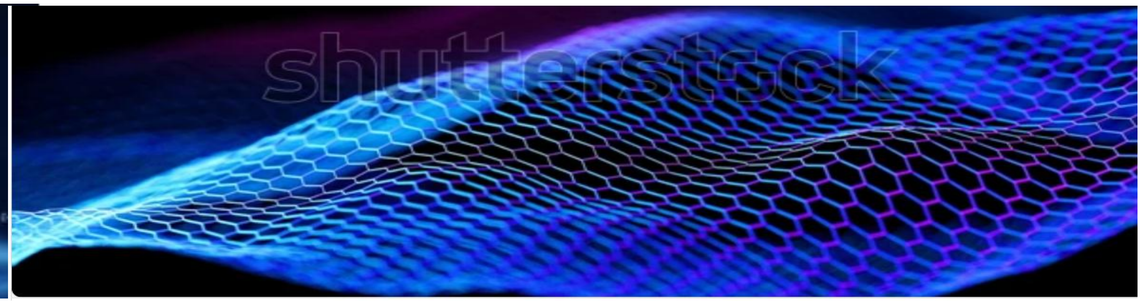
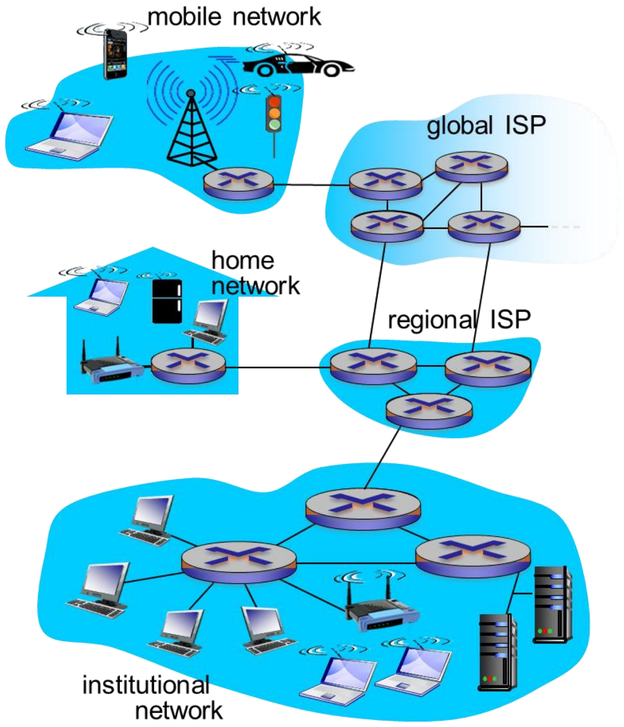


Introduction to Systems and Networks
INSY 3071



Workshet Lamenew (workshet.lamenew@aau.edu.et)

Phone: 0911435318

Class begins on September 25, 2025

Layers of Enterprise Architecture

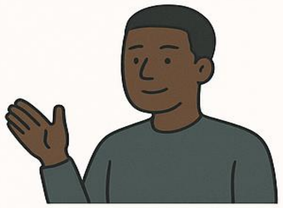
Business

Business Analyst

Data

Data Architect

Application



Application Architect

IT Infrastructure

Systems Architect

Which profession do you intend to assume?

System Analyst
Requirements Engineer
Software Architect / Designer

Data Engineer
Data Scientist
AI Specialist
Database Administrator

Programmer
Application Developer
Web Master
Mobile App Developer

Network Engineer
Network Administration
System Administration
Cybersecurity Expert

Industrial Project and Seminar

Modules in the Syllabus of the BSc in Information Systems at the School of Information Science

Foundations of Information Systems
Information Systems Development

Intelligent Systems
Database and Information Management

Fundamentals of Programming
Advanced Programming and Data Structures
Internet and Mobile Technology
Human Computer Interaction

Computer Networks, Administration and Security

Brief Description of the Course

- Information systems focusing on one of its components: ***network infrastructure***
- Highlights on the global network of networks: ***the Internet***
- Data transmission and the associated media (***Copper, Fiber, Wireless***)
- ***Network protocols*** as viewed from the OSI and ***TCP/IP***
- Emphasis will be given to ***IP addressing*** and the associated configurations
- ***Internetworking*** of networks including ***routing*** algorithms
- ***Advanced topics*** such as network performance, mobile networks, linking to ISPs, security

Learning Outcomes

- ***Understand*** the ***network infrastructure components*** of information systems
- ***Understand*** the ***notions and structure of data communications***
- ***Understand*** the concept of network protocols with a ***focus on TCP/IP***
- ***Practice*** the use of ***IP addressing*** and ***configurations***
- ***Familiarize*** with ***advanced topics*** in network performance, multimedia and security

Role of the Instructor

- Delivers lectures
- Provides consultations to students (Thursday Afternoon)
- Facilitates group discussions
- Works on projects with the students
- Evaluates class exercises, tests and final exam

Role of the students

- Attend lectures and lab sessions
- Participate in group discussions
- Work on home take assignments and a network design and configuration project in group
- Present final project work

Course Syllabus

1. Introduction to Systems and Networks

- Overview of Information Systems
- Components of Information Systems
- Global Digital Technology Systems
- The Internet as Global Digital Platform
- IT Infrastructure (client-server vs peer-to-peer)

Course Syllabus

2. Overview of Data Communication and Computer Networks

- Communication Model
- Computer Networks (Types, Components)
- Circuit Switched and Packet Switched Networks
- Network Topology and Network Devices
- Wired and Wireless Networks
- Emerging Network Systems

Course Syllabus

3. Network Protocols

- Introduction to Protocols (Syntax, Semantics, Timing)
- The OSI Reference Model
- The TCP/IP Reference Model
- Anatomy of TCP/UDP and IP
- IP Addressing (IPV4 and IPV6)

Course Syllabus

4. Internetworking

- Introduction to Internetworking
- Introduction to Routing
- Routing Protocols
    - Interior Gateway Routing Protocols
    - Border Gateway Routing Protocols
- VLAN and Inter VLAN Routing
- Software Defined Networks

Course Syllabus

5. Advanced Topics in Computer Networks

- Network Performance
- Wireless and Mobile Networks
- Linking to ISPs
- Security in Computer Networks (Preventing, Detecting, Recovery)

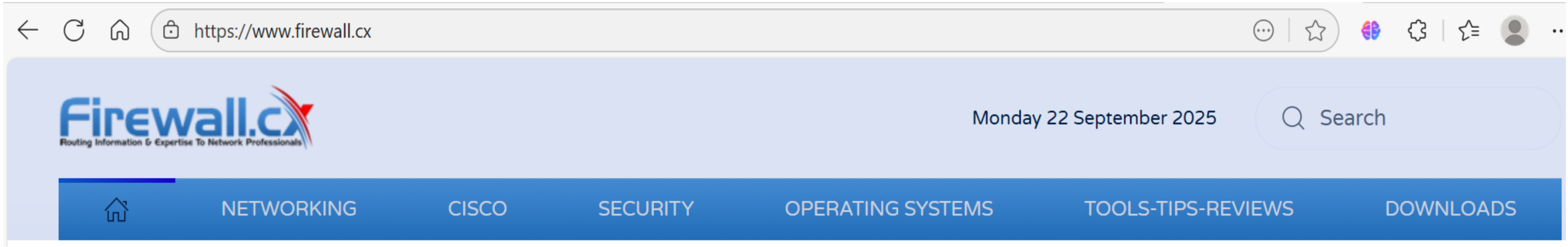
Assessment criteria

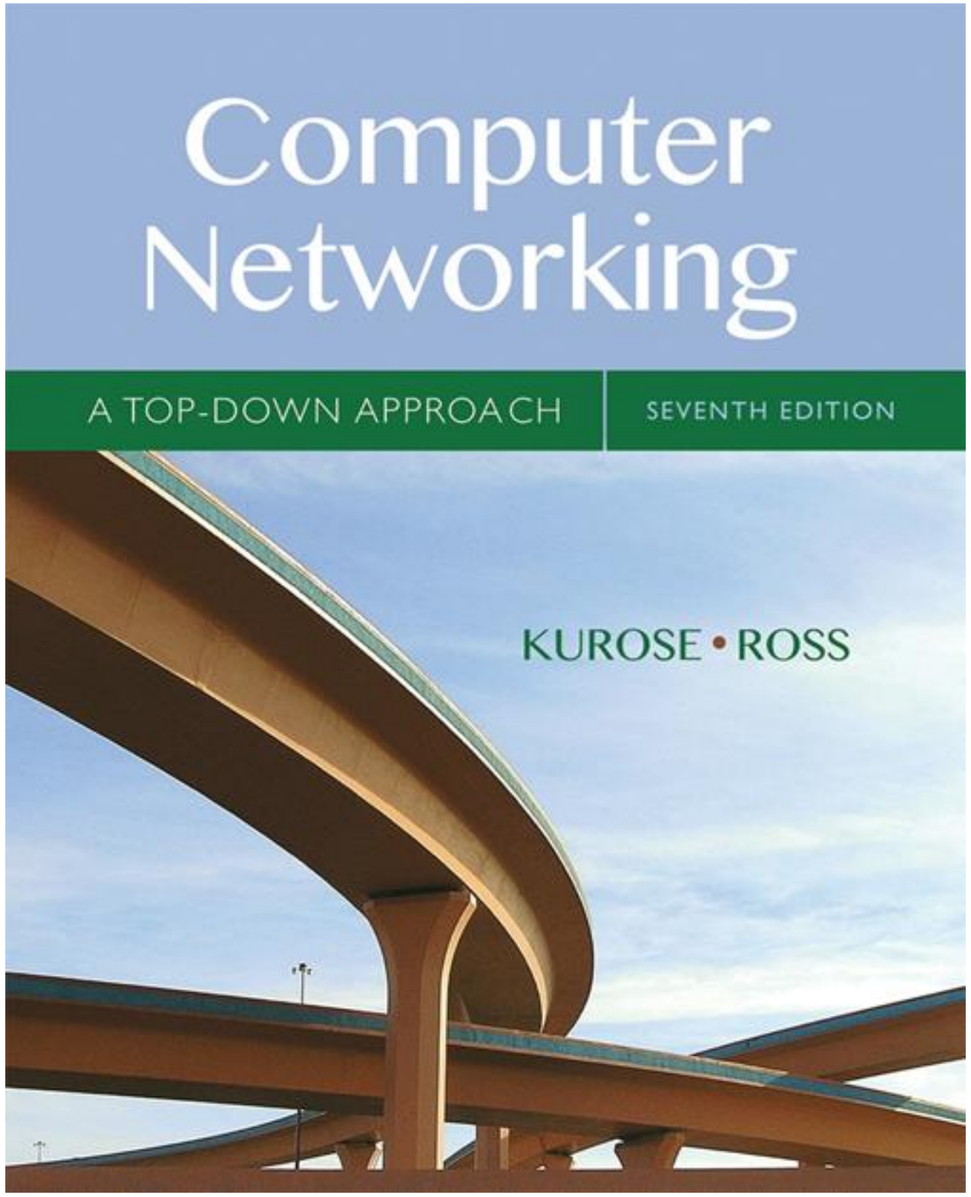
- Attendance, participation in ***the lab sessions***, home take assignments and class exercises (15%)
- Test (15%)
- Project (25%)
    - You are requested to start to visit the new building where the School of Information Science is located. You will be given orientation how to develop network requirements; design a network; and how tom implement on a simulation software. You will be required to design a network for the whole building and do configurations on a simulation tool and make presentations on a scheduled date.
- Final Exam (45%)

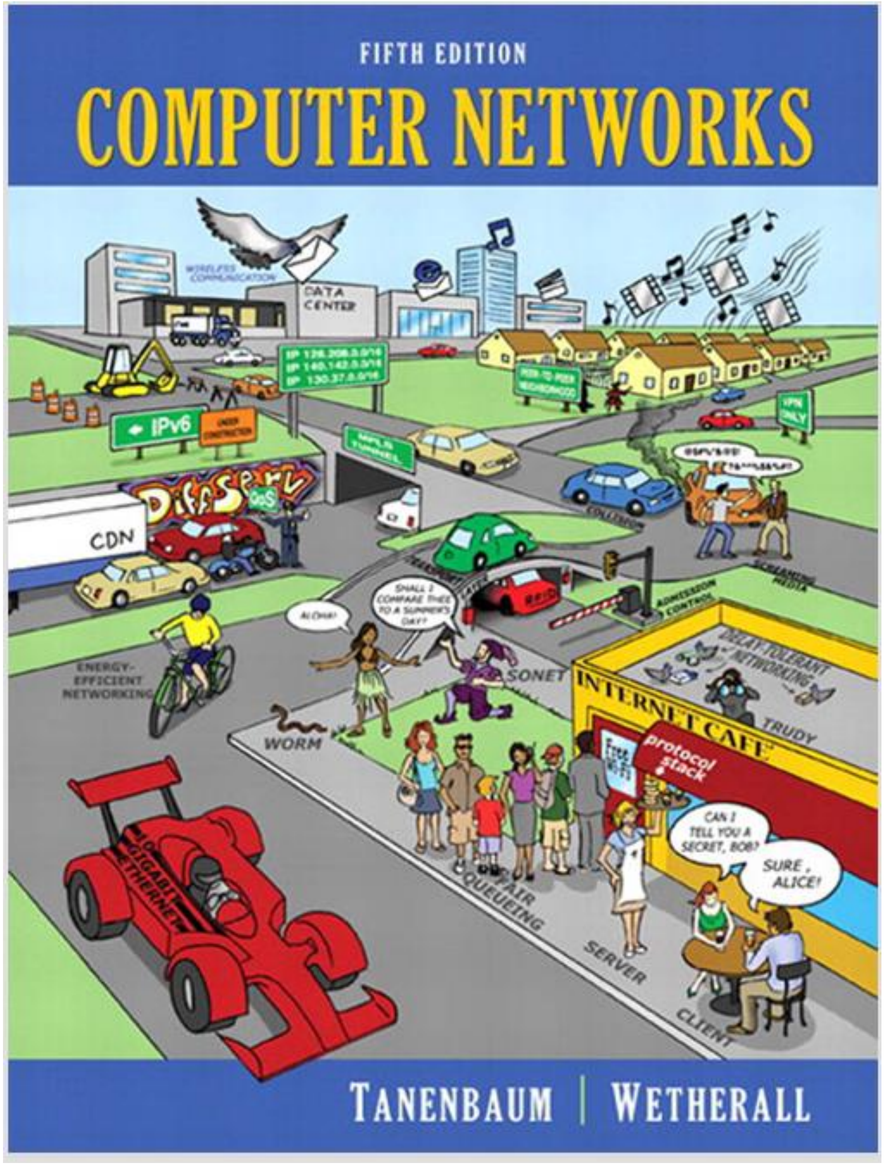
References

- Kurose and Ross. 2017. Computer Networking: A Top-Down Approach. 7th Ed.

- Tanenbaum. 2011. Computer Networks. 5thEd.




Computer Networking
A TOP-DOWN APPROACH
SEVENTH EDITION
KUROSE • ROSS

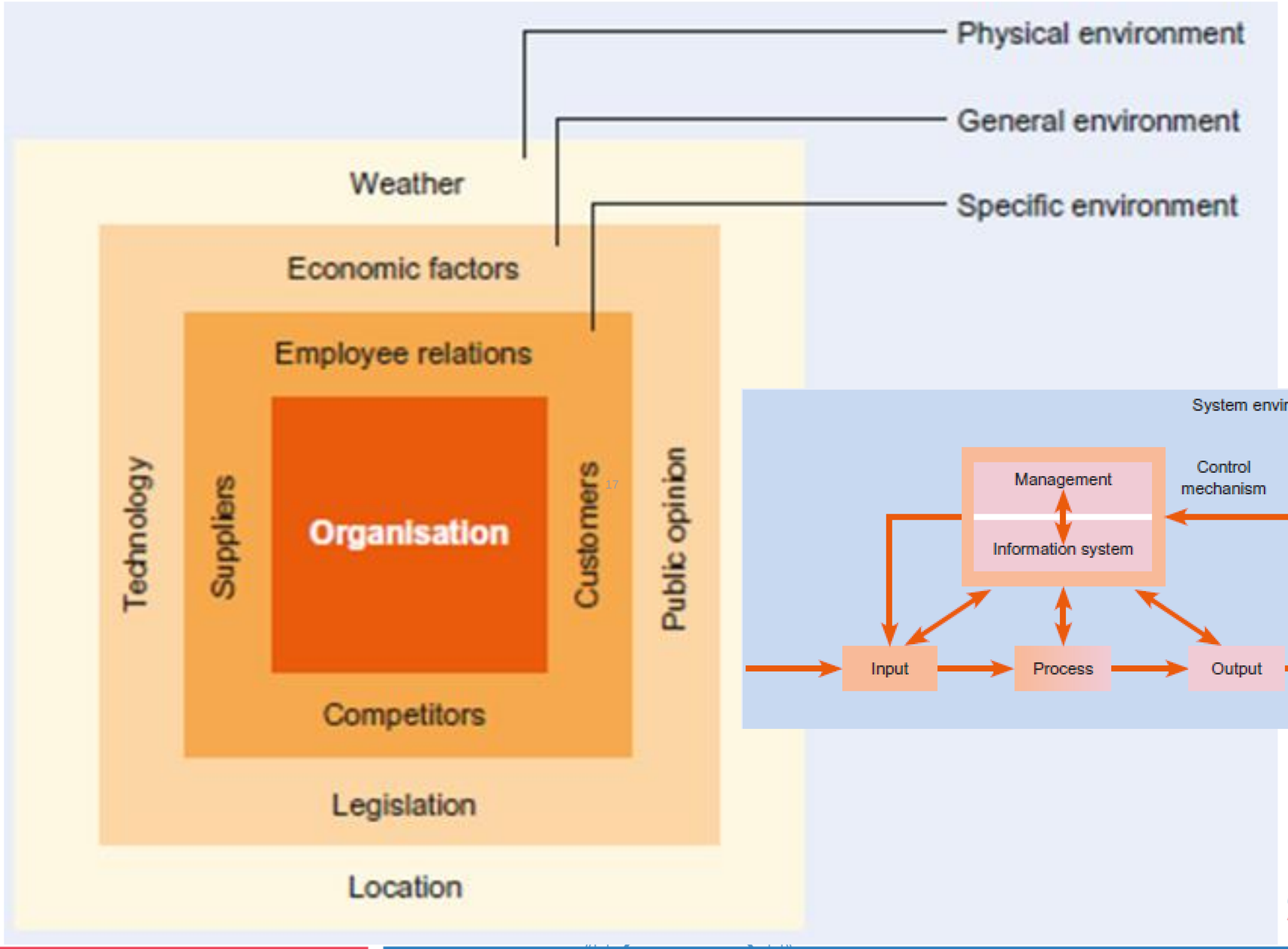

FIFTH EDITION
COMPUTER NETWORKS
TANENBAUM | WETHERALL

1. Introduction to Systems and Networks

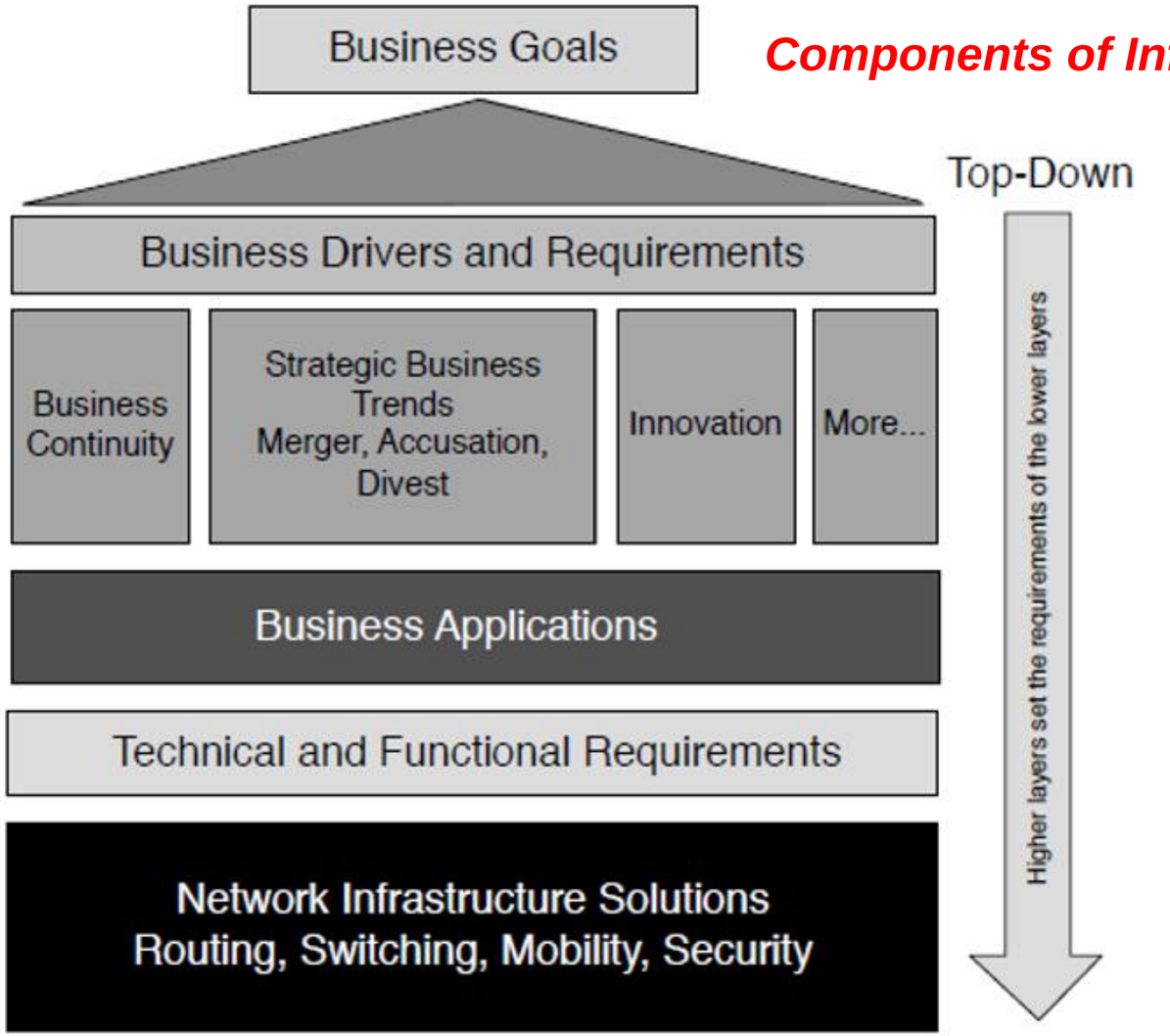
- Overview of Information Systems
- Components of Information Systems
- Global Digital Technology Systems
- The Internet as Global Digital Platform
- IT Infrastructure (client-server vs peer-to-peer)

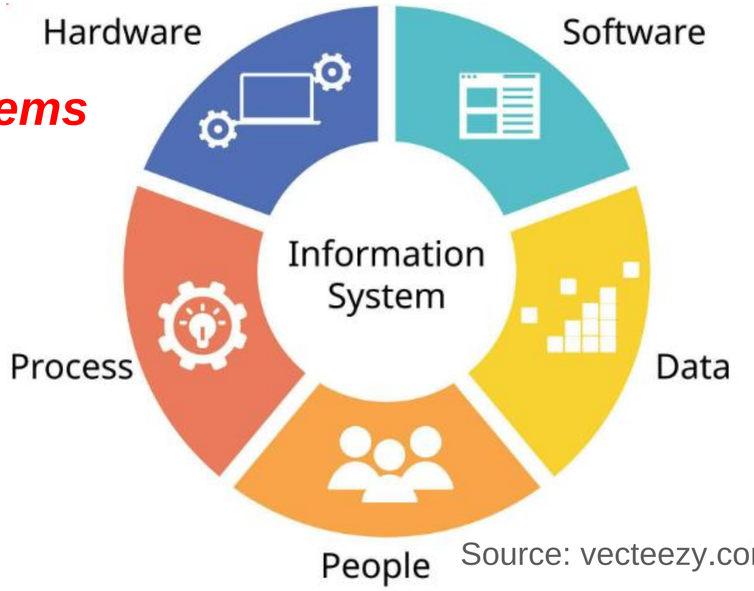
Information System

- Information system is an arrangement of people, data, processes, communication, and ***information technology (hardware and software)***
  - that interact to ***capture***, ***transmit***, *store*, retrieve, ***manipulate*** and/or ***display*** information needed
    - to support and improve day-to-day operations in a business as well as support the problem solving and decision-making needs of
      - management and other users.

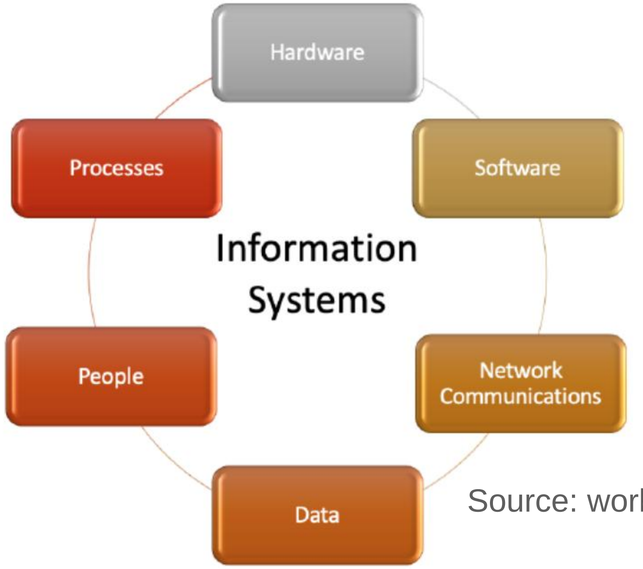

Physical environment
General environment
Specific environment
Weather
Economic factors
Employee relations
Technology
Suppliers
Organisation
Customers
Public opinion
Competitors
Legislation
Location
System environment
Management
Control mechanism
Information system
Input
Process
Output

Components of Information Systems





Source: vecteezy.com



Source: workforce.libretexts.org

Global Digital Technology Systems

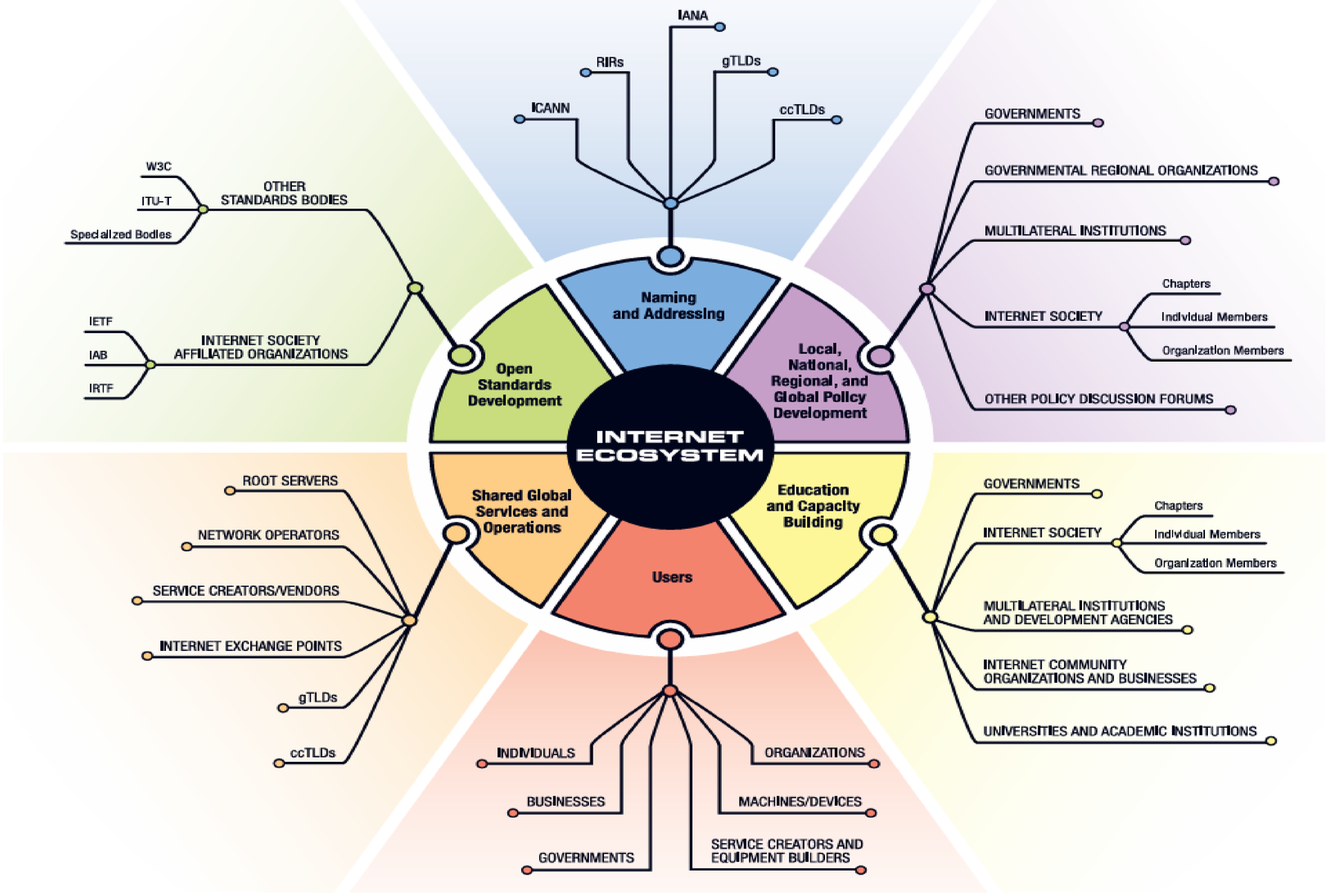
- *Interconnect* hardware (client and servers, network devices, cables), software (system and application), data, digital platforms, and people
- Global *communications* are performed using such systems to collect, process, store, and transmit information worldwide
- Enable global communication, *innovation*, and the transformation of businesses, economies, and daily life through technologies like
    - Desktop, laptop, smart phones, tablets, IoT devices, etc.
- Facilitate the *digital transformation* of organizations

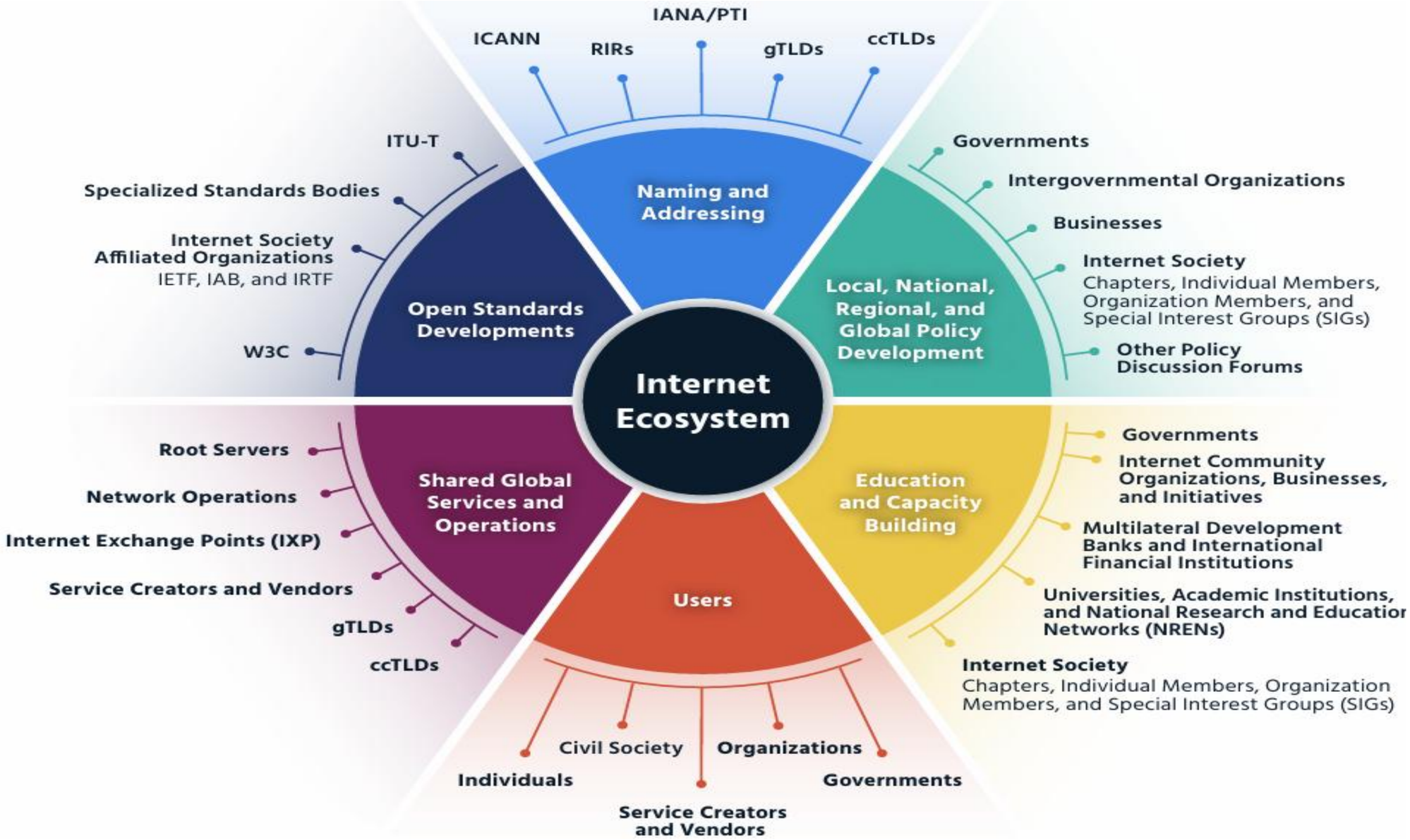
Digital Network

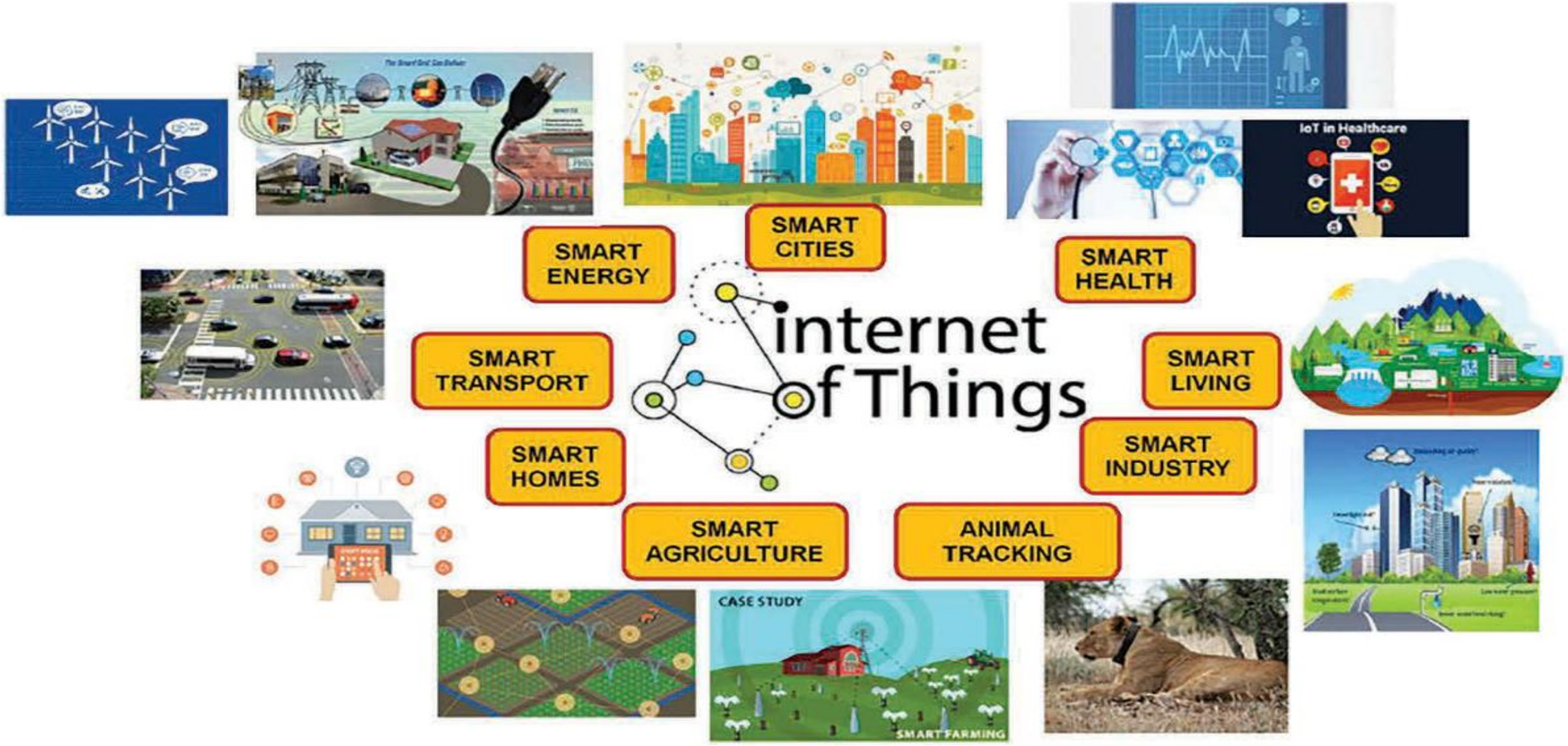
Global Digital Technology Systems

The Internet

- Huge network of millions of computers and related devices from all corners of the globe
- Users are able to communicate, exchange information, and partake in general resources
- More decentralized and does not have a specific owner
- Carries various information and services
    - email, online chat, web browsing, file transfer, multimedia, cloud,

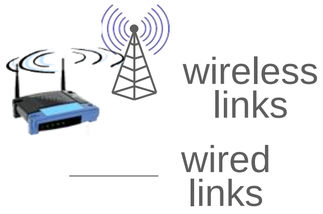

INTERNET ECOSYSTEM
Naming and Addressing
IANA
RIRs
gTLDs
ICANN
ccTLDs
Open Standards Development
OTHER STANDARDS BODIES
W3C
ITU-T
Specialized Bodies
INTERNET SOCIETY AFFILIATED ORGANIZATIONS
IETF
IAB
IRTF
Local, National, Regional, and Global Policy Development
GOVERNMENTS
GOVERNMENTAL REGIONAL ORGANIZATIONS
MULTILATERAL INSTITUTIONS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
OTHER POLICY DISCUSSION FORUMS
Shared Global Services and Operations
ROOT SERVERS
NETWORK OPERATORS
SERVICE CREATORS/VENDORS
INTERNET EXCHANGE POINTS
gTLDs
ccTLDs
Education and Capacity Building
GOVERNMENTS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
MULTILATERAL INSTITUTIONS AND DEVELOPMENT AGENCIES
INTERNET COMMUNITY ORGANIZATIONS AND BUSINESSES
UNIVERSITIES AND ACADEMIC INSTITUTIONS
Users
INDIVIDUALS
ORGANIZATIONS
BUSINESSES
MACHINES/DEVICES
GOVERNMENTS
SERVICE CREATORS AND EQUIPMENT BUILDERS


Internet Ecosystem
Naming and Addressing
IANA/PTI
ICANN
RIRs
gTLDs
ccTLDs
Open Standards Developments
ITU-T
Specialized Standards Bodies
Internet Society Affiliated Organizations
IETF, IAB, and IRTF
W3C
Local, National, Regional, and Global Policy Development
Governments
Intergovernmental Organizations
Businesses
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Other Policy Discussion Forums
Shared Global Services and Operations
Root Servers
Network Operations
Internet Exchange Points (IXP)
Service Creators and Vendors
gTLDs
ccTLDs
Education and Capacity Building
Governments
Internet Community Organizations, Businesses, and Initiatives
Multilateral Development Banks and International Financial Institutions
Universities, Academic Institutions, and National Research and Education Networks (NRENs)
Internet Society
Chapters, Individual Members, Organization Members, and Special Interest Groups (SIGs)
Users
Civil Society
Organizations
Individuals
Governments
Service Creators and Vendors


SMART ENERGY
SMART CITIES
SMART HEALTH
SMART TRANSPORT
internet of Things
SMART LIVING
SMART HOMES
SMART INDUSTRY
SMART AGRICULTURE
ANIMAL TRACKING
IoT in Healthcare
CASE STUDY
SMART FARMING

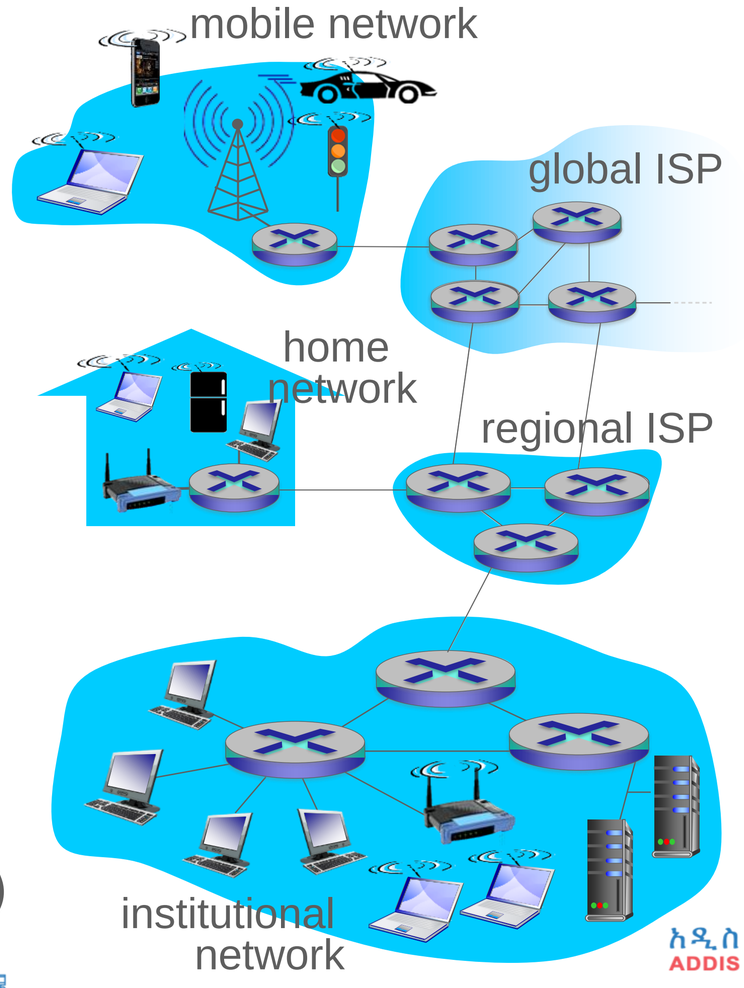
What's the Internet: "nuts and bolts" view

- billions of connected computing devices:
  - *hosts* = *end systems*
  - running *network apps*

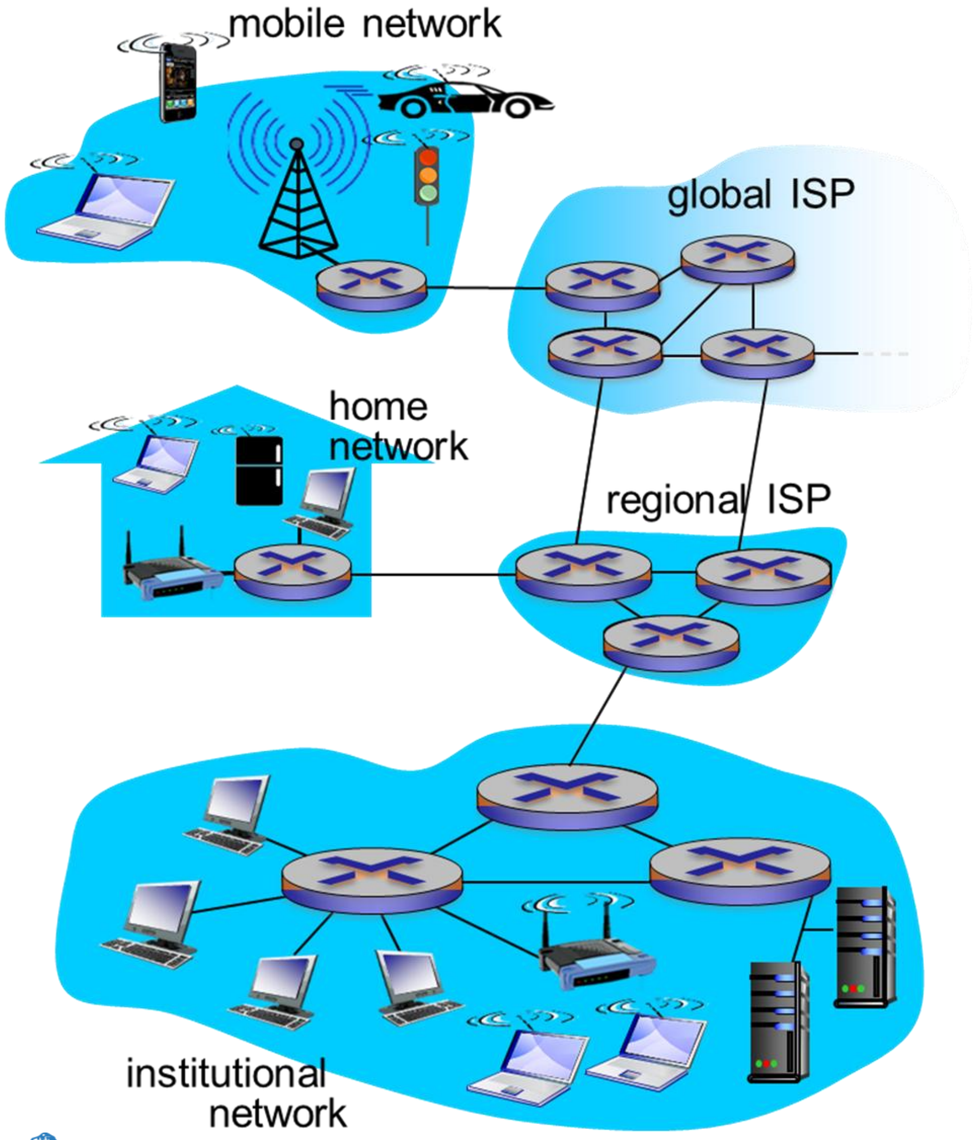


- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate: *bandwidth*

- *packet switches:* forward packets (chunks of data)
  - *routers* and *switches*



- *Internet:* "network of networks"
  - Interconnected ISPs
- *protocols* control sending, receiving of messages
  - e.g., TCP, IP, HTTP, Skype, 802.11
- *Internet standards*
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



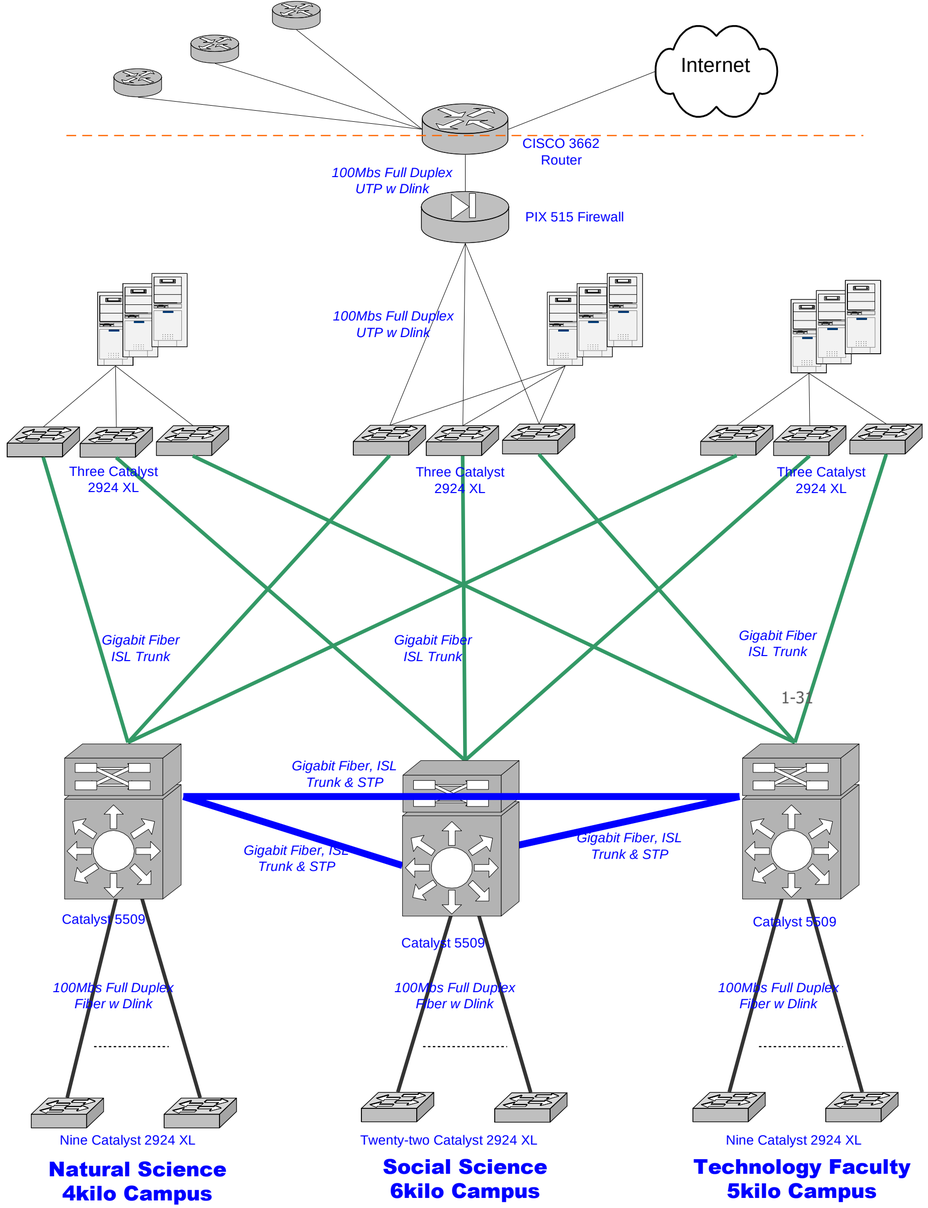
IT Infrastructure

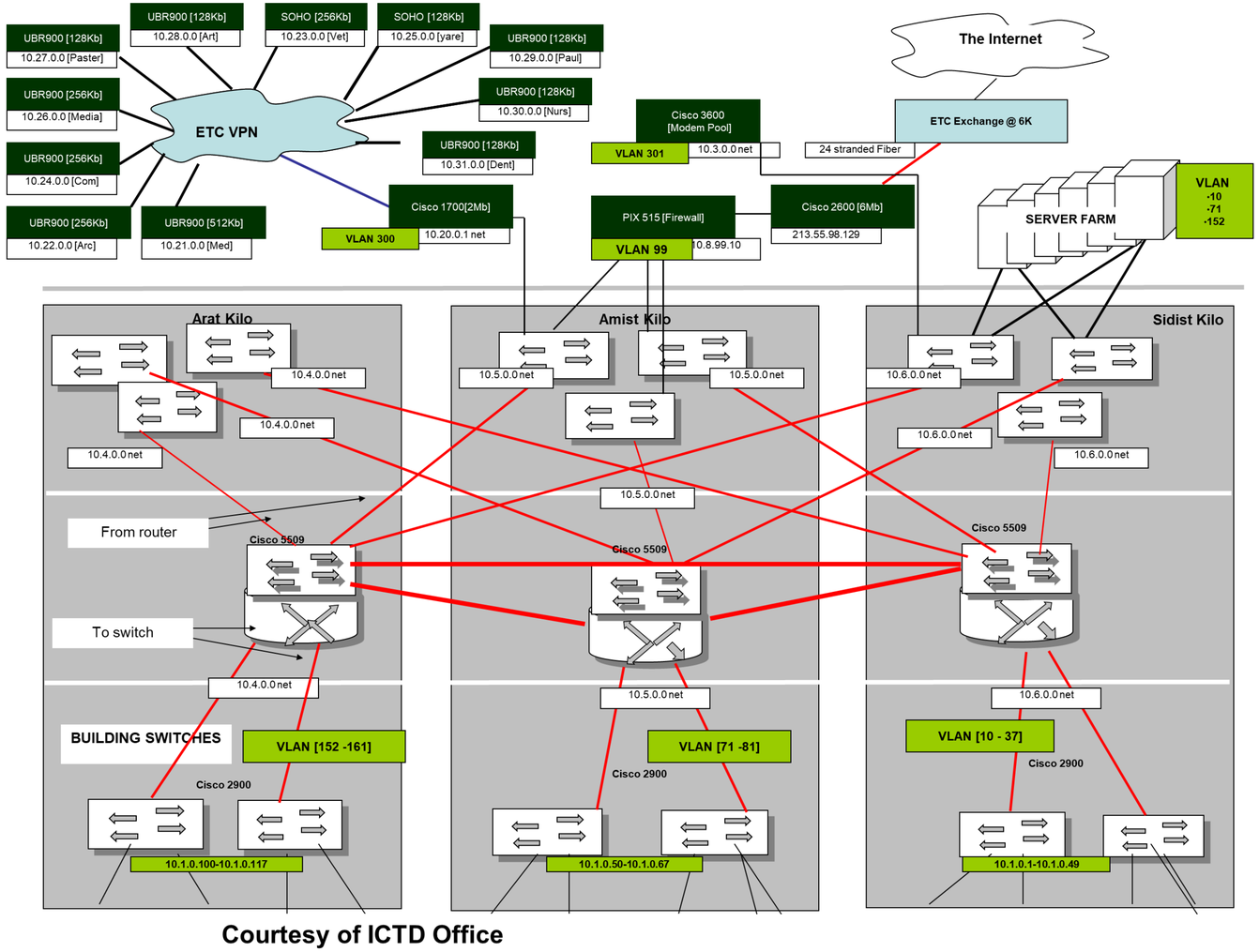
- Backbone comprising the computing hardware, software, networks, storage,
- A foundational framework of physical and virtual components
- Enables individuals, businesses and societies to process, store, communicate, and deliver data/information

IT Infrastructure

- Client-server systems
  - use dedicated, centralized servers to provide resources to multiple clients
  - offer enhanced security and management
- Peer-to-peer (P2P)
  - decentralize resources, allowing every device to act as both a client and a server
  - cost-effective, resilient, and scalable network that grows with demand

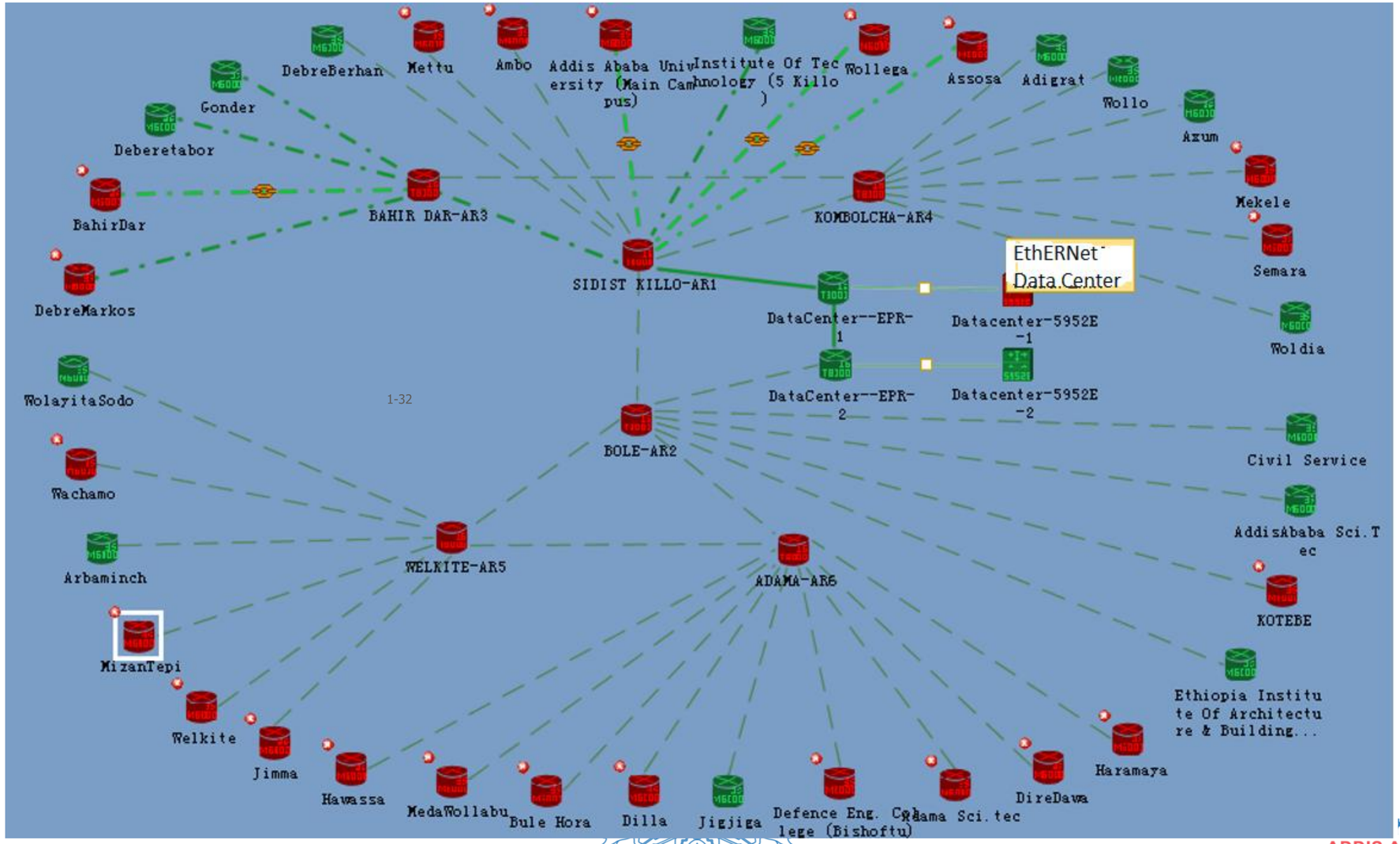
AAUNet Infrastructure: State-of-the-art tech





Courtesy of ICTD Office

Ethiopian Educational and Research Network (EthERNet)



2. Overview of Data Communication and Computer Networks

- Communication Model
- Computer Networks (Types, Components)
- Circuit Switched and Packet Switched Networks
- Network Topology and Network Devices
- Wired and Wireless Networks
- Emerging Network Systems

Communication Model

Person to Person

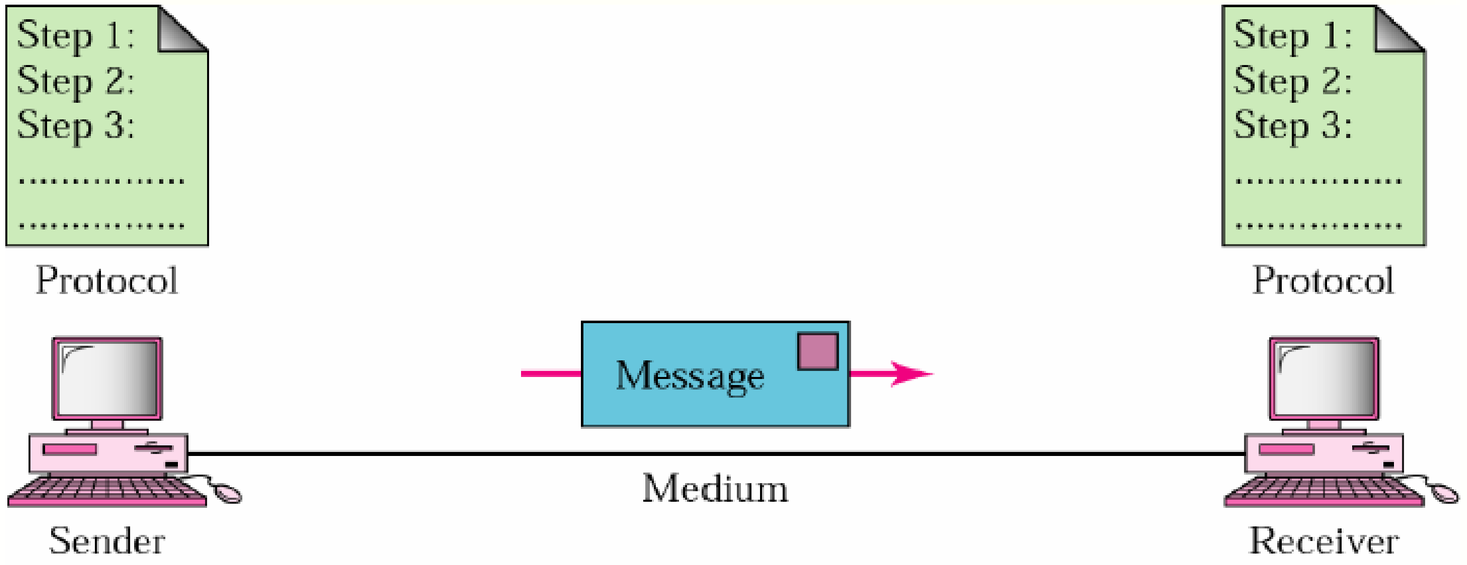
Person to People

People to People

Computer to Computer

Computers to Computers

- A data communication system has 5 components



1. Sender: the device - computer, video camera, …
2. Receiver: still the device
3. Message: the information to be communicated (text, numbers, pictures, sound, video - or combinations)
4. Medium: the physical path by which a message travels from sender to receiver
5. Protocol: the set of rules that govern data communications; an agreement between the communicating devices

Modes of Data Communication

- Data Transmission mode defines the direction of the flow of information between two communication devices
- When data are transmitted from one point to another, three modes of transmission can be identified:
  - ***Simplex*** (unidirectional)
  - ***Half Duplex*** (both directions but only in one direction at a time)
  - ***Full Duplex*** (data can be transmitted in both directions simultaneously)

Computer Network

- A computer network is a group of computers and associated peripheral devices connected by a communication channel capable of sharing files and other resources among several users.

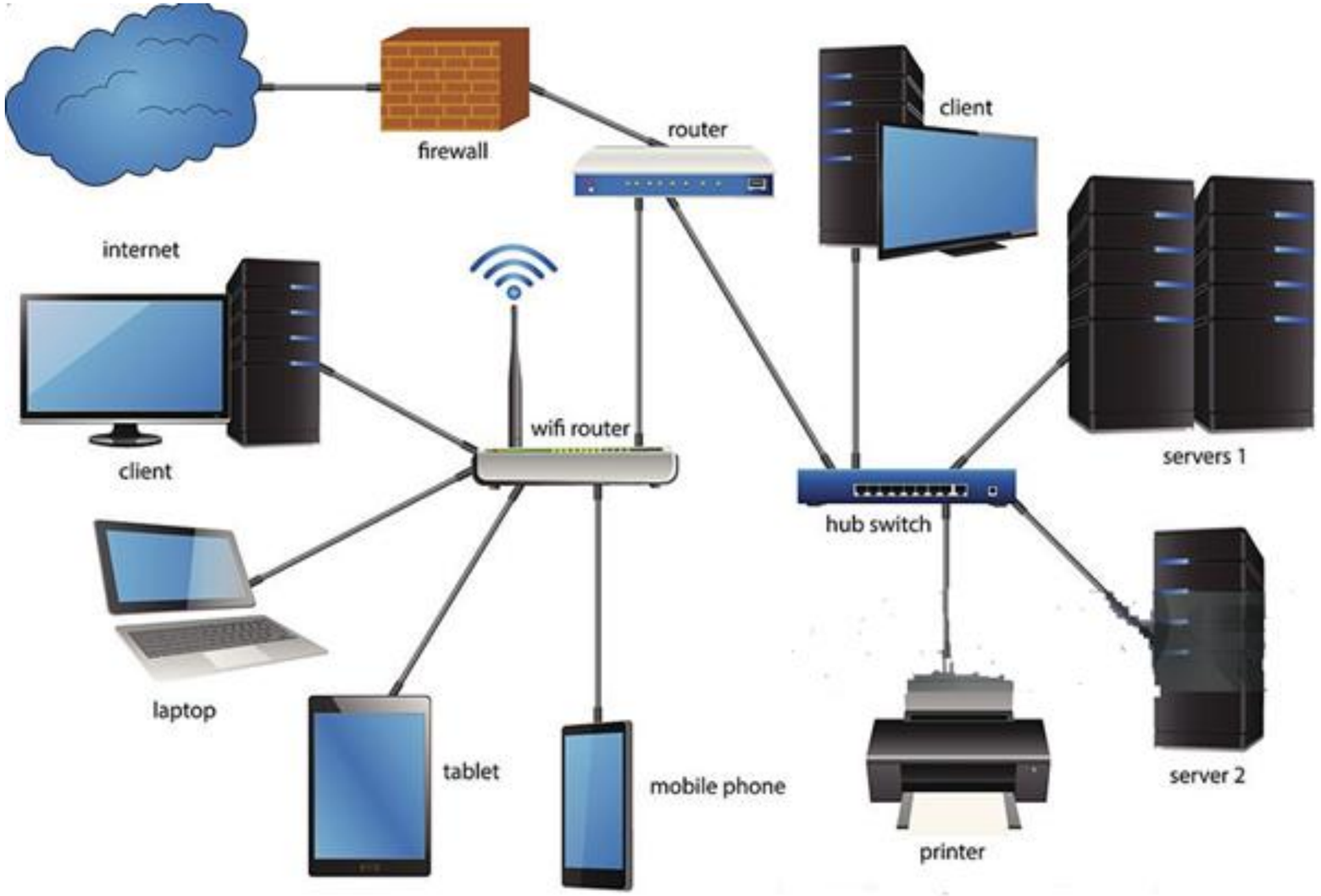
- Computer network is a connection of two or more computers that are connected with one another for the purpose of communicating data or information electronically.

Computer Network

- This connecting together of computers and other devices is called a *Network*, and the concept or practice of connected computers sharing resources is called *Networking.*

Components of Computer Networks

- A network operation needs devices that are designed to handle certain network functions: Physical and Soft Components
  - Physical
    - Computing devices (desktop, laptop, tablet, mobile phones, etc.)
    - Transmission media (cables)
    - Networking devices (hubs, switches, bridges, and routers)
    - Security devices (Firewall)
  - Software components (OS, network protocols, applications)


internet
firewall
router
client
client
wifi router
servers 1
hub switch
laptop
tablet
mobile phone
server 2
printer

Types of Networks

Personal Area Network (PAN)

- PAN is an interconnection of ***personal devices*** to communicate over a short distance like within 10 meters usually using wireless technology.
- The computing devices used in a PAN are mostly ***mobile phones with wireless data interfaces, tablets and laptops.***

Types of Networks

Local Area Network (LAN)

- Collection of devices connected in ***one physical location***, such as a building, office, or home.
- A LAN ***can be small or large***, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
- LAN connects ***network devices*** in such a way that users of PCs can share data and peripheral devices such as storage, scanners and printers.

Types of Networks

Campus Area Network (CAN)

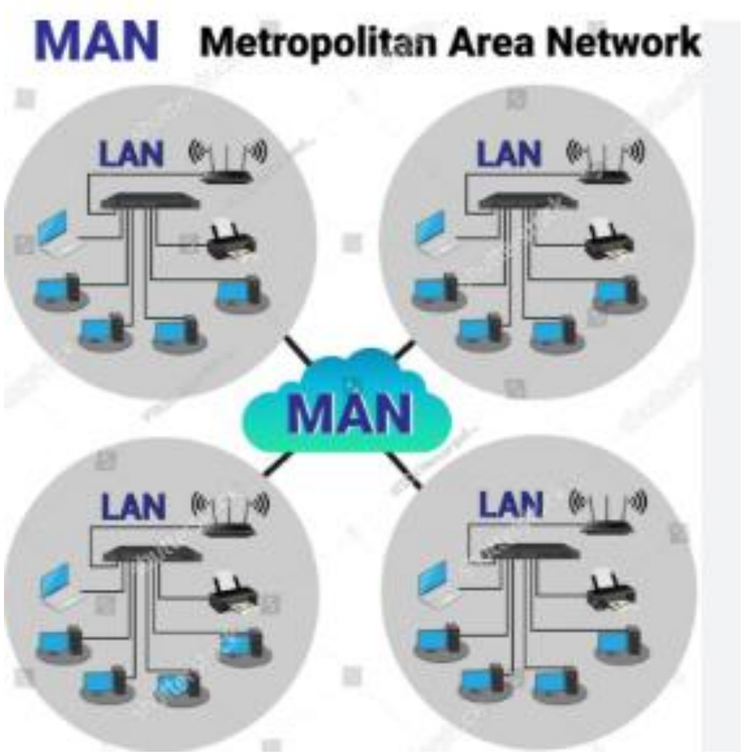
- CAN is a ***group of interconnected LANs*** within a limited geographical area like school campus, university campus, military bases, or organizational campuses and corporate buildings.

- The ***LAN at the CNCS of AAU*** can be said to be a CAN, connecting various departments and buildings.

Types of Networks

Metropolitan Area Network (MAN)

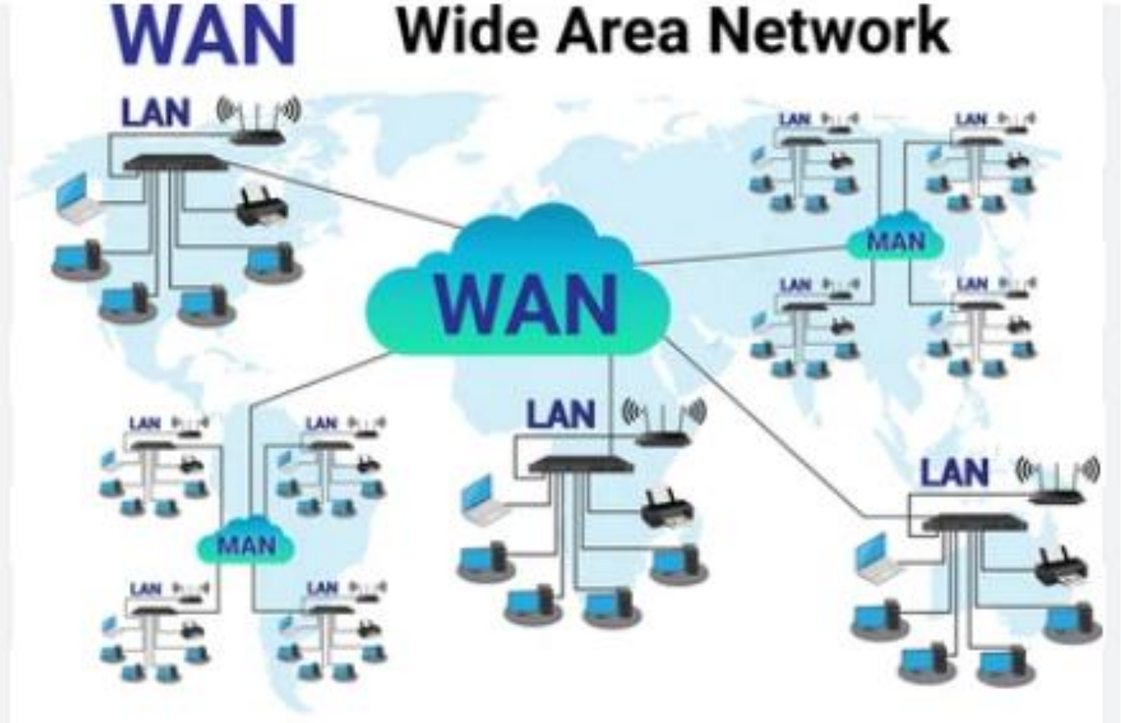
- A MAN is larger than a LAN but smaller than a WAN.
- It usually employs telecom infrastructure to connect various networks in a city or town which are geographically apart.
- MAN allows for centralized management and control of the network.



Types of Networks

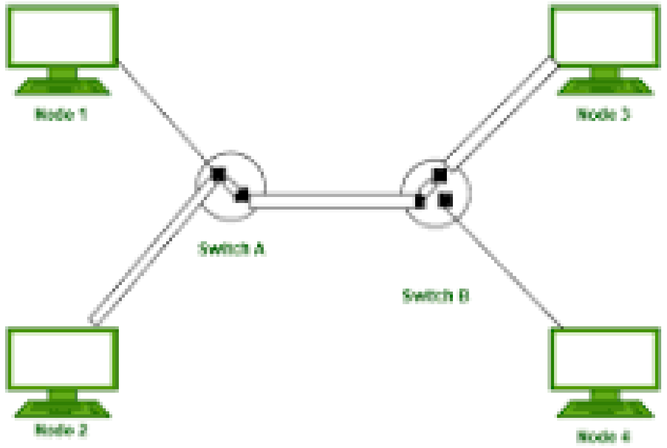
Wide Area Network (WAN)

- Connects computers over a large geographical distance through a shared communication path.
- The most common example of WAN is the Internet. The data transfer rate is slow in comparison to LAN because of large distances and high number of connected systems within the network.
- .



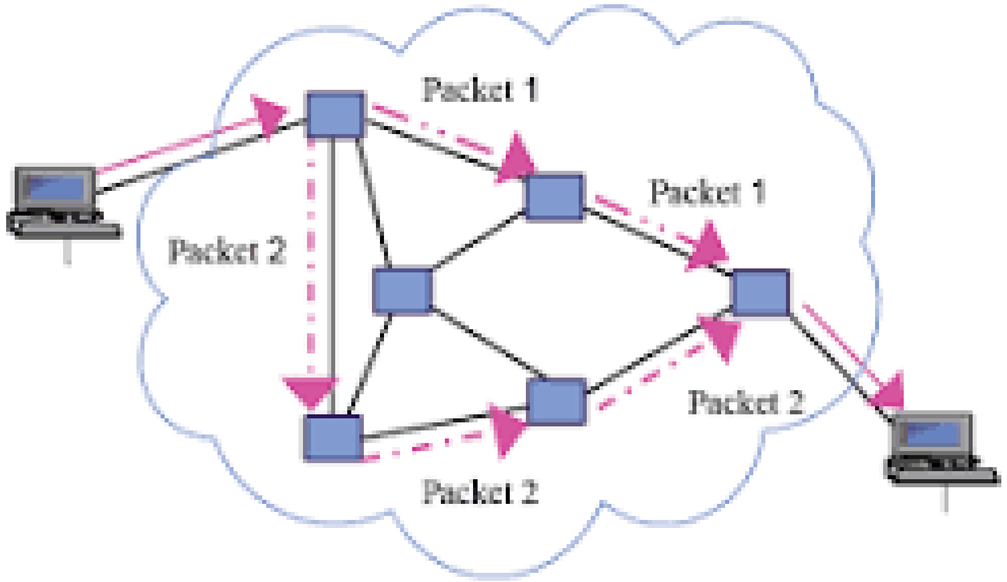
Circuit Switched and Packet Switched Networks

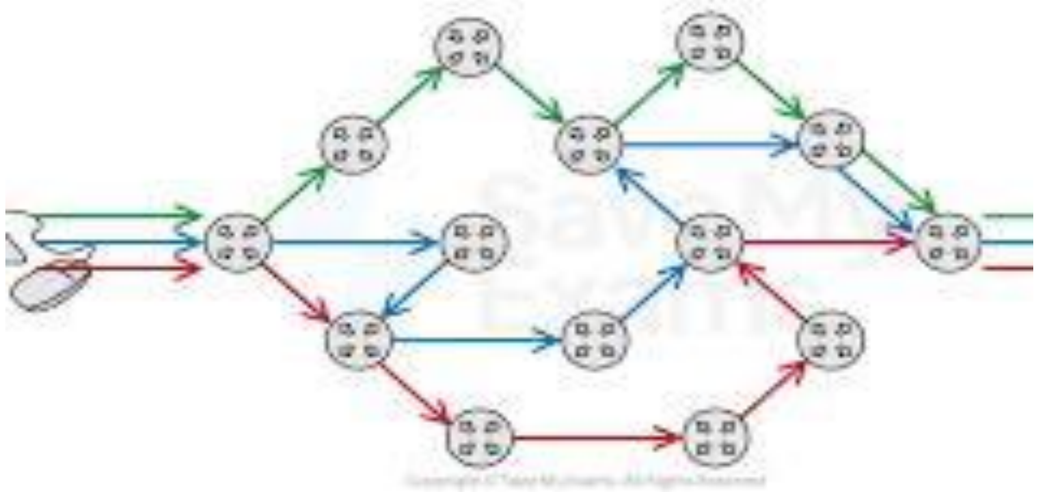
- ***Circuit switching*** dedicates a physical path for the entire duration a communication
- Examples include
  - Traditional phone line, GSM network
- Offer guaranteed quality
  - but inefficient use of resources



• Circuit Switched and Packet Switched Networks

- ***Packet switching***, used by the internet, **breaks data into small, independent packets** that find the best route, allowing for flexible, cost-effective data transfer and better bandwidth use, though it can ***introduce variable latency*** and requires data reassembly at the destination



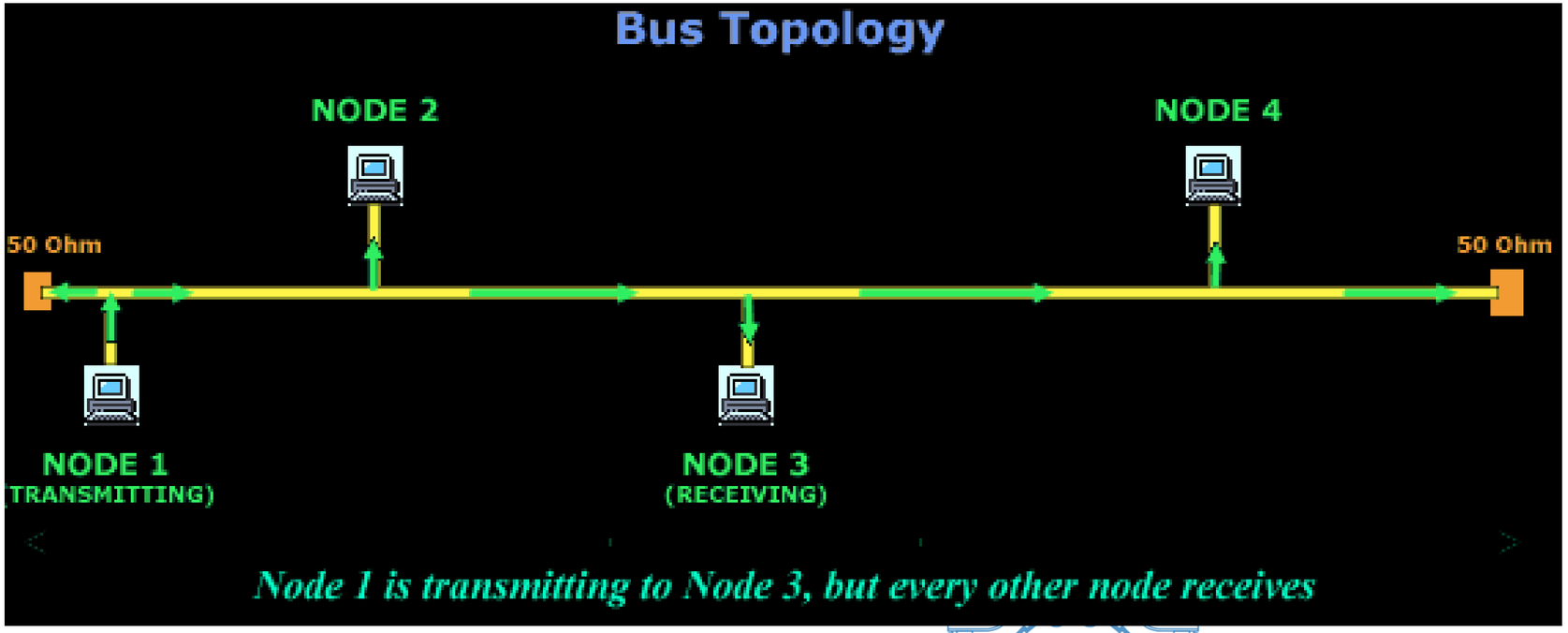


Network Topology and Network Devices

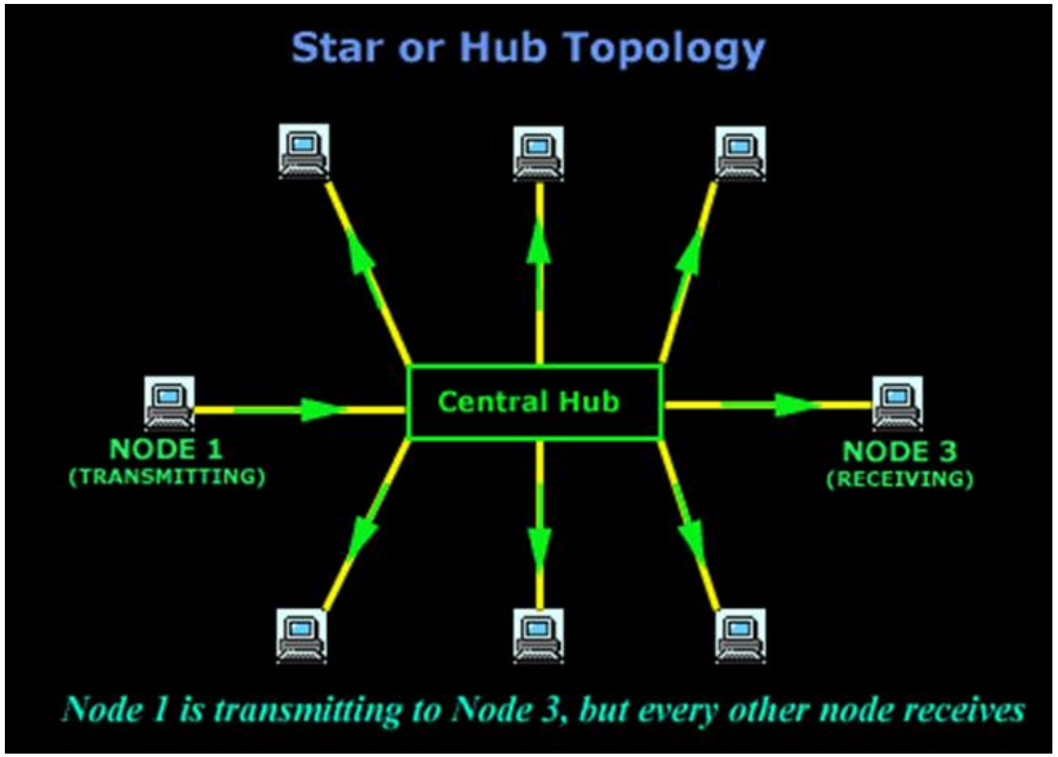
- Network topology refers to the way in which a network is laid out physically
- Two or more links form a topology
- The topology of a network is the ***geometric representation*** of the relationship of all the links and linking devices (usually called nodes) to one another

Bus Topology

All workstations are connected directly to the main backbone that carries the data. Traffic generated by any computer will travel across the backbone and be received by all workstations

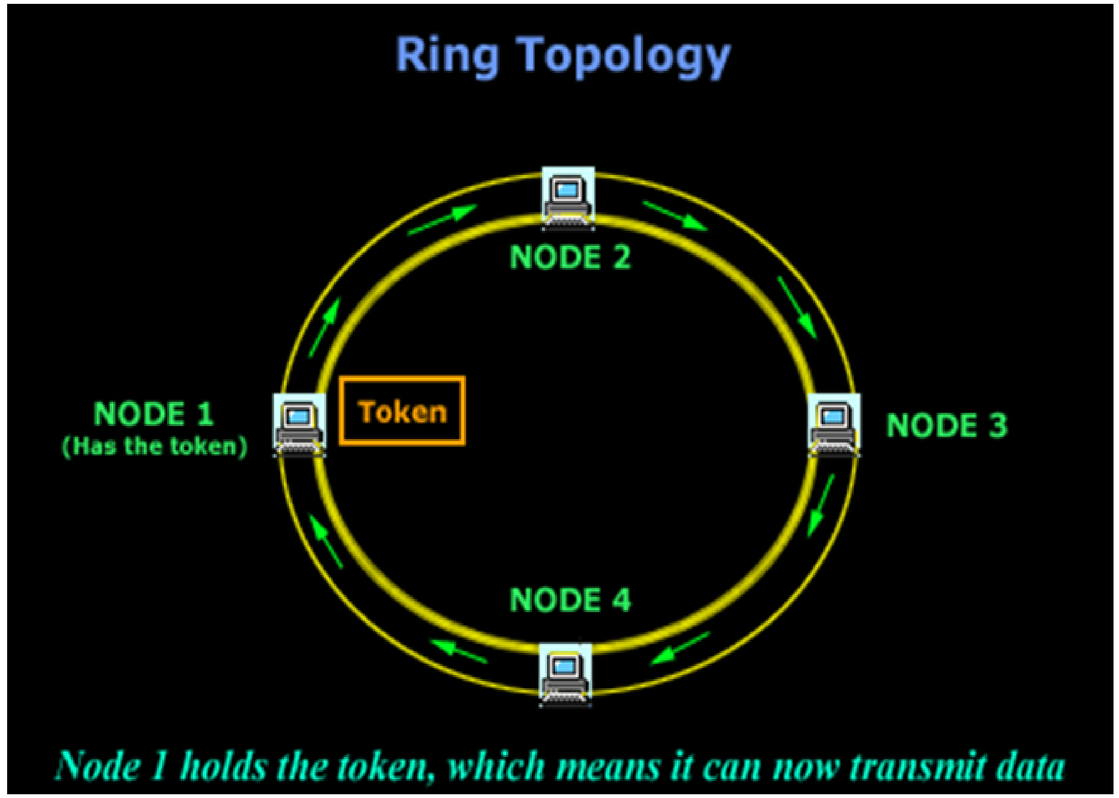


Star Topology



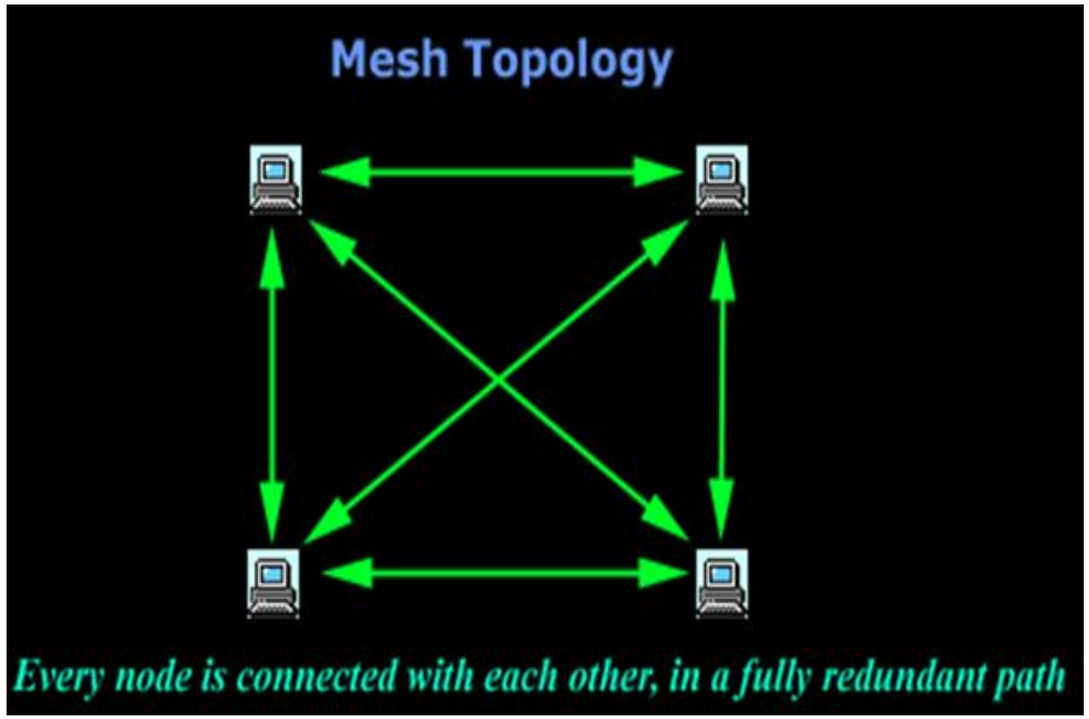
- The Star topology is one of the most common network topologies **found in most offices and home networks**.
- It has become ***very popular*** in contrast to the bus type ***because of the cost and the ease of troubleshooting.***
- Data is relayed using ***CSMA/CD*** method

Ring Topology



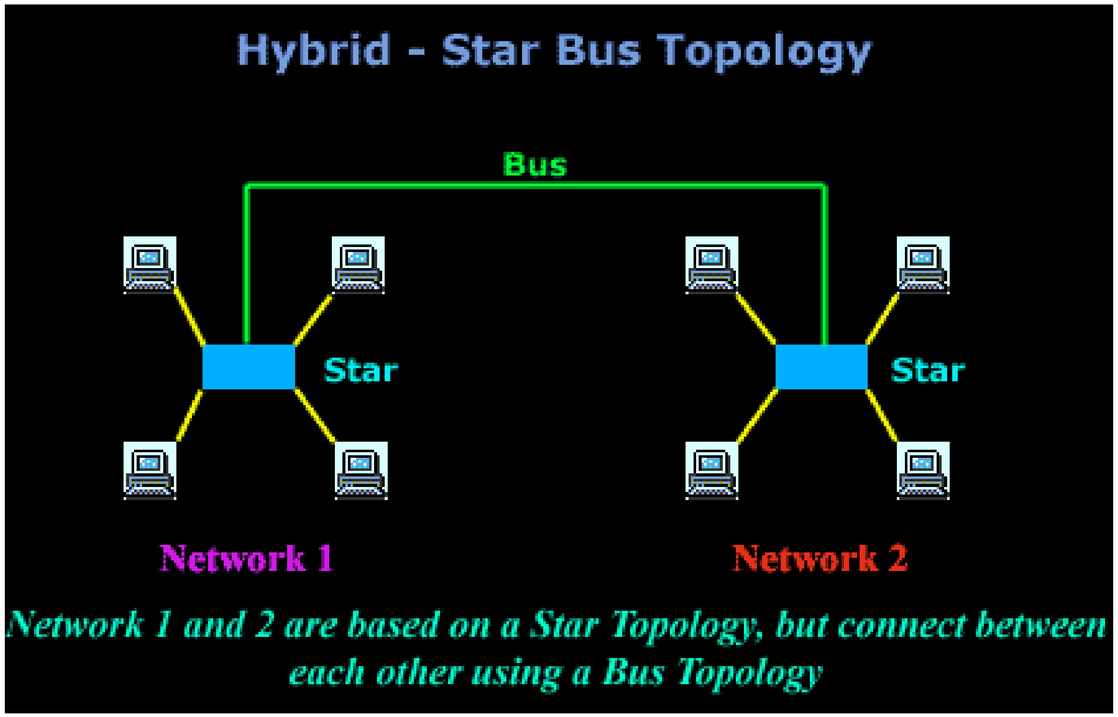
- In the ring topology, computers are connected on ***a single circle of cable.***
- The method by which the data is transmitted around the ring is called ***token passing***.
- A *token* is a special series of bits that contains control information.

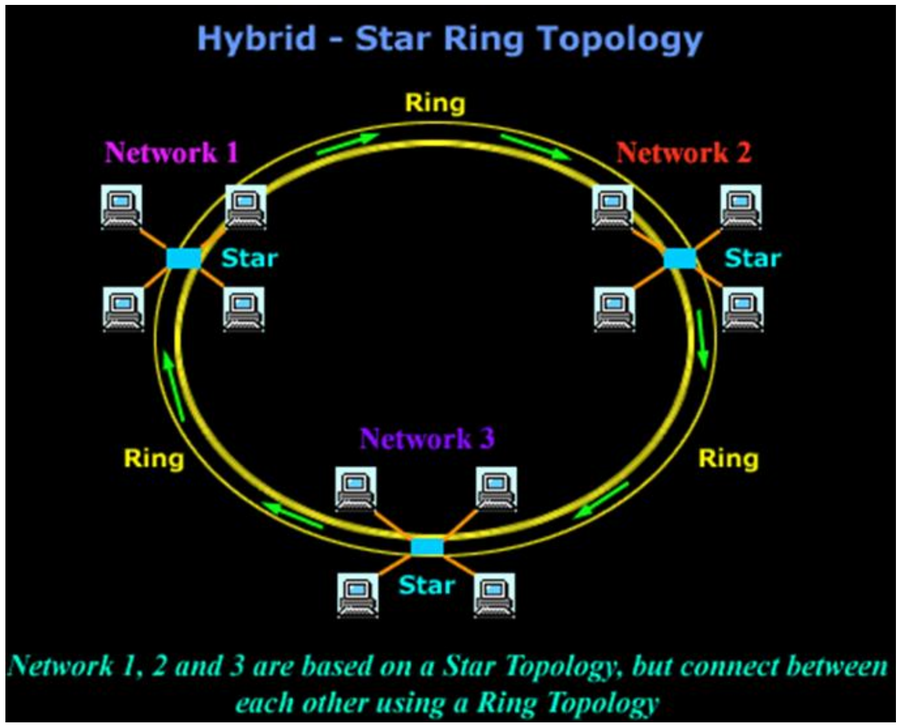
Mesh Topology



- Each computer is connected to every other computer by a separate cable.
- This configuration provides redundant paths.

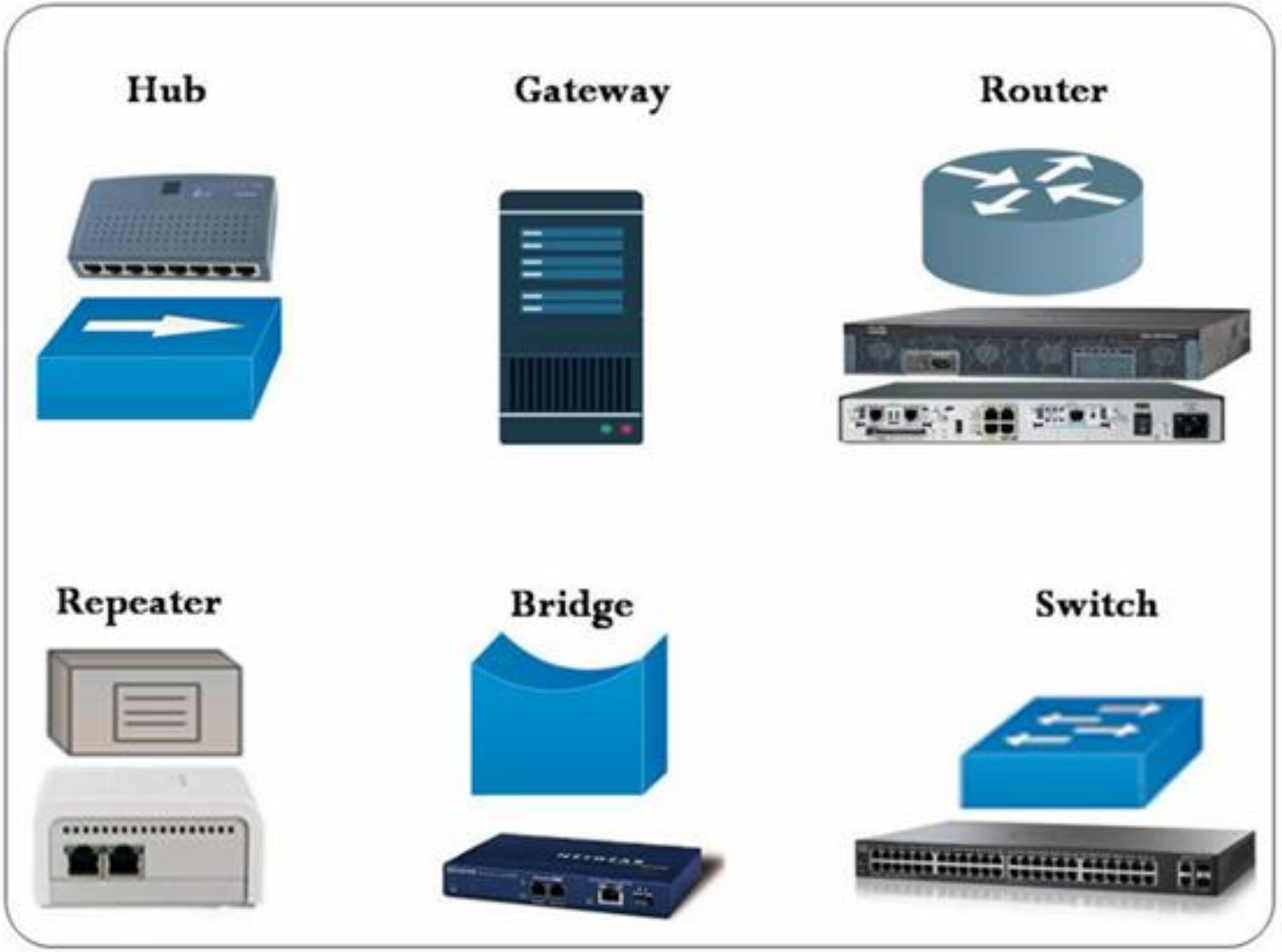
Hybrid Topology





Network Devices (Connecting Devices)

- Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other.
- Network devices like hubs, repeaters, bridges, switches, routers, and gateways help manage and direct data flow in a network.
- They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks.
- Each device serves a specific role, from simple data forwarding to complex routing between networks.

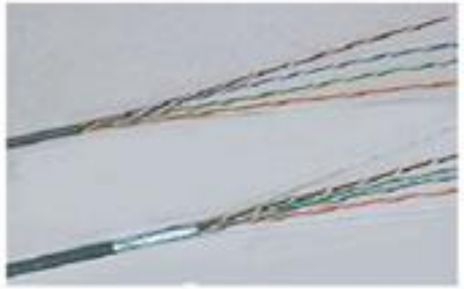

Hub
Gateway
Router
Repeater
Bridge
Switch

Wired and Wireless Networks

- Guided (wired networks) are formed using cables
  - Copper (Twisted Pair)
    - Shielded Twisted Pair (STP)
    - Unshielded Twisted Pair (UTP)
  - Copper (Coaxial)
    - Thicknet
    - Thinnet
  - Fiber
    - Single mode
    - Double mode

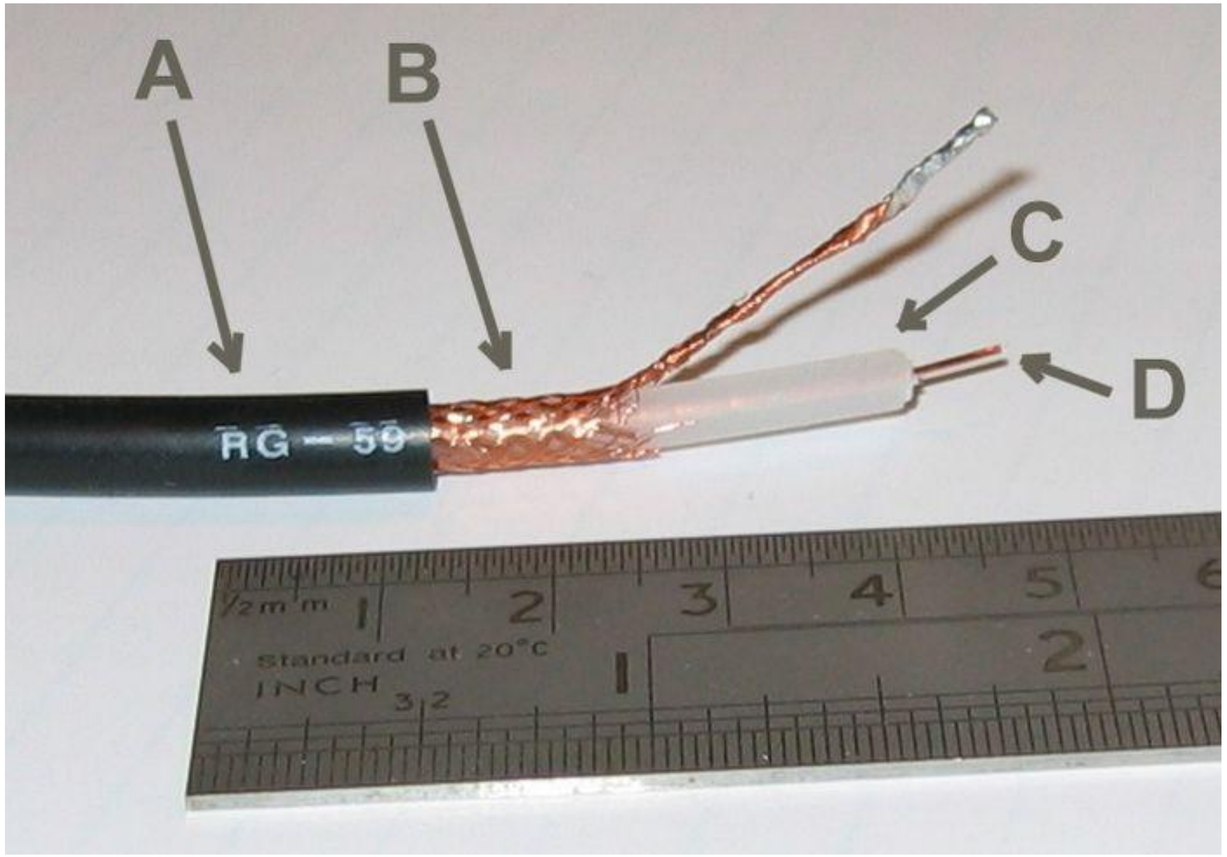
Network Media

Copper



Fiber Optics

Wireless

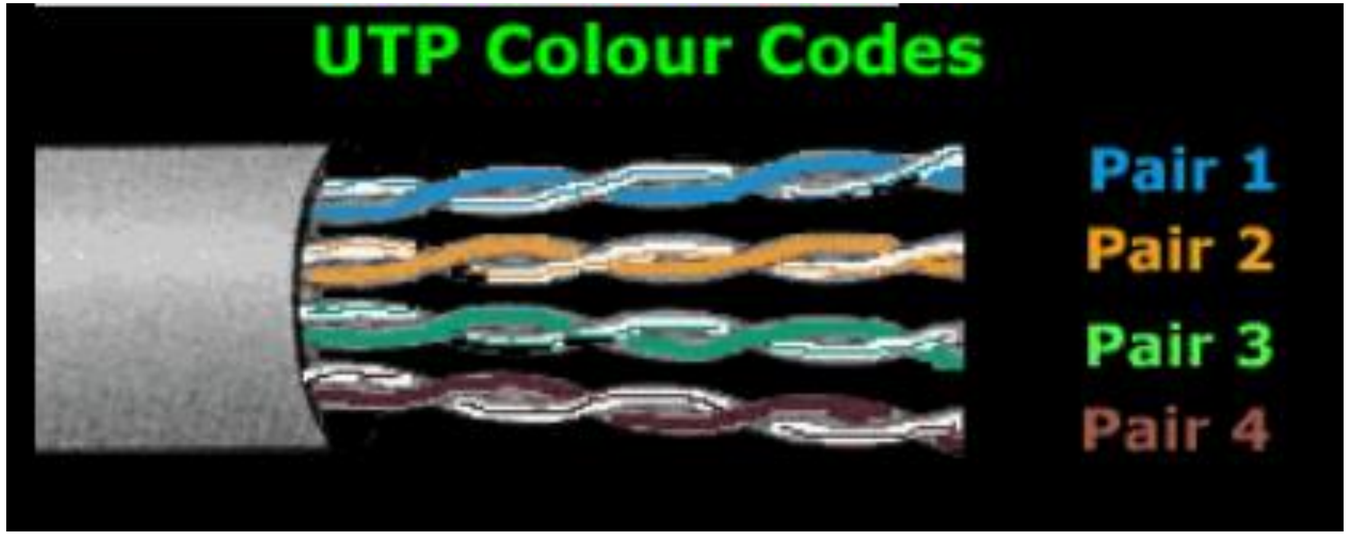


A. Outer plastic sheath

B. Woven copper shield

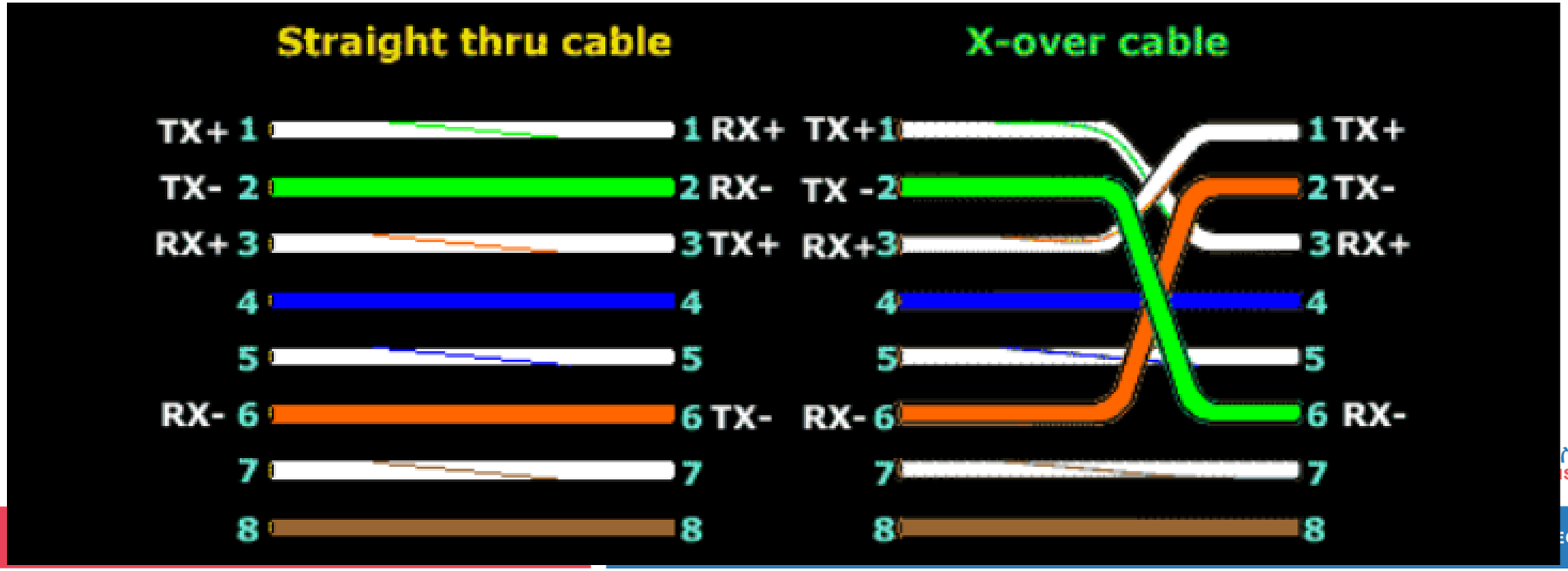
C. Inner dielectric insulator

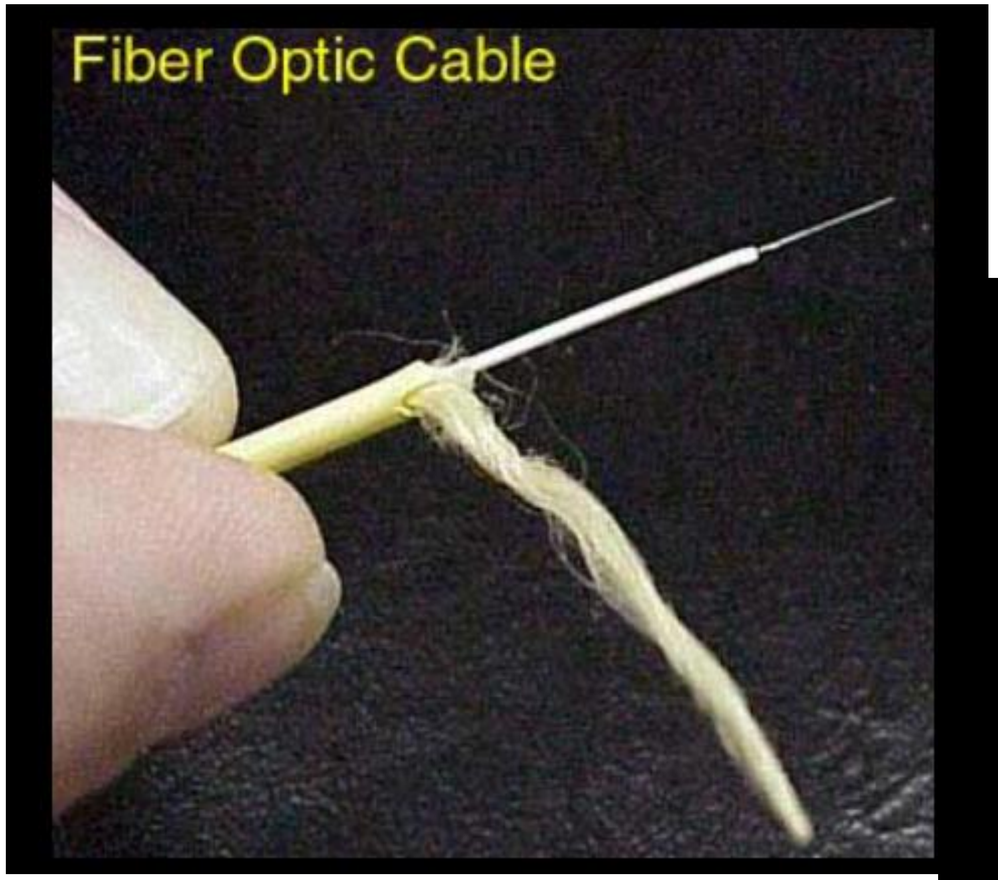
D. Copper core

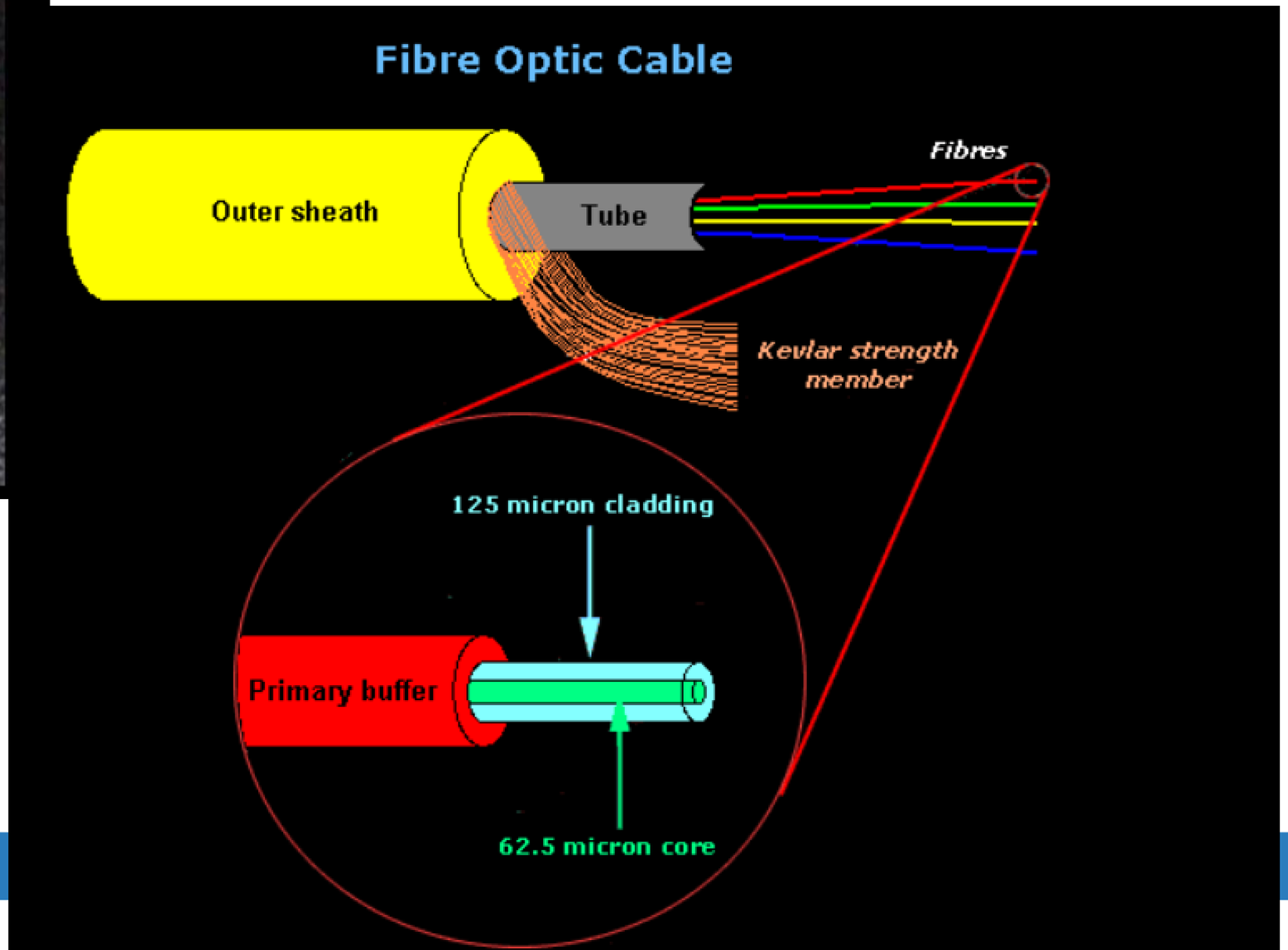

UTP Colour Codes
Pair 1
Pair 2
Pair 3
Pair 4

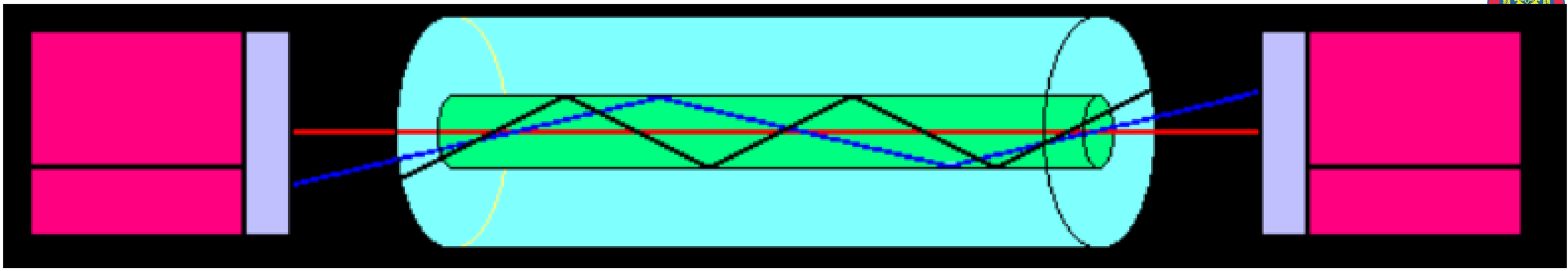
Color Codes for T568A
Pin color - pair name
1 white/green (pair 3) RecvData+
2 green (pair 3) RecvData-
3 white/orange (pair 2) TxData +
4 blue (pair 1)
5 white/blue (pair 1)
6 orange (pair 2) TxData -
7 white/brown (pair 4)
8 brown (pair 4)

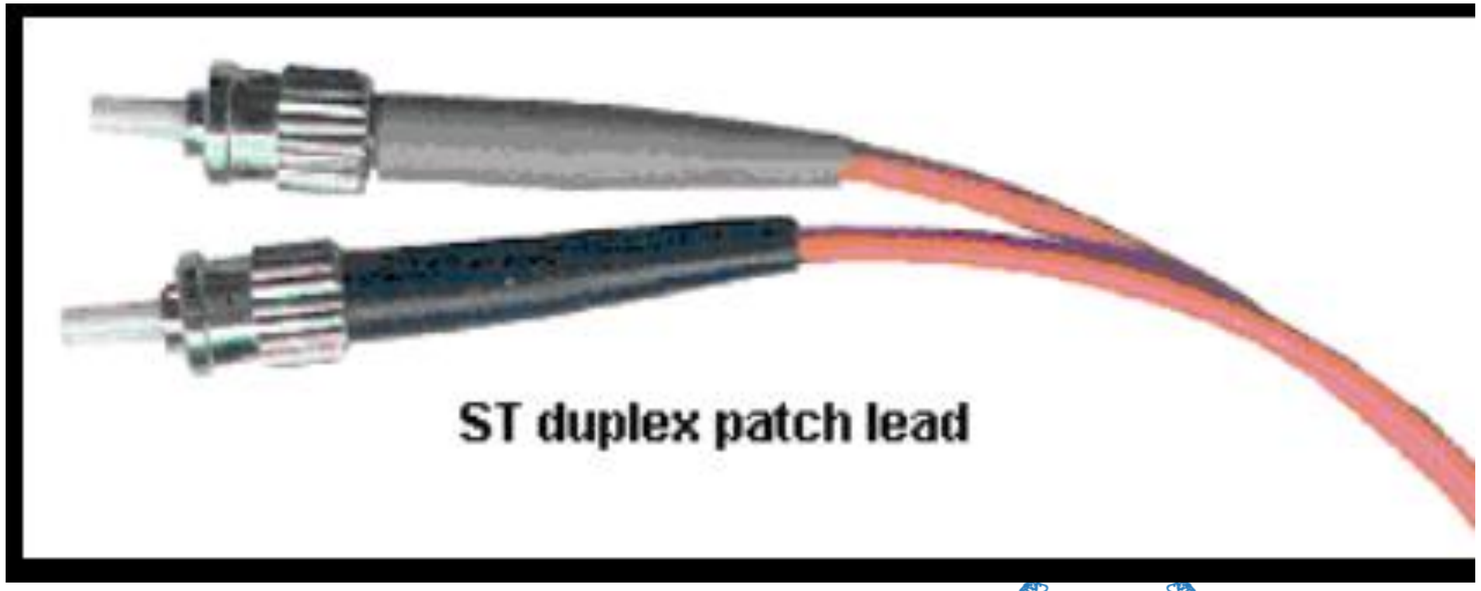
Color Codes for T568B
Pin color - pair name
1 white/orange (pair 2) TxData +
2 orange (pair 2) TxData -
3 white/green (pair 3) RecvData+
4 blue (pair 1)
5 white/blue (pair 1)
6 green (pair 3) RecvData-
7 white/brown (pair 4)
8 brown (pair 4)




Fiber Optic Cable


Fibre Optic Cable
Outer sheath
Tube
Fibres
Kevlar strength member
125 micron cladding
Primary buffer
62.5 micron core




ST duplex patch lead

Images for access point

tp link | wi fi | wifi extender | netgear | wireless router

Feedback

Emerging Network Systems

Home take and class exercises

- What is meant by a signal?
- Write the types of data transmission media and the types of signals they propagate including the types of energy the signals are carried. Write also the encoding systems employed for each of the media described.
- Please note that you send the answers via email (workshet.lamenew@aau.edu.et)
- File name should be “your name, your father’s name and your ID (only the number)
- Write the advantages and disadvantages of network topologies
- Indicate the most popularly used data transmission media based on your practical observation
- Write the types of cables and

3. Network Protocols

- Introduction to Protocols (Syntax, Semantics, Timing)
- The OSI Reference Model
- The TCP/IP Reference Model
- Anatomy of TCP/UDP and IP
- IP Addressing (IPV4 and IPV6)

Introduction to Protocols

- Protocol can be defined as ***language*** that consists of set of ***rules*** (syntax and semantics) that help the communicators ***understand*** each other so that meaningful and successful communication is done.
- ***Network protocol*** is a set of rules that govern data communication between different devices in the network. It determines
  - ***what*** is being communicated,
  - ***how*** it is being communicated (how to format, send and receive data), and
  - ***when*** it is being communicated. It permits connected devices to communicate with each other, ***irrespective*** of internal and structural differences.

Introduction to Protocols

- Network protocols are ***the reason you can easily communicate*** with people all over the world,

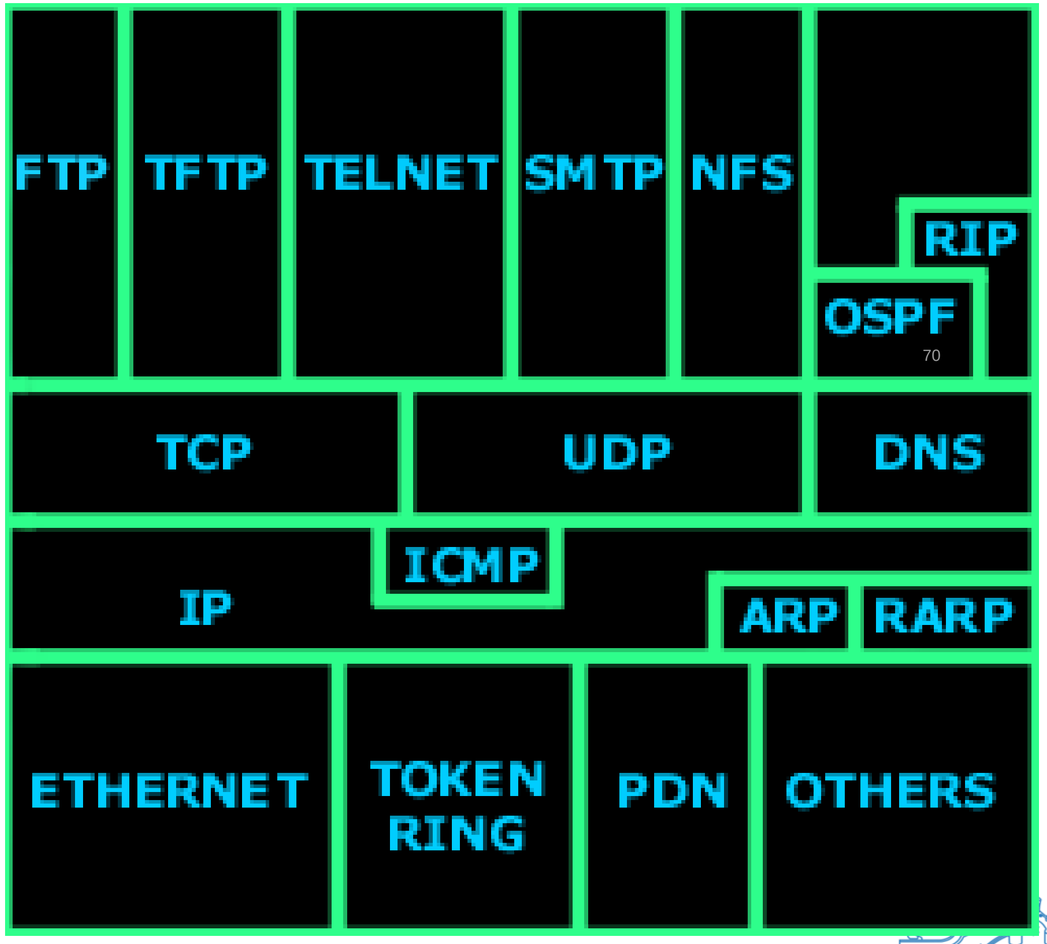
- They play a critical role in modern digital communications.

- Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols.

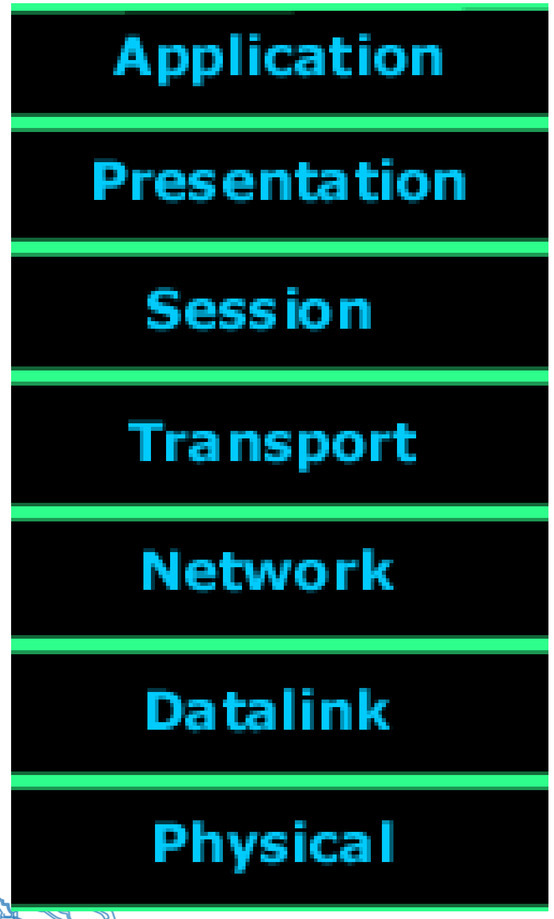
Protocol Layering

- OSI/ISO Reference model
- TCP/IP Reference model

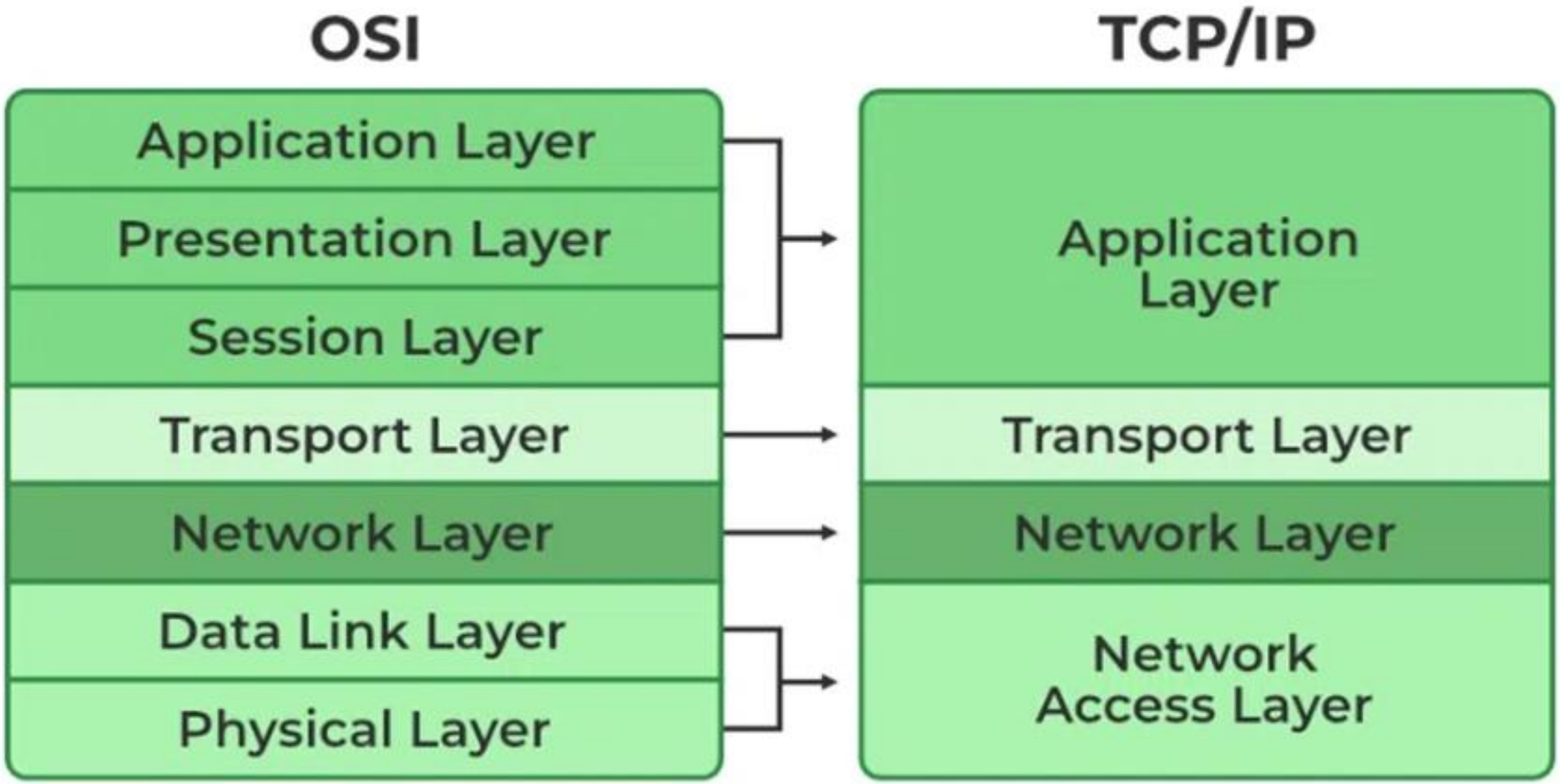
TCP/IP Protocol Stack

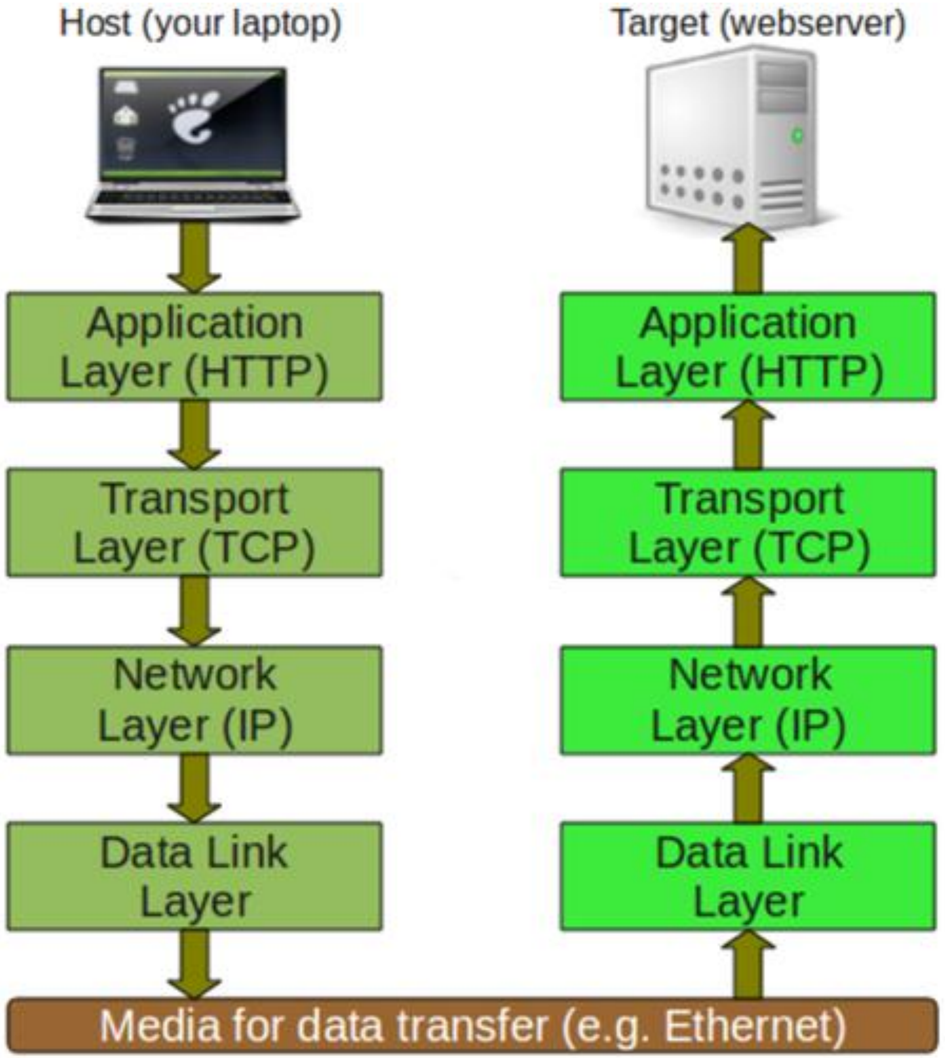


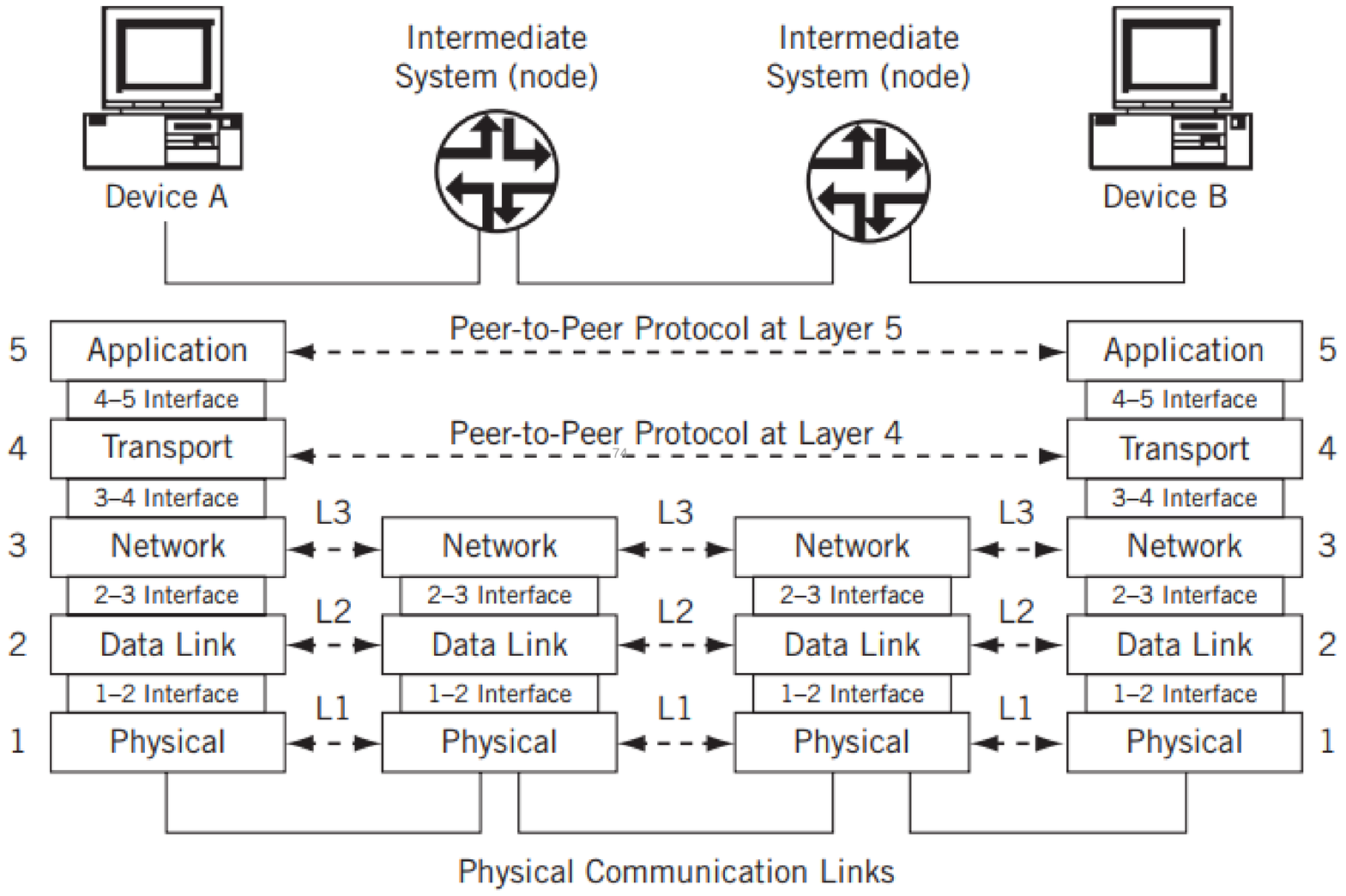
The OSI Model



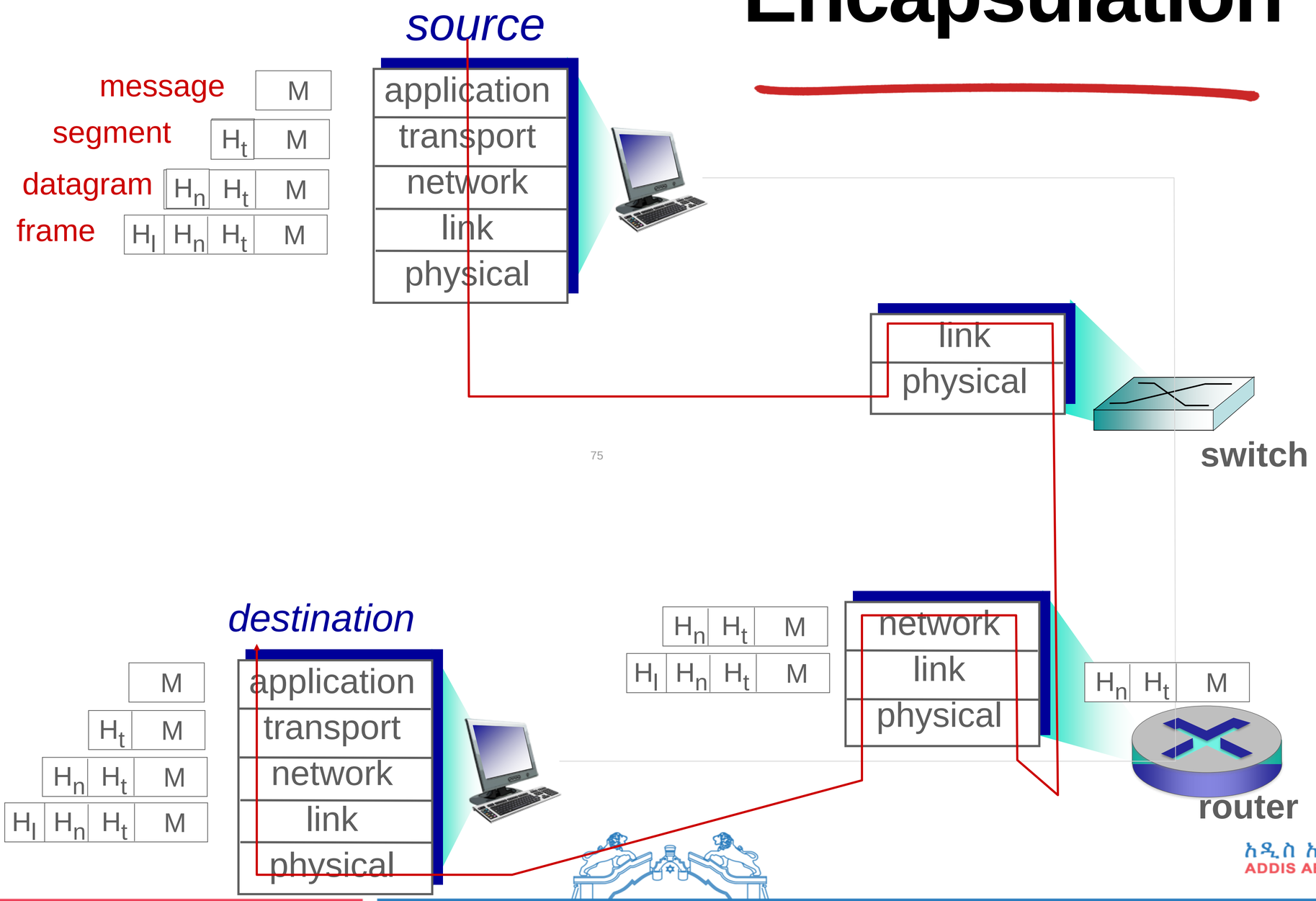
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

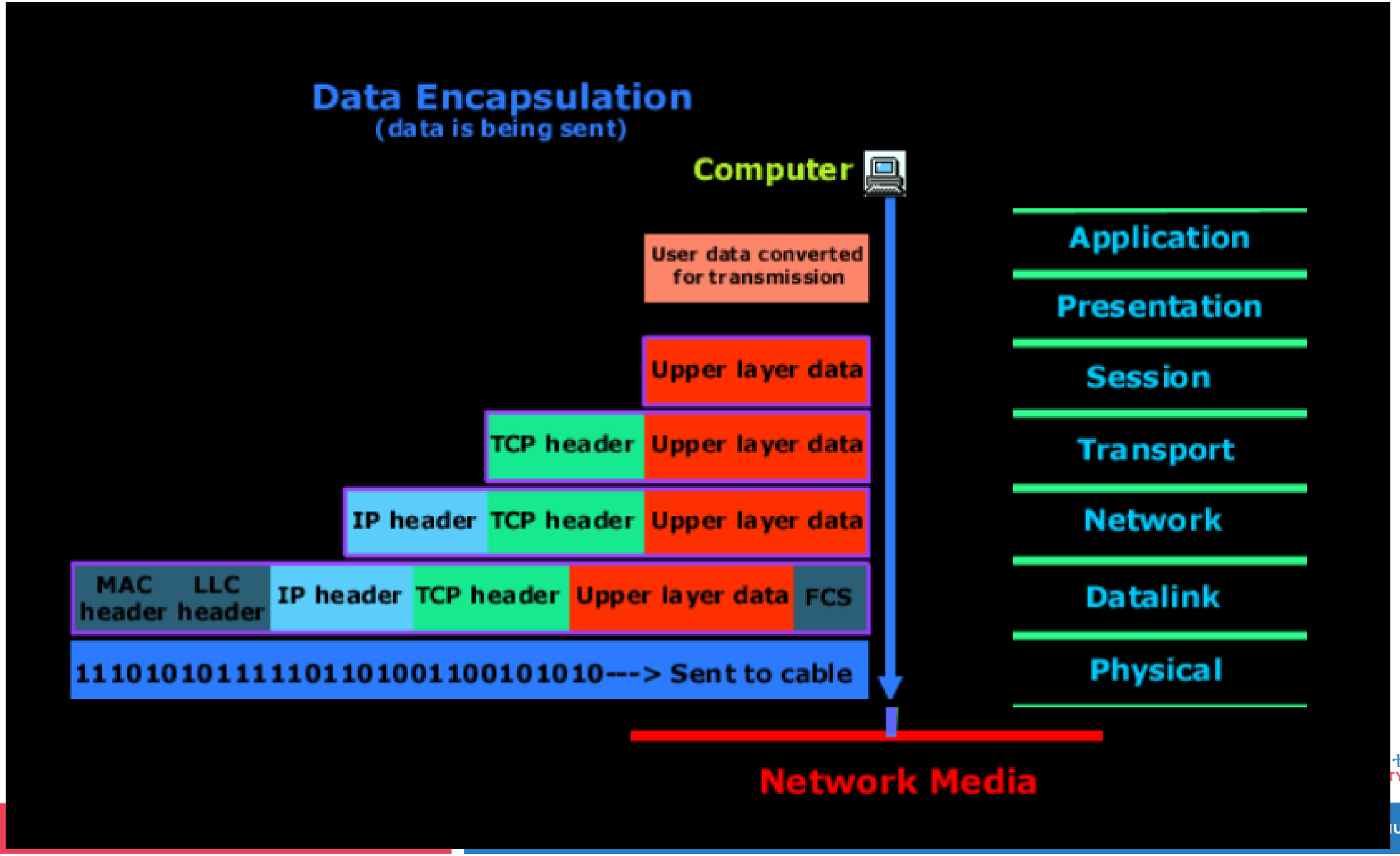

OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

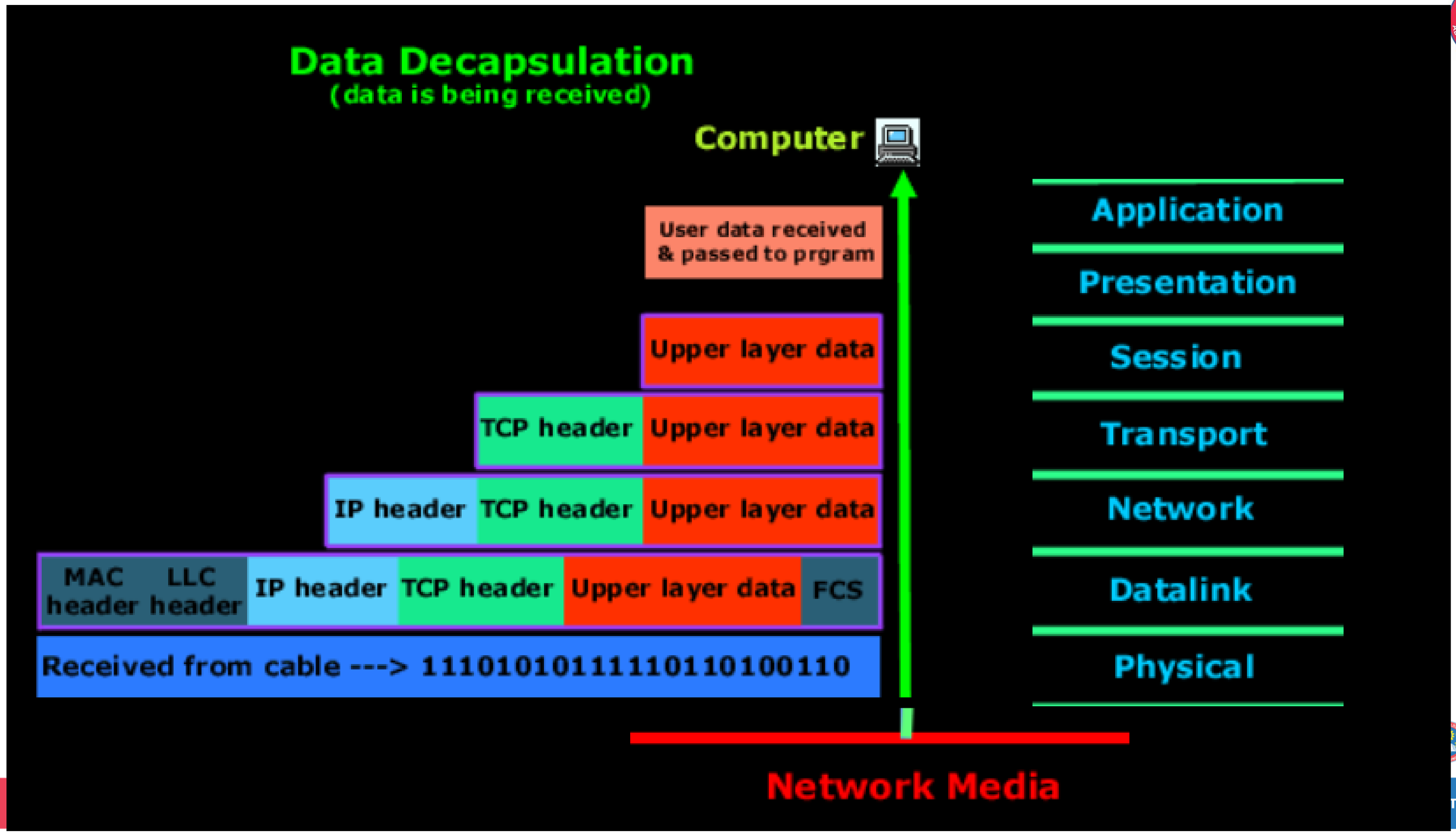

Host (your laptop)
Target (webserver)
Application Layer (HTTP)
Transport Layer (TCP)
Network Layer (IP)
Data Link Layer
Application Layer (HTTP)
Transport Layer (TCP)
Network Layer (IP)
Data Link Layer
Media for data transfer (e.g. Ethernet)

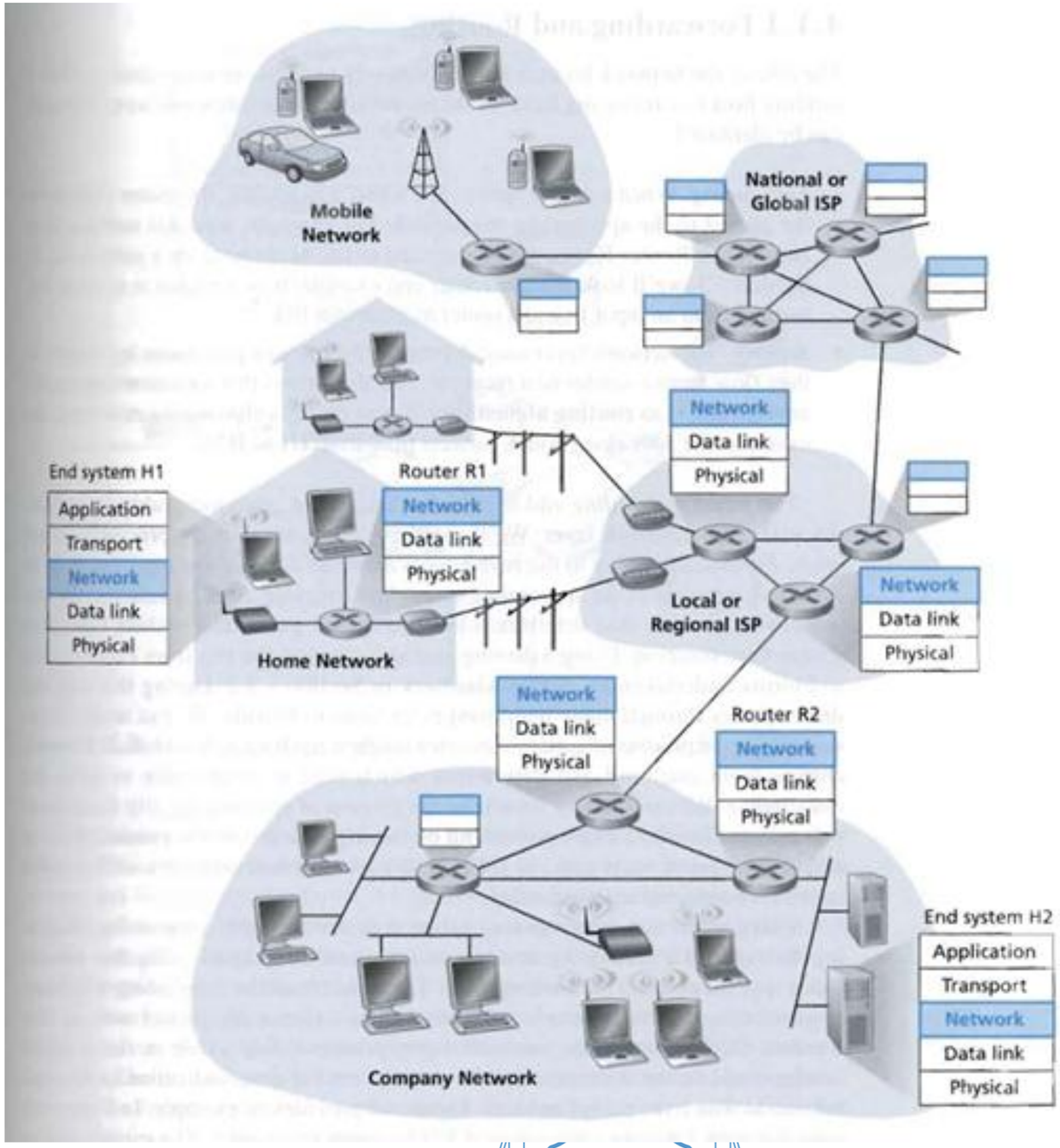

Intermediate System (node)
Intermediate System (node)
Device A
Device B
Peer-to-Peer Protocol at Layer 5
Peer-to-Peer Protocol at Layer 4
5
Application
4–5 Interface
4
Transport
3–4 Interface
3
Network
2–3 Interface
2
Data Link
1–2 Interface
1
Physical
L3
L2
L1
Physical Communication Links

Encapsulation




Data Encapsulation
(data is being sent)
Computer
User data converted for transmission
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
11101010111110110100100101010---> Sent to cable
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media


Data Decapsulation
(data is being received)
Computer
User data received & passed to prgram
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
Received from cable ---> 11101010111110110100110
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media


Mobile Network
National or Global ISP
Network
Data link
Physical
End system H1
Application
Transport
Network
Data link
Physical
Router R1
Network
Data link
Physical
Home Network
Local or Regional ISP
Network
Data link
Physical
Network
Data link
Physical
Router R2
Network
Data link
Physical
End system H2
Application
Transport
Network
Data link
Physical
Company Network

Protocols

- Protocol layering (design issues for layers)
  - Addressing
  - Error control
  - Flow control
  - Disassembling, transmitting, reassembling
  - Multiplexing and demultiplexing
  - Routing

Services, interfaces, protocols

- Connection-oriented service
- Connectionless service

Services, interfaces, protocols

LISTEN

CONNECT

RECEIVE

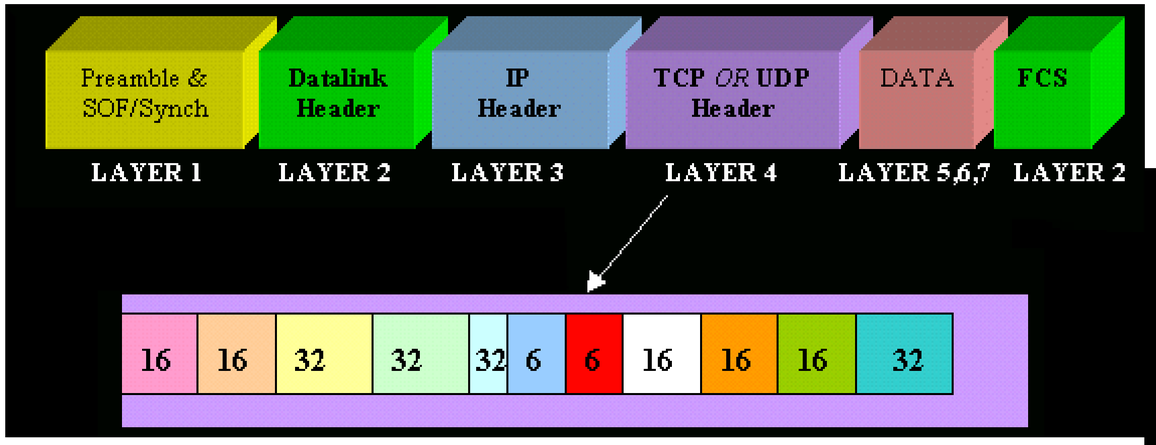
SEND

DISCONNECT

Anatomy of TCP/IP Protocols

- Transport Layer protocols
  - Connection oriented (TCP)
  - Connectionless (UDP)

- Internet Protocol (IP)



TCP Header

16 Source Port: Specifies the port on the sending TCP module.

16 Destination Port: Specifies the port on the receiving TCP module.

32 Sequence Number: Ensure correct sequencing of data packets . Local

32 Ack Number: Next expected TCP octet

32 HLEN: length of this layers packet

6 Reserved

6 Code Bits: Control functions, **FIN, SYN, RST, ACK, PSH, URG**

16 Windows Size: Number of octets that the sender is willing to accept

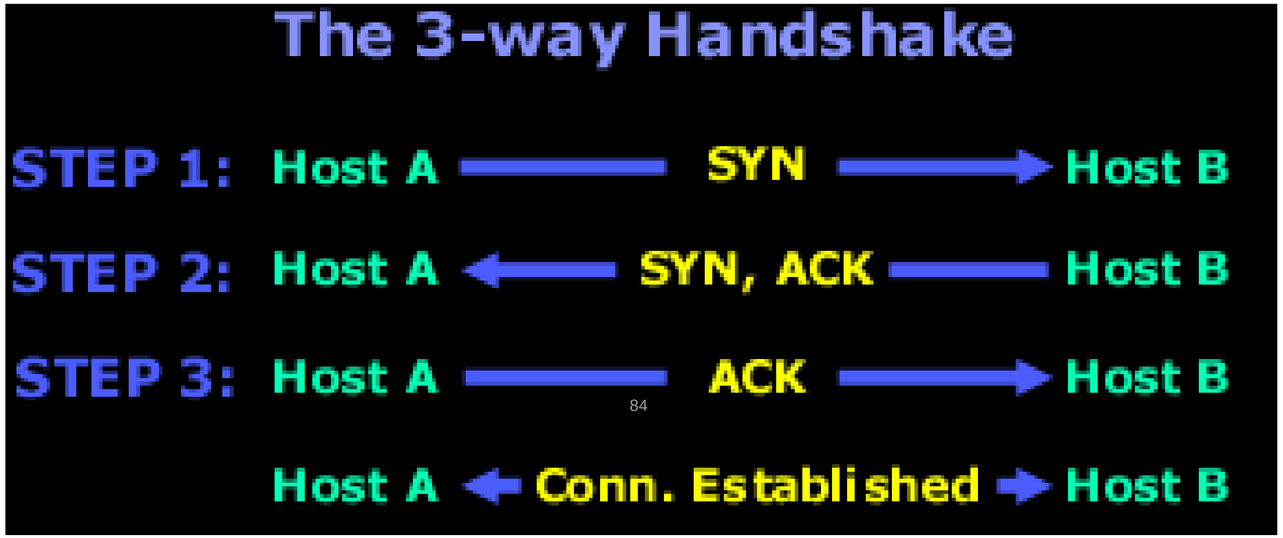
16 Checksum: TCP header checksum. (everything in the tcp packet)

16 Urgent Pointer: Indicates the end of the urgent data

32 Options: Max. TCP segment

The lengths in the diagram are in Bits, unless specified.
Note that 8 Bits = 1 Byte

The following diagram explains the basic function of the 3-way handshake:



