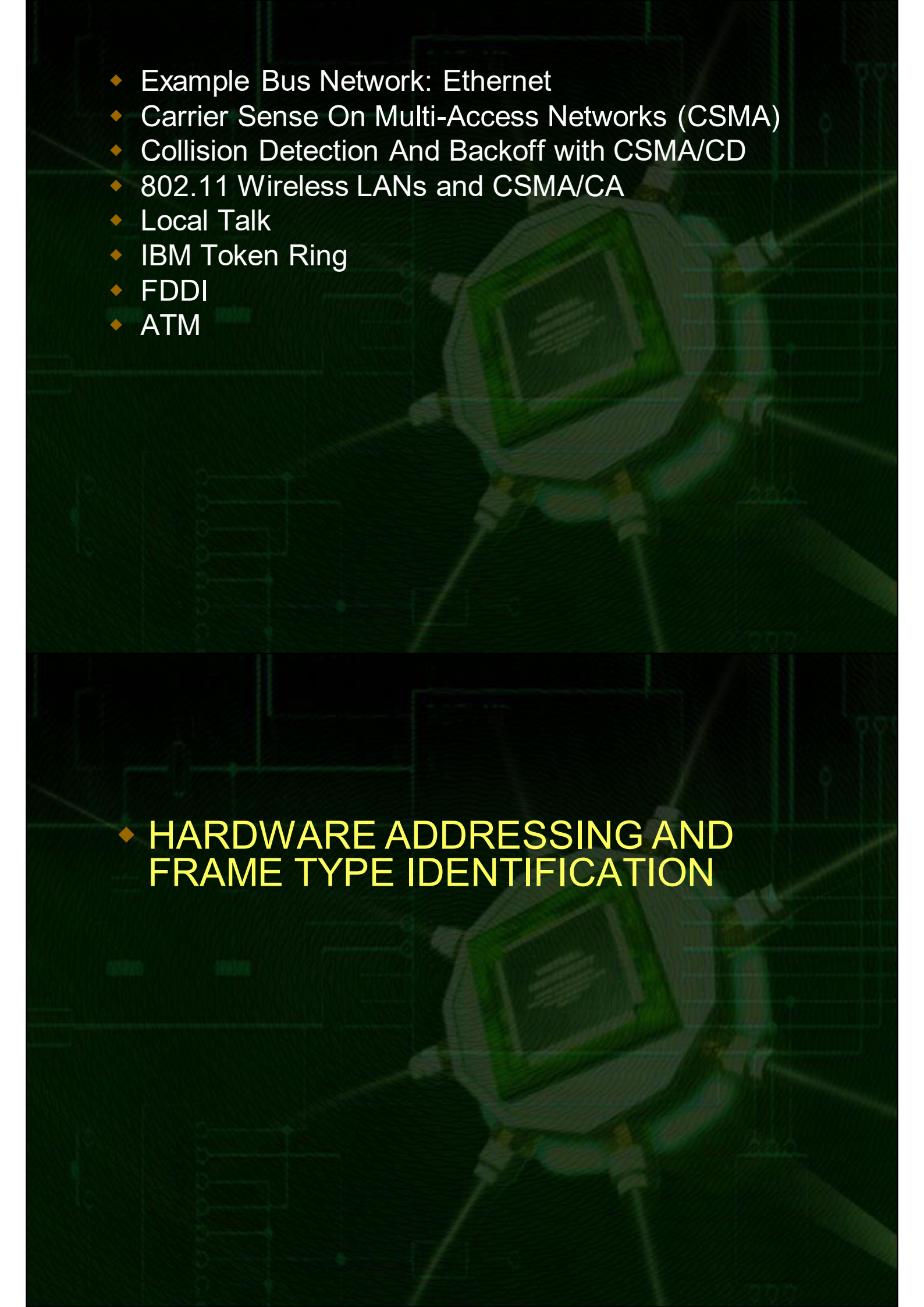
- 
- ◆ The Concepts of Packets
 - ◆ Packets and Time-Division Multiplexing
 - ◆ Packets and Hardware Frames
 - ◆ Byte Stuffing
 - ◆ Transmission Errors
 - ◆ Parity Bits and Parity Checking

- ◆ Probability, Mathematics, and Error Detection
- ◆ Detecting Errors with Checksums
- ◆ Detecting Errors with Cyclic Redundancy Checks
- ◆ Combining Building Blocks
- ◆ Burst Errors
- ◆ Frame Format and Error Detection Mechanisms

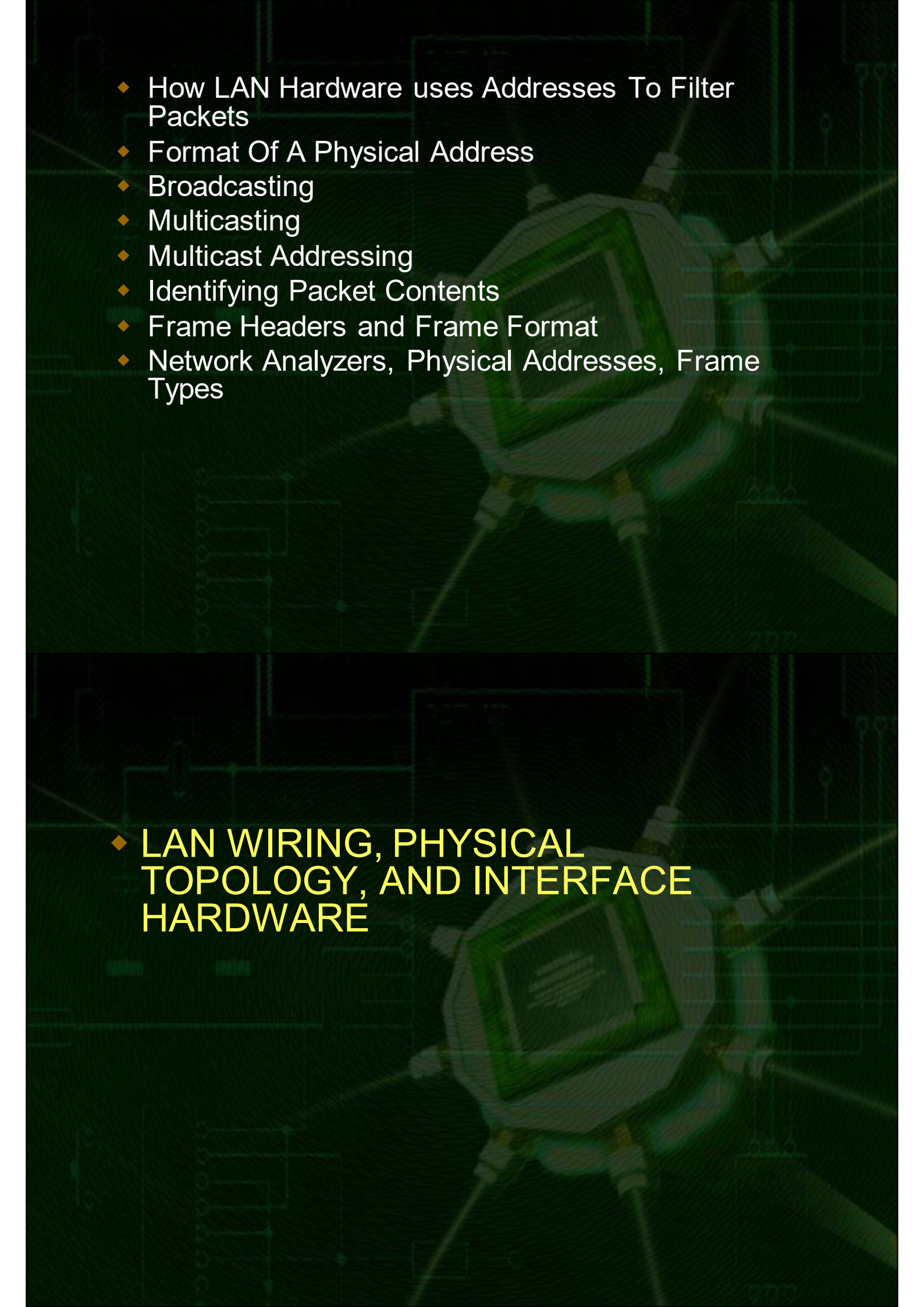


◆ LAN TECHNOLOGY AND NETWORK TOPOLOGY

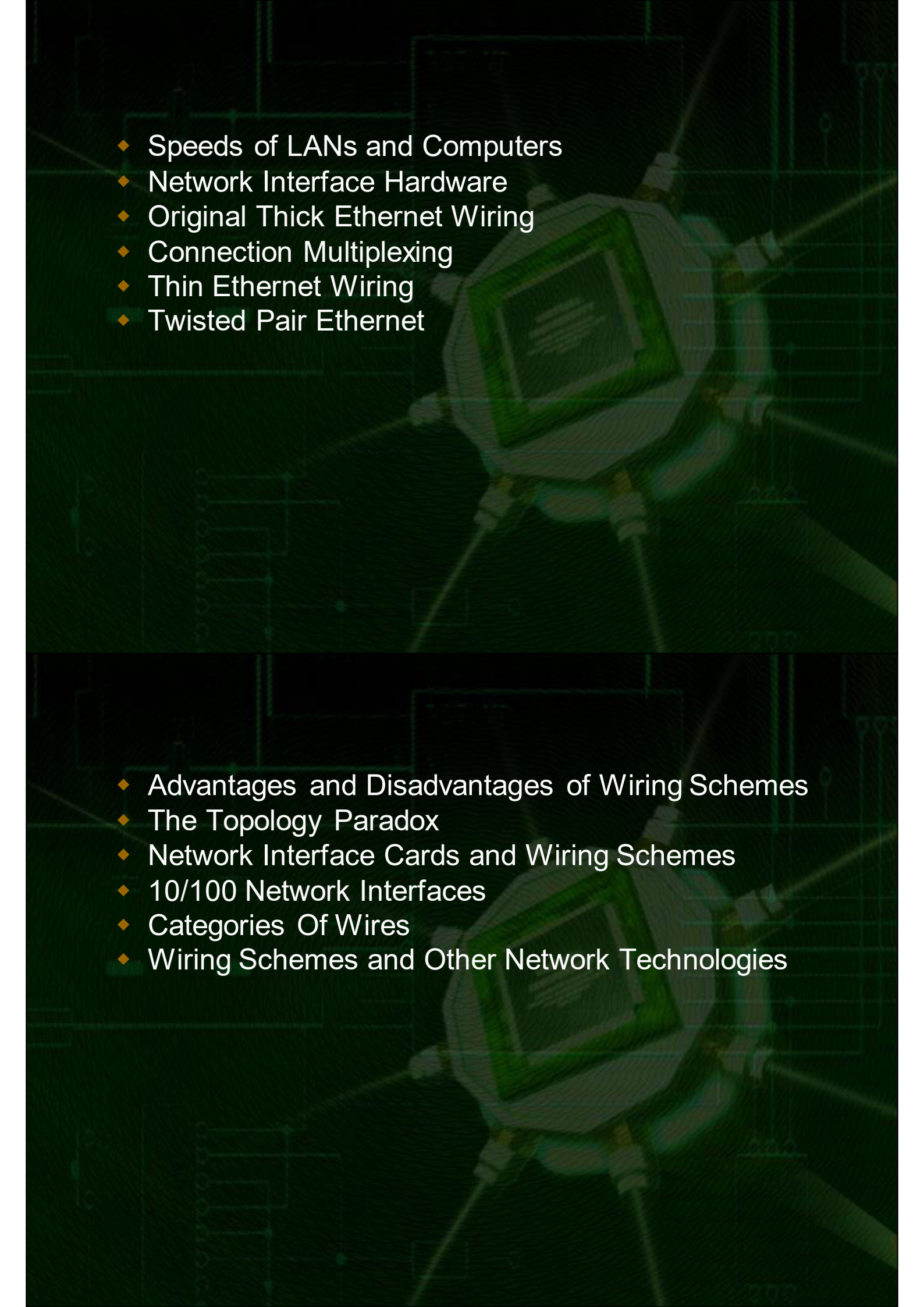
- ◆ Direct Point-to-Point Communication
- ◆ Shared Communication Channels
- ◆ Significance Of LANs and Locality of Reference
- ◆ LAN Topologies
 - Star Topology
 - Ring Topology
 - Bus Topology

- 
- ◆ Example Bus Network: Ethernet
 - ◆ Carrier Sense On Multi-Access Networks (CSMA)
 - ◆ Collision Detection And Backoff with CSMA/CD
 - ◆ 802.11 Wireless LANs and CSMA/CA
 - ◆ Local Talk
 - ◆ IBM Token Ring
 - ◆ FDDI
 - ◆ ATM

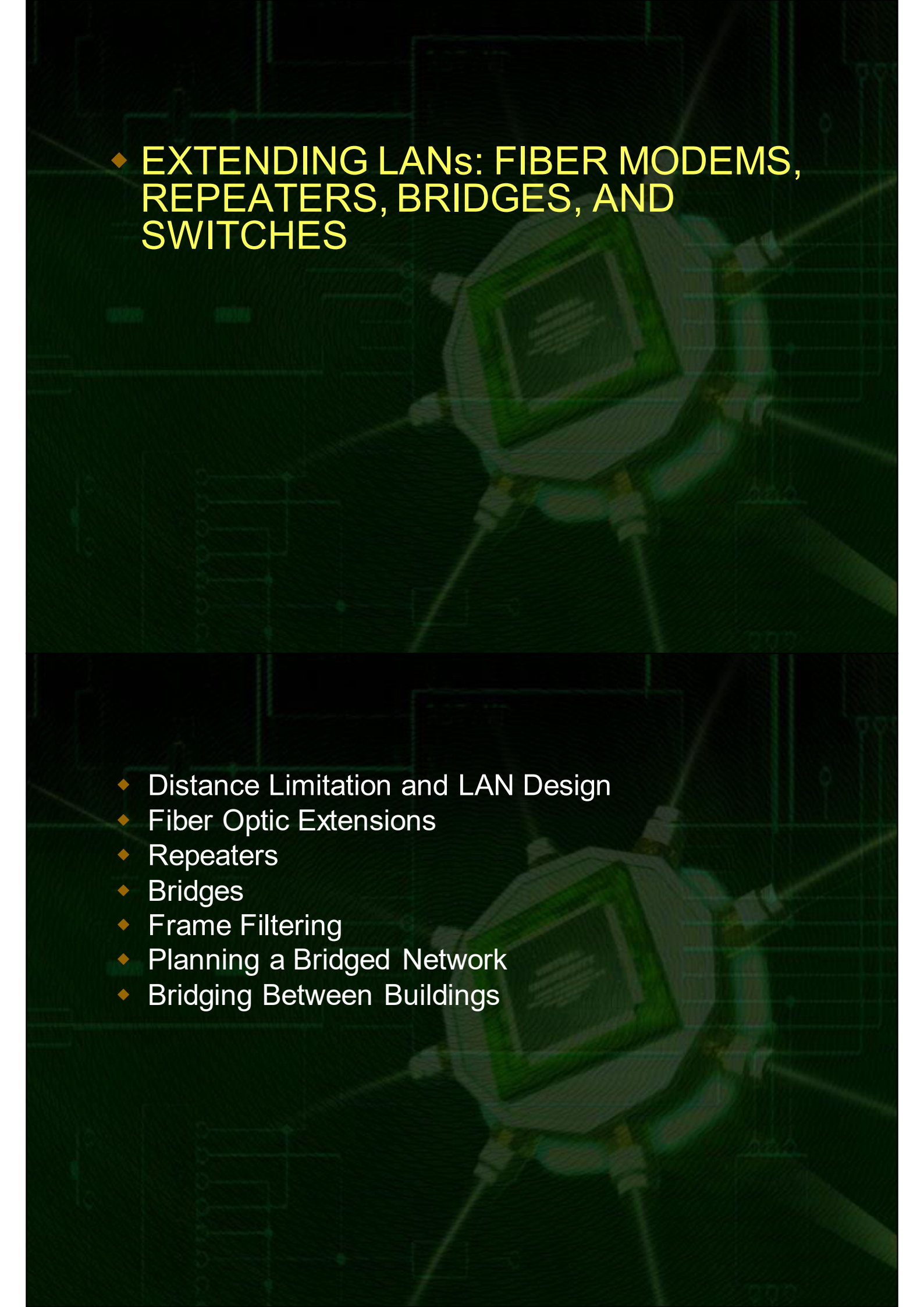
◆ HARDWARE ADDRESSING AND FRAME TYPE IDENTIFICATION

- 
- ◆ How LAN Hardware uses Addresses To Filter Packets
 - ◆ Format Of A Physical Address
 - ◆ Broadcasting
 - ◆ Multicasting
 - ◆ Multicast Addressing
 - ◆ Identifying Packet Contents
 - ◆ Frame Headers and Frame Format
 - ◆ Network Analyzers, Physical Addresses, Frame Types

◆ LAN WIRING, PHYSICAL TOPOLOGY, AND INTERFACE HARDWARE

- 
- ◆ Speeds of LANs and Computers
 - ◆ Network Interface Hardware
 - ◆ Original Thick Ethernet Wiring
 - ◆ Connection Multiplexing
 - ◆ Thin Ethernet Wiring
 - ◆ Twisted Pair Ethernet

- ◆ Advantages and Disadvantages of Wiring Schemes
- ◆ The Topology Paradox
- ◆ Network Interface Cards and Wiring Schemes
- ◆ 10/100 Network Interfaces
- ◆ Categories Of Wires
- ◆ Wiring Schemes and Other Network Technologies

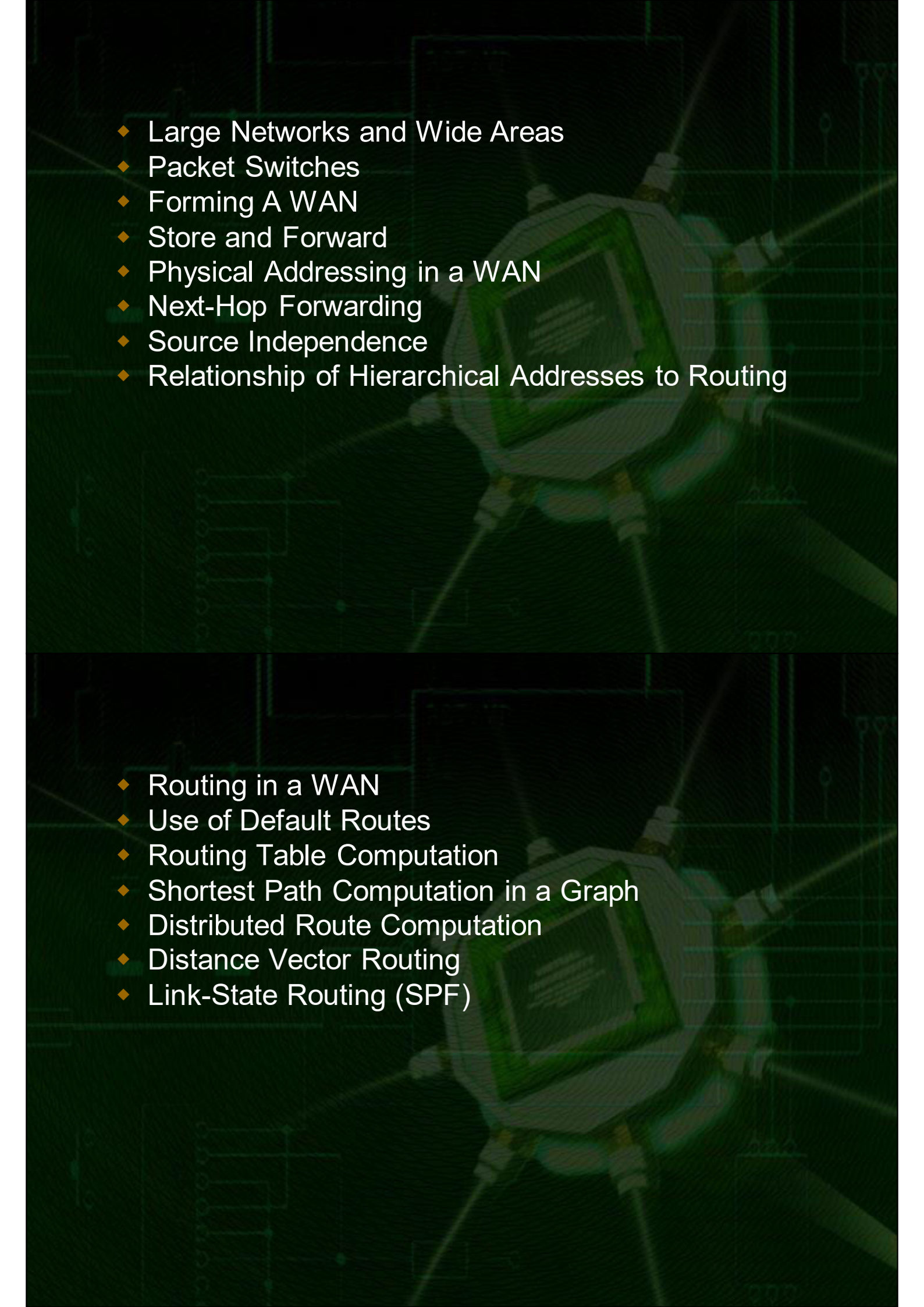


◆ EXTENDING LANs: FIBER MODEMS, REPEATERS, BRIDGES, AND SWITCHES

- ◆ Distance Limitation and LAN Design
- ◆ Fiber Optic Extensions
- ◆ Repeaters
- ◆ Bridges
- ◆ Frame Filtering
- ◆ Planning a Bridged Network
- ◆ Bridging Between Buildings

- 
- ◆ Bridging across Longer Distances
 - ◆ A Cycle Of Bridges
 - ◆ Distributed Spanning Tree
 - ◆ Switching
 - ◆ Combining Switches and Hubs
 - ◆ Bridging and Switching with Other Technologies

- 
- ◆ **WAN TECHNOLOGIES AND ROUTING**

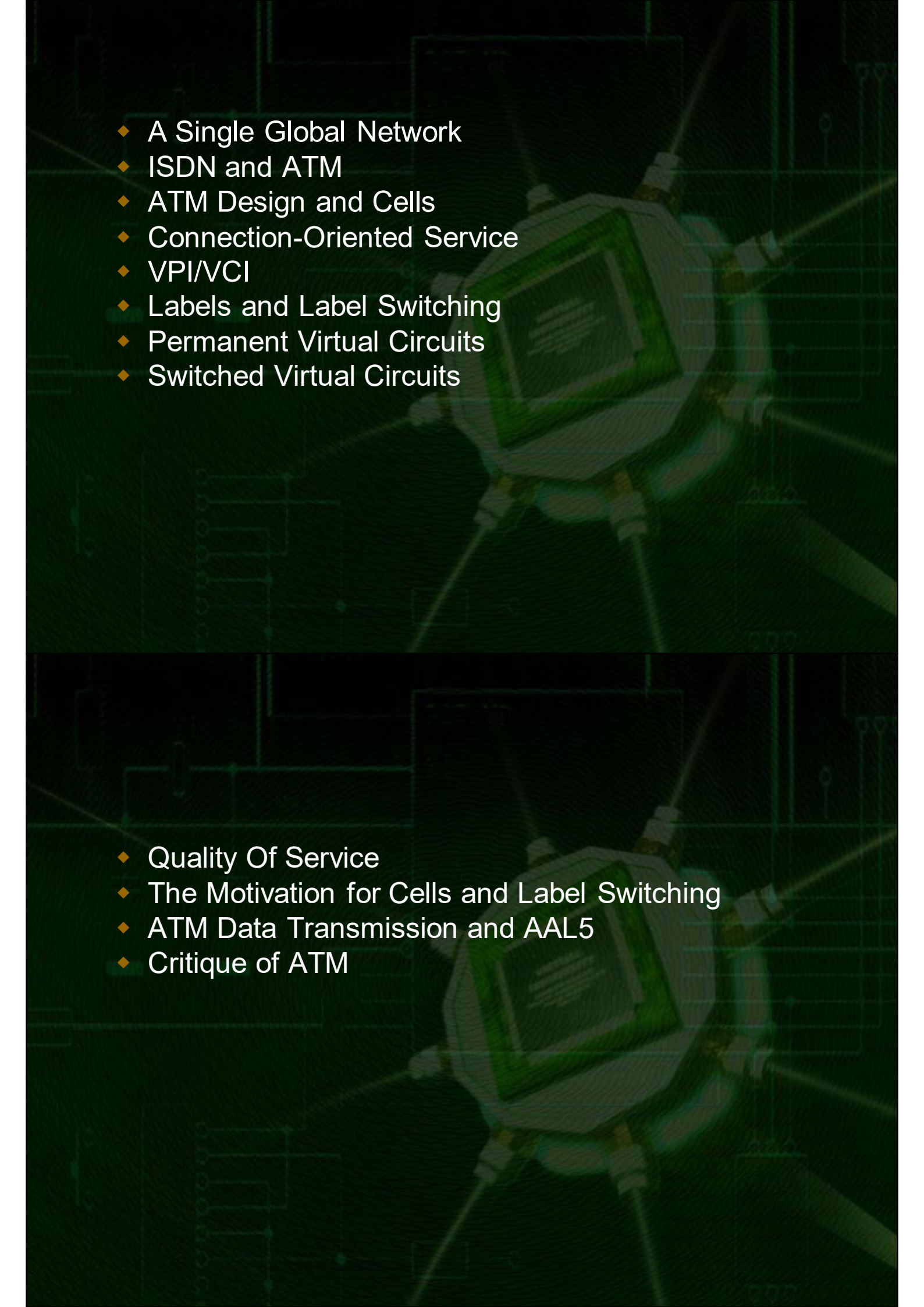
- 
- ◆ Large Networks and Wide Areas
 - ◆ Packet Switches
 - ◆ Forming A WAN
 - ◆ Store and Forward
 - ◆ Physical Addressing in a WAN
 - ◆ Next-Hop Forwarding
 - ◆ Source Independence
 - ◆ Relationship of Hierarchical Addresses to Routing

- ◆ Routing in a WAN
- ◆ Use of Default Routes
- ◆ Routing Table Computation
- ◆ Shortest Path Computation in a Graph
- ◆ Distributed Route Computation
- ◆ Distance Vector Routing
- ◆ Link-State Routing (SPF)

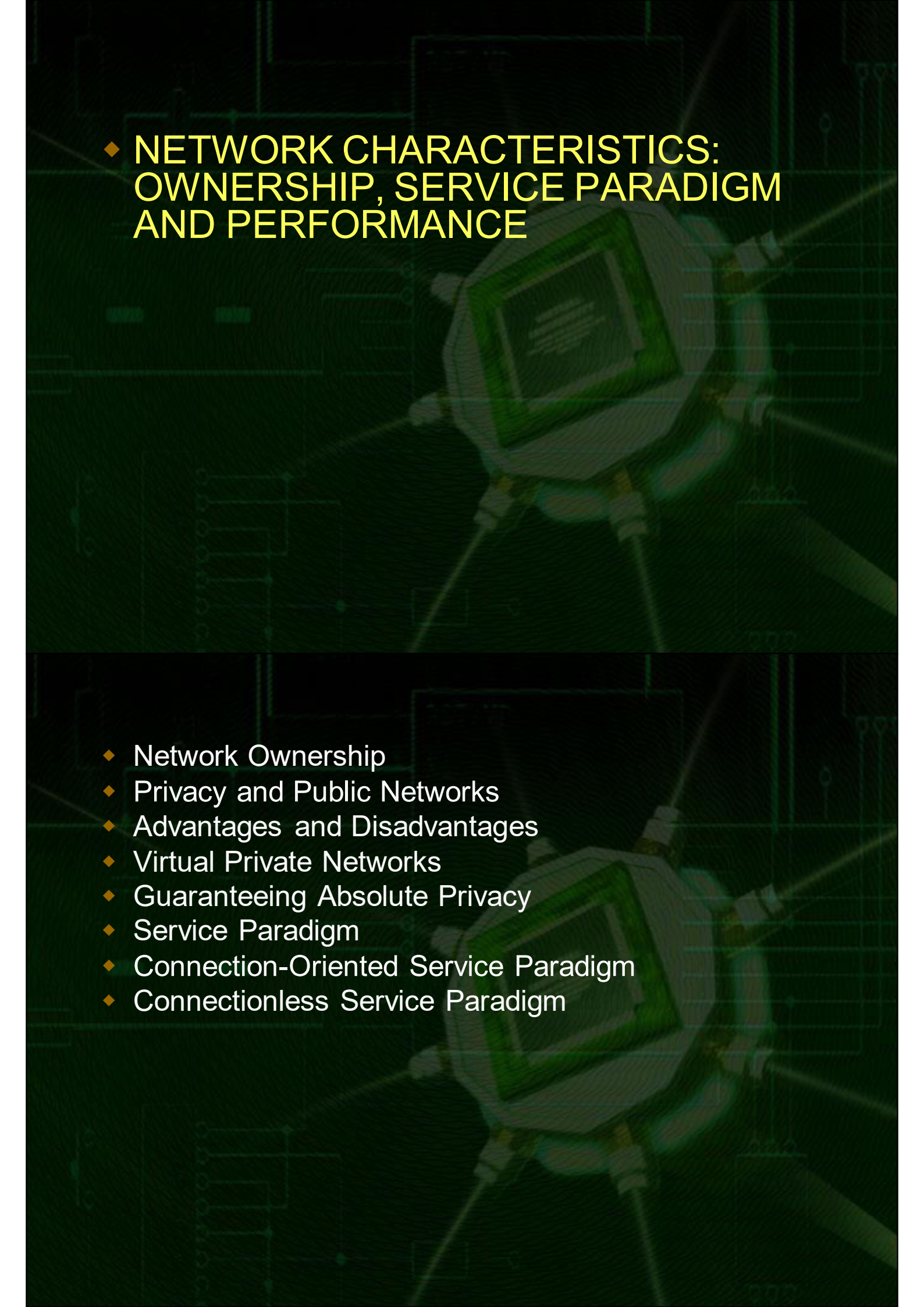
- ◆ Example WAN Technologies

- ARPANET
- FRAME RELAY
- SMDS
- ATM

- ◆ CONNECTION-ORIENTED NETWORKING AND ATM

- 
- ◆ A Single Global Network
 - ◆ ISDN and ATM
 - ◆ ATM Design and Cells
 - ◆ Connection-Oriented Service
 - ◆ VPI/VCI
 - ◆ Labels and Label Switching
 - ◆ Permanent Virtual Circuits
 - ◆ Switched Virtual Circuits

- ◆ Quality Of Service
- ◆ The Motivation for Cells and Label Switching
- ◆ ATM Data Transmission and AAL5
- ◆ Critique of ATM



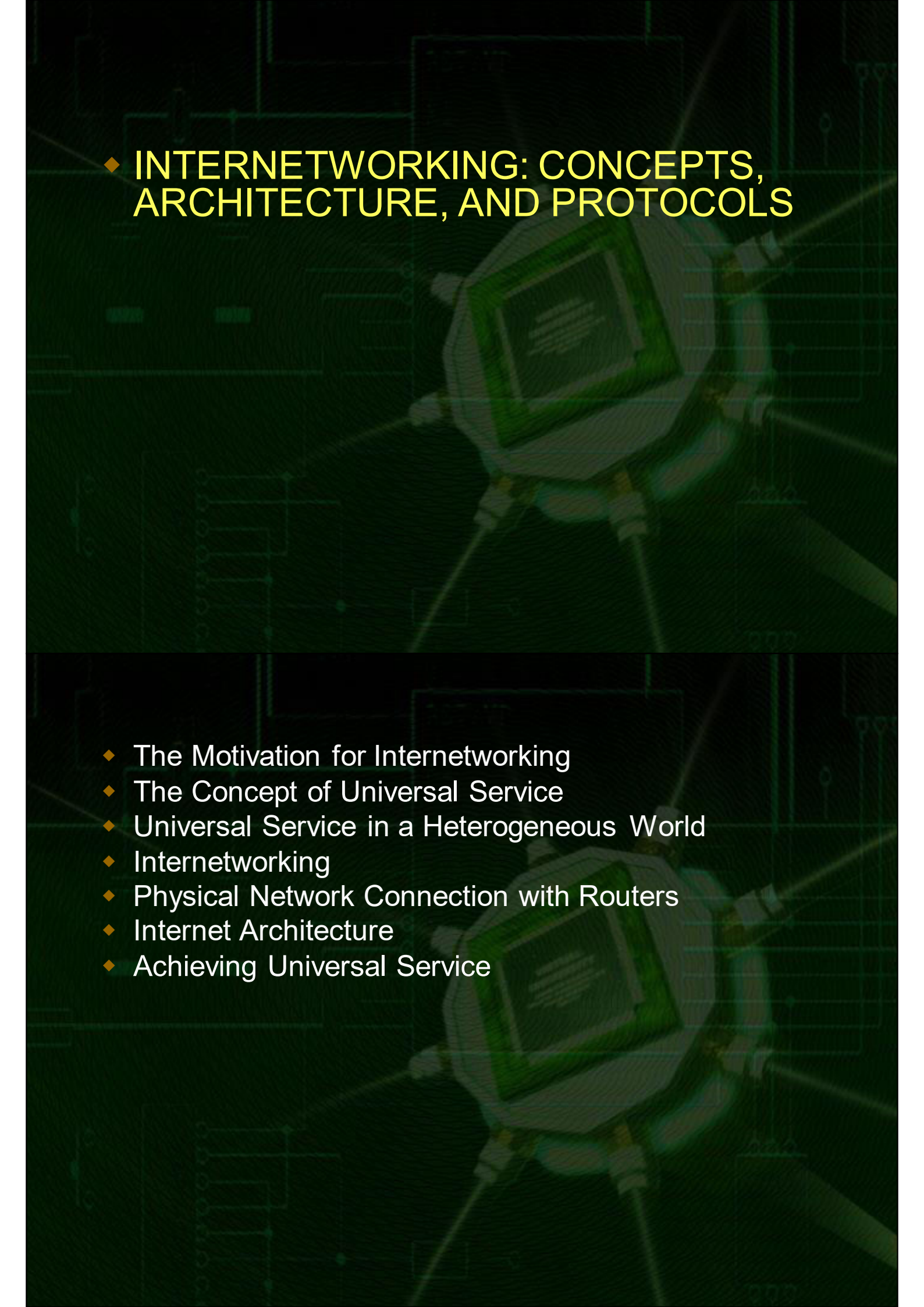
◆ NETWORK CHARACTERISTICS: OWNERSHIP, SERVICE PARADIGM AND PERFORMANCE

- ◆ Network Ownership
- ◆ Privacy and Public Networks
- ◆ Advantages and Disadvantages
- ◆ Virtual Private Networks
- ◆ Guaranteeing Absolute Privacy
- ◆ Service Paradigm
- ◆ Connection-Oriented Service Paradigm
- ◆ Connectionless Service Paradigm

- ◆ Interior and Exterior Service Paradigm
- ◆ Comparison of Service Paradigm
- ◆ Addresses of Connection Identifiers
- ◆ Network Performance Characteristics
 - Delay
 - Throughput
- ◆ Jitter

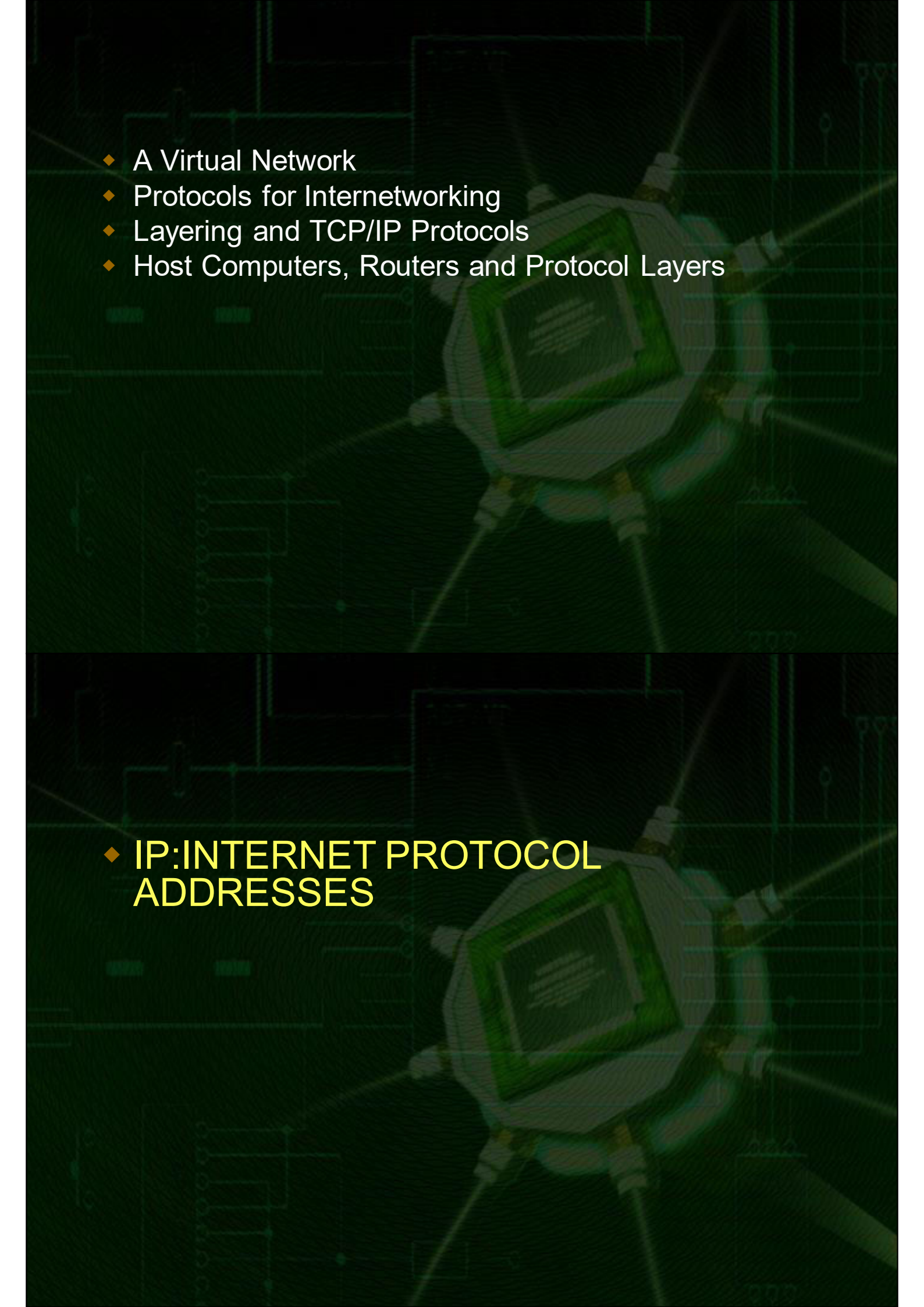
PART III

- ◆ INTERNETWORKING

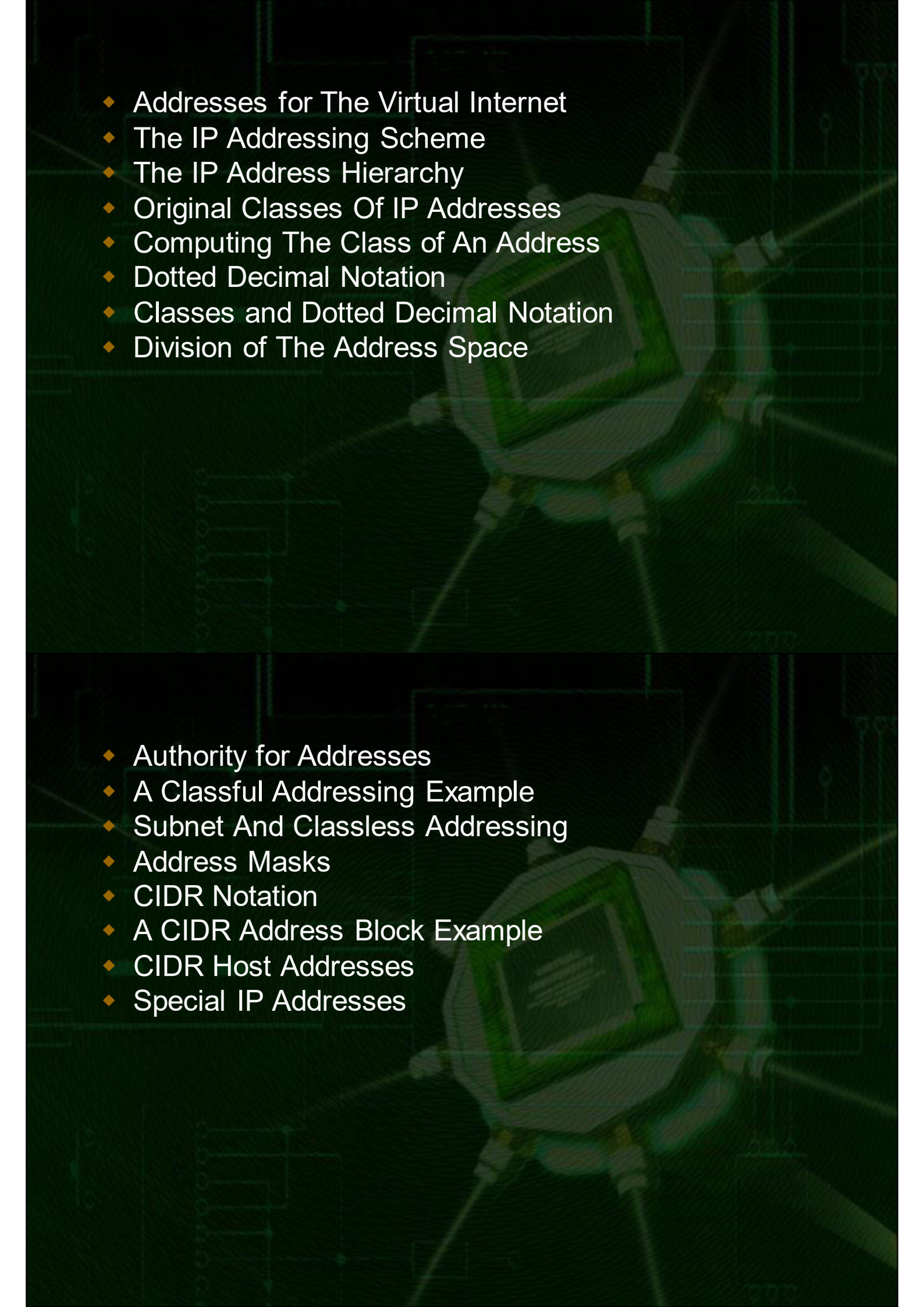
The background of the slide is a dark green, textured image. It features a faint, glowing circuit board pattern. In the center, there is a stylized, glowing green computer monitor or screen, which appears to be part of a larger electronic device. The overall aesthetic is technical and digital.

◆ INTERNETWORKING: CONCEPTS, ARCHITECTURE, AND PROTOCOLS

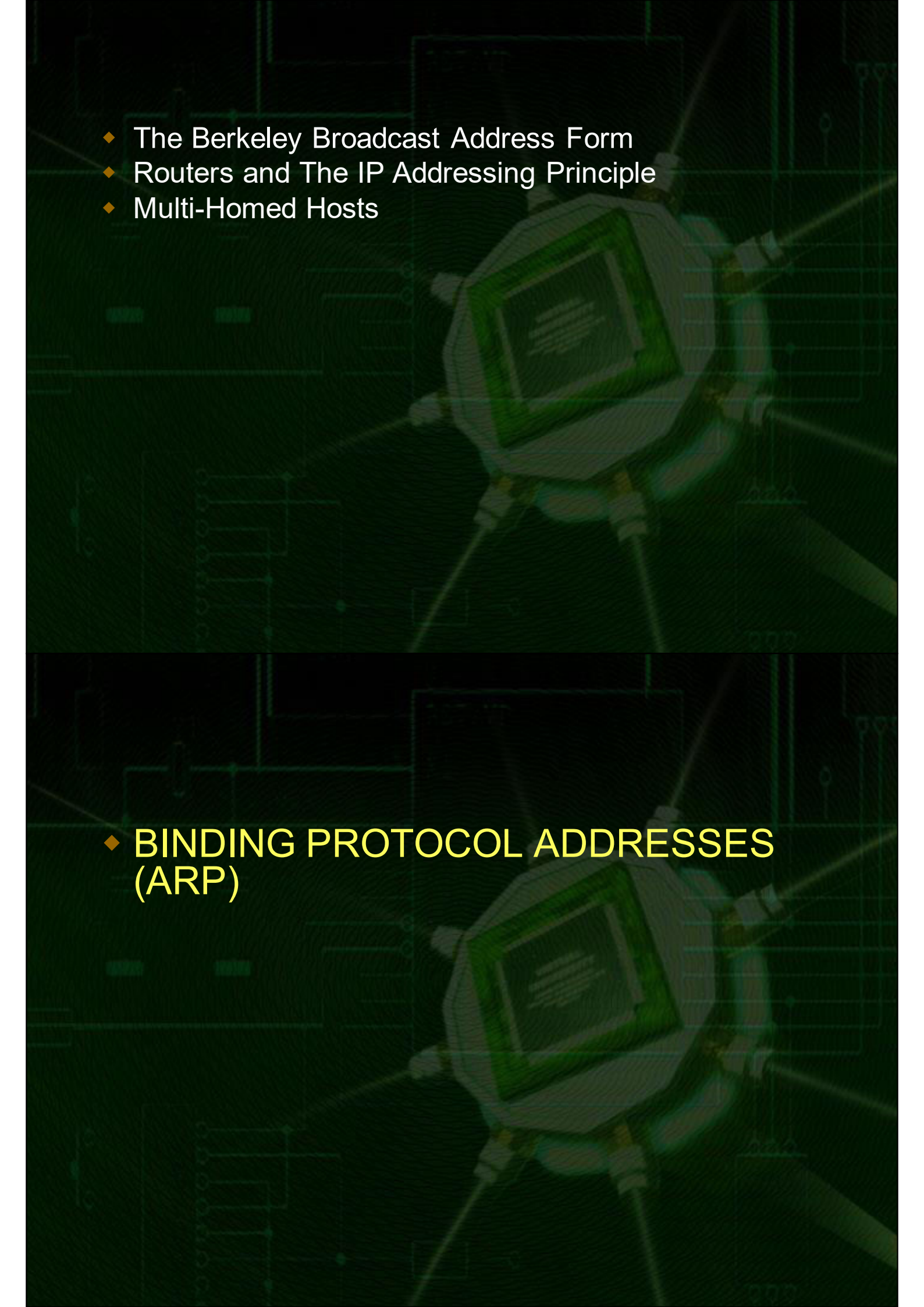
- ◆ The Motivation for Internetworking
- ◆ The Concept of Universal Service
- ◆ Universal Service in a Heterogeneous World
- ◆ Internetworking
- ◆ Physical Network Connection with Routers
- ◆ Internet Architecture
- ◆ Achieving Universal Service

- 
- ◆ A Virtual Network
 - ◆ Protocols for Internetworking
 - ◆ Layering and TCP/IP Protocols
 - ◆ Host Computers, Routers and Protocol Layers

- ◆ **IP:INTERNET PROTOCOL
ADDRESSES**

- 
- ◆ Addresses for The Virtual Internet
 - ◆ The IP Addressing Scheme
 - ◆ The IP Address Hierarchy
 - ◆ Original Classes Of IP Addresses
 - ◆ Computing The Class of An Address
 - ◆ Dotted Decimal Notation
 - ◆ Classes and Dotted Decimal Notation
 - ◆ Division of The Address Space

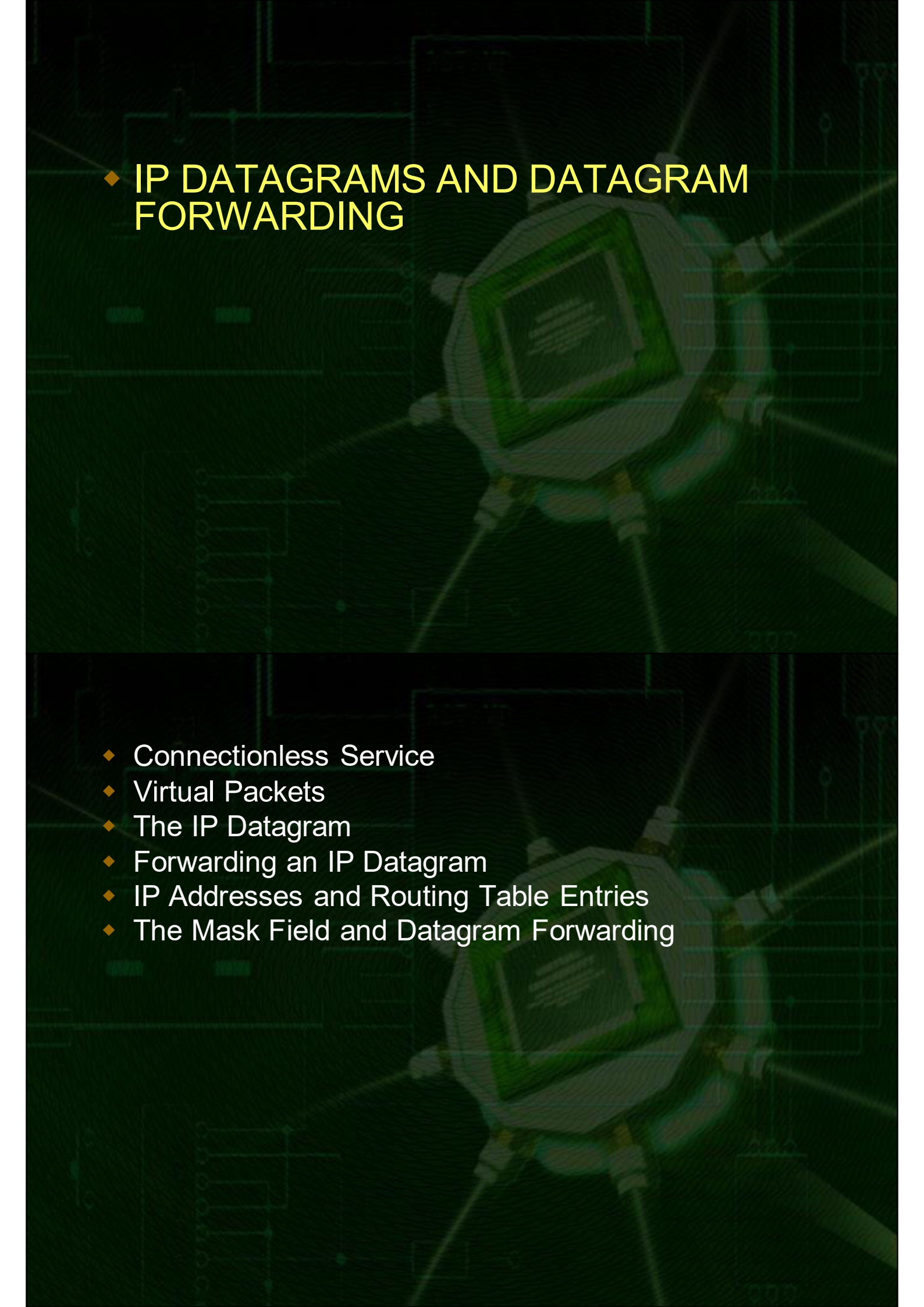
- ◆ Authority for Addresses
- ◆ A Classful Addressing Example
- ◆ Subnet And Classless Addressing
- ◆ Address Masks
- ◆ CIDR Notation
- ◆ A CIDR Address Block Example
- ◆ CIDR Host Addresses
- ◆ Special IP Addresses

- 
- ◆ The Berkeley Broadcast Address Form
 - ◆ Routers and The IP Addressing Principle
 - ◆ Multi-Homed Hosts

- ◆ **BINDING PROTOCOL ADDRESSES (ARP)**

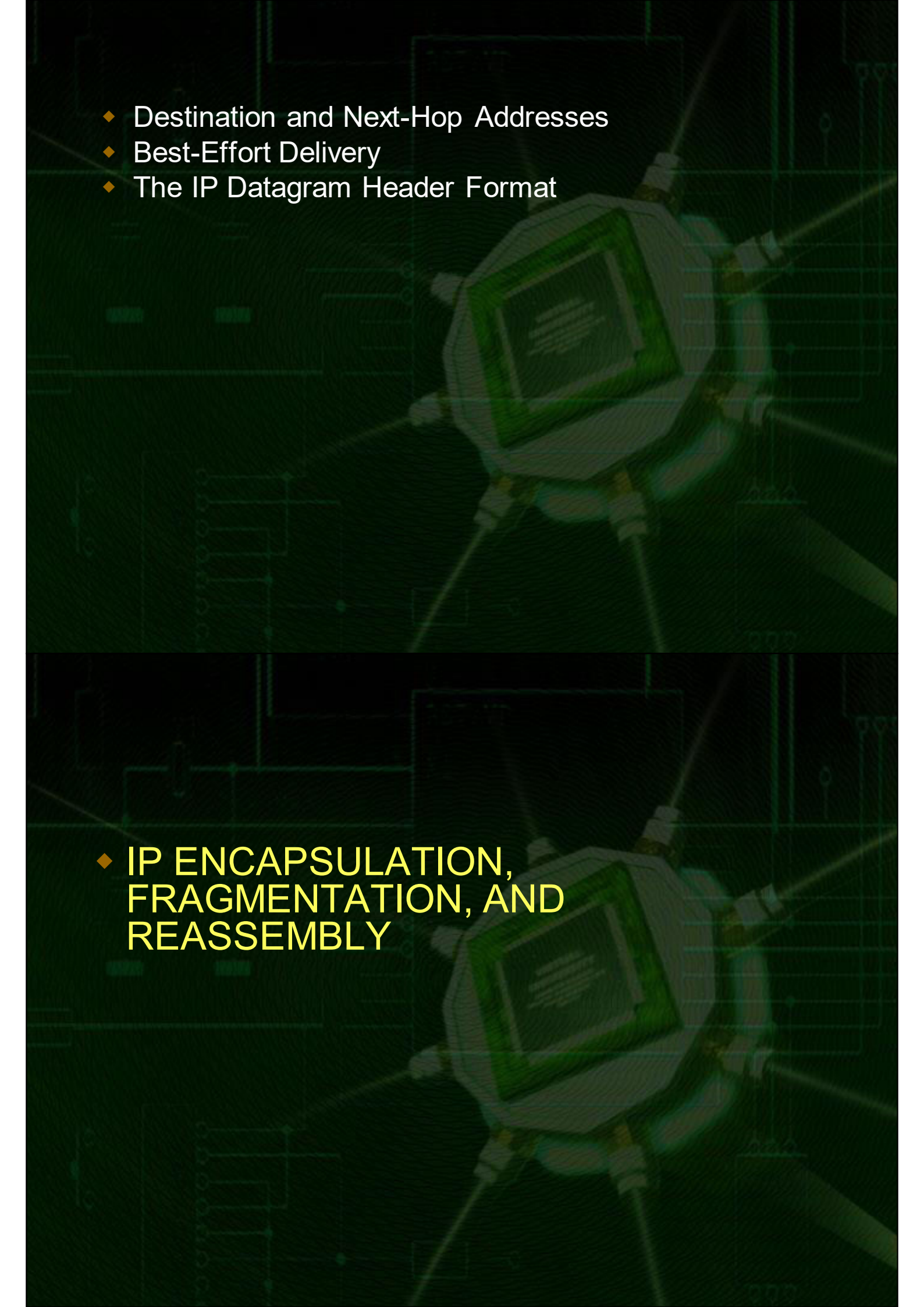
- 
- ◆ Protocol Addresses and Packet Delivery
 - ◆ Address Resolution
 - ◆ Address Resolution Techniques
 - ◆ Address Resolution with Table Lookup
 - ◆ Address Resolution with Closed-Form Computation
 - ◆ Address Resolution With Message Exchange

- ◆ Address Resolution Protocol
- ◆ ARP Message Delivery
- ◆ ARP Message Format
- ◆ Sending An ARP Message
- ◆ Identifying ARP Frames
- ◆ Caching ARP Responses
- ◆ Processing An Incoming ARP Message
- ◆ Layering, Address Resolution, Protocol Addresses



◆ IP DATAGRAMS AND DATAGRAM FORWARDING

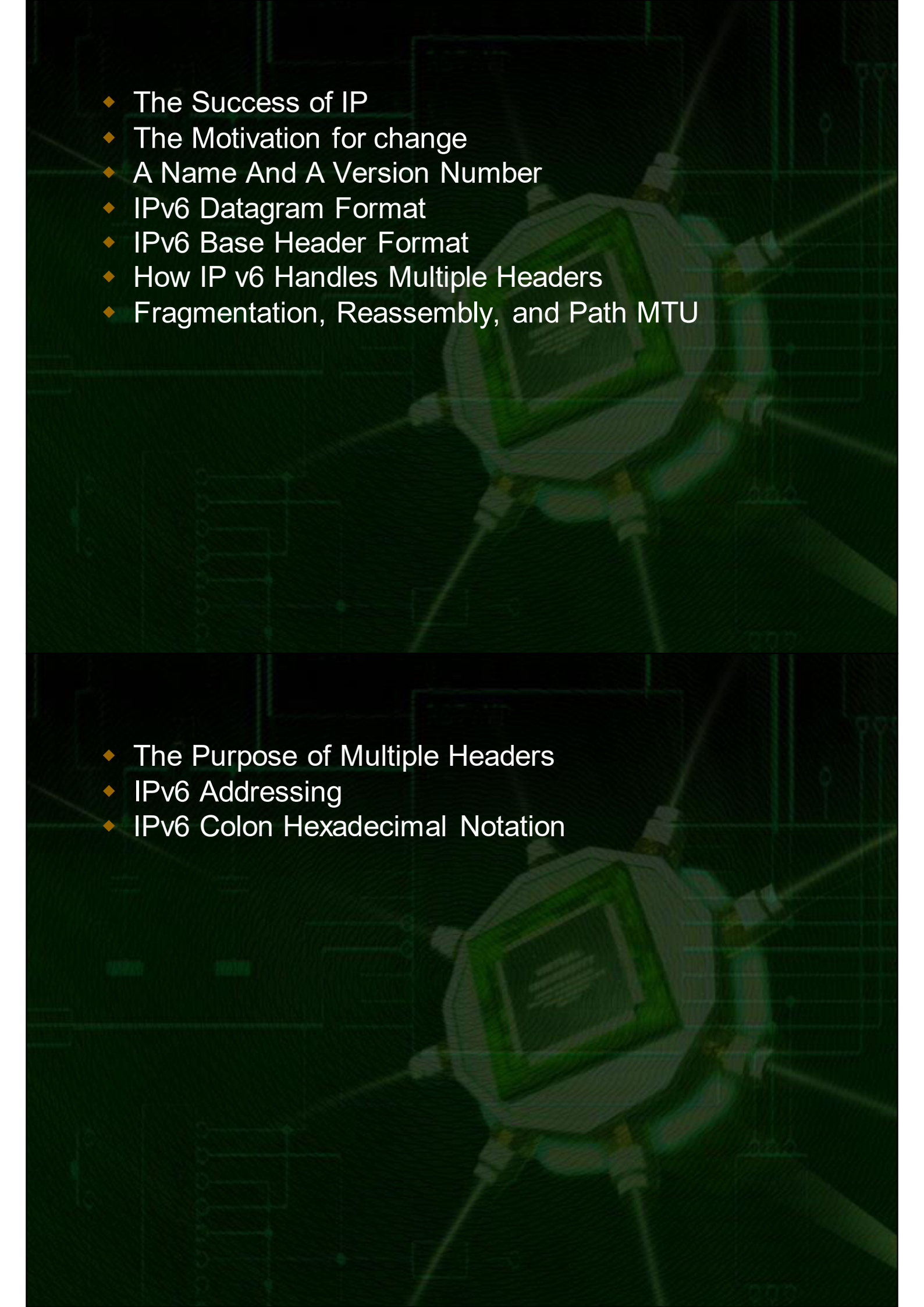
- ◆ Connectionless Service
- ◆ Virtual Packets
- ◆ The IP Datagram
- ◆ Forwarding an IP Datagram
- ◆ IP Addresses and Routing Table Entries
- ◆ The Mask Field and Datagram Forwarding

- 
- ◆ Destination and Next-Hop Addresses
 - ◆ Best-Effort Delivery
 - ◆ The IP Datagram Header Format

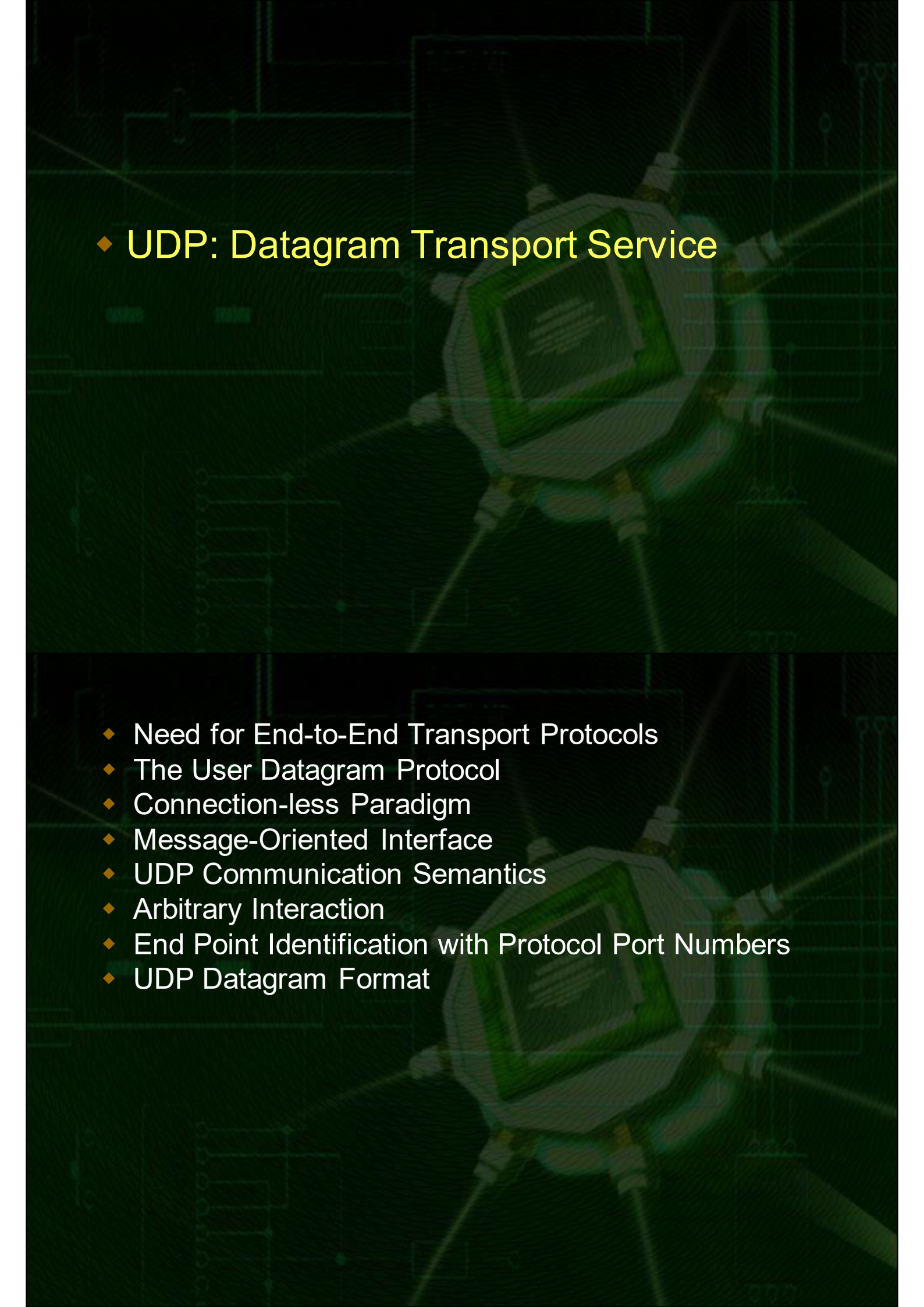
- ◆ IP ENCAPSULATION,
FRAGMENTATION, AND
REASSEMBLY

- 
- ◆ Datagram Transmission and Frames
 - ◆ Encapsulation
 - ◆ Transmission Across an Internet
 - ◆ MTU, Datagram Size, and Encapsulation
 - ◆ Reassembly
 - ◆ Identifying a Datagram
 - ◆ Fragment Loss
 - ◆ Fragmenting A Fragment

◆ THE FUTURE IP (IPv6)

- 
- ◆ The Success of IP
 - ◆ The Motivation for change
 - ◆ A Name And A Version Number
 - ◆ IPv6 Datagram Format
 - ◆ IPv6 Base Header Format
 - ◆ How IP v6 Handles Multiple Headers
 - ◆ Fragmentation, Reassembly, and Path MTU

- ◆ The Purpose of Multiple Headers
- ◆ IPv6 Addressing
- ◆ IPv6 Colon Hexadecimal Notation



◆ UDP: Datagram Transport Service

- ◆ Need for End-to-End Transport Protocols
- ◆ The User Datagram Protocol
- ◆ Connection-less Paradigm
- ◆ Message-Oriented Interface
- ◆ UDP Communication Semantics
- ◆ Arbitrary Interaction
- ◆ End Point Identification with Protocol Port Numbers
- ◆ UDP Datagram Format

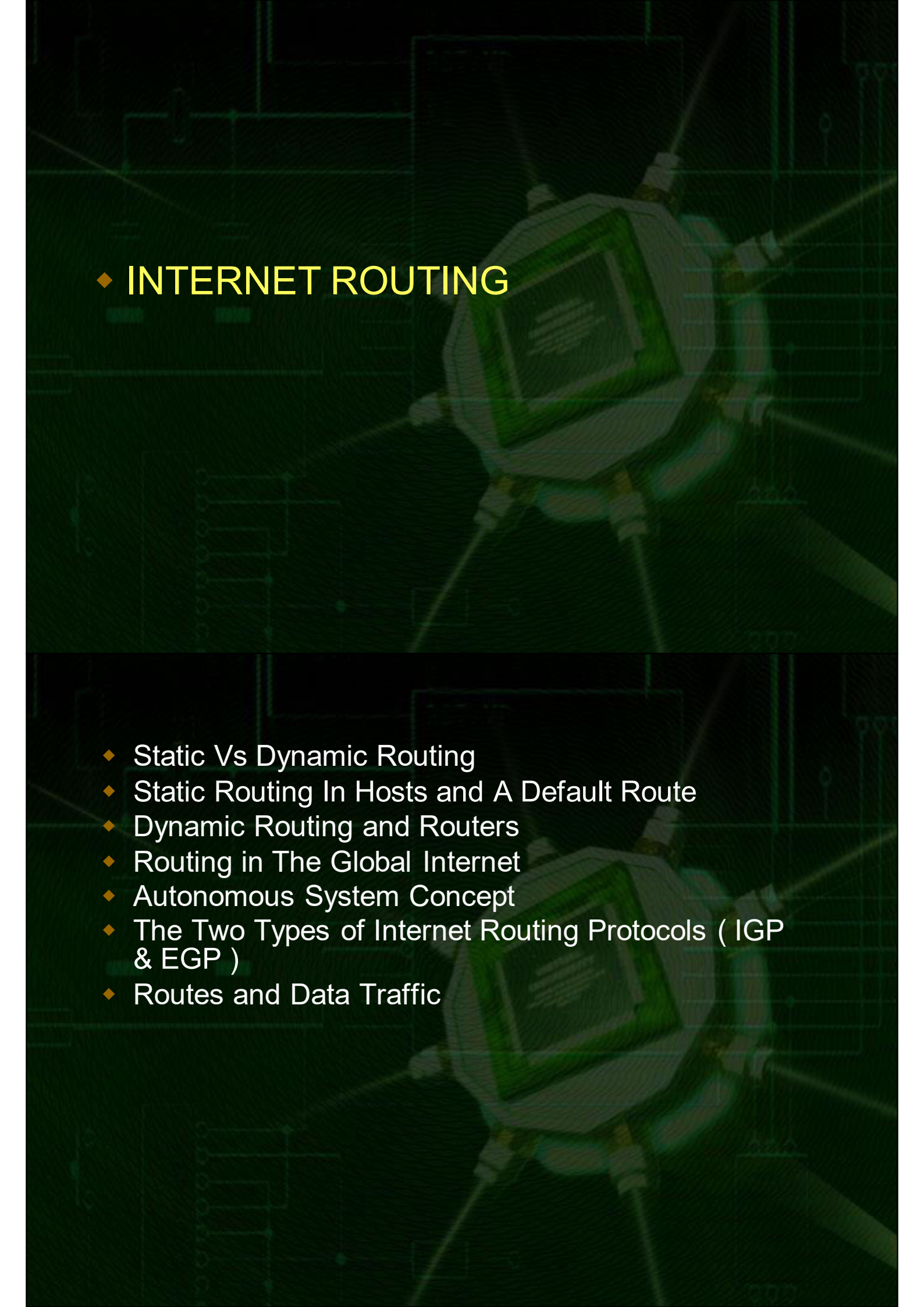
The background of the slide features a dark, textured image of a satellite in space, with its solar panels and various instruments visible. Overlaid on this is a faint, green, glowing circuit board pattern that covers the entire slide, giving it a high-tech, digital appearance.

◆ TCP: RELIABLE TRANSPORT SERVICE

- ◆ The Need For Reliable Transport
- ◆ The Transmission Control Protocol
- ◆ The Service TCP Provides to Applications
- ◆ End-To-End Service and Datagrams
- ◆ Achieving Reliability
- ◆ Packet Loss and Retransmission Times
- ◆ Adaptive Retransmission
- ◆ Buffers, Flow Control, and Windows

- ◆ Three-Way Handshake
- ◆ Congestion Control
- ◆ TCP Segment Format

- ◆ Network Address Translation



◆ INTERNET ROUTING

- ◆ Static Vs Dynamic Routing
- ◆ Static Routing In Hosts and A Default Route
- ◆ Dynamic Routing and Routers
- ◆ Routing in The Global Internet
- ◆ Autonomous System Concept
- ◆ The Two Types of Internet Routing Protocols (IGP & EGP)
- ◆ Routes and Data Traffic

- ◆ Border Gateway Protocol (BGP)
- ◆ The Routing Information Protocol (RIP)
- ◆ RIP Packet Format
- ◆ The Open Shortest path First Protocol (OSPF)
- ◆ An Example OSPF Graph
- ◆ OSPF Areas
- ◆ Multicast Routing

◆ THE END

www.vuCtn.com

Good Luck

Regards : Zarva Chaudhary

Admin:

* Zarva Chaudhary *

* Chaudhary Moazzam *

* Laiba Maki *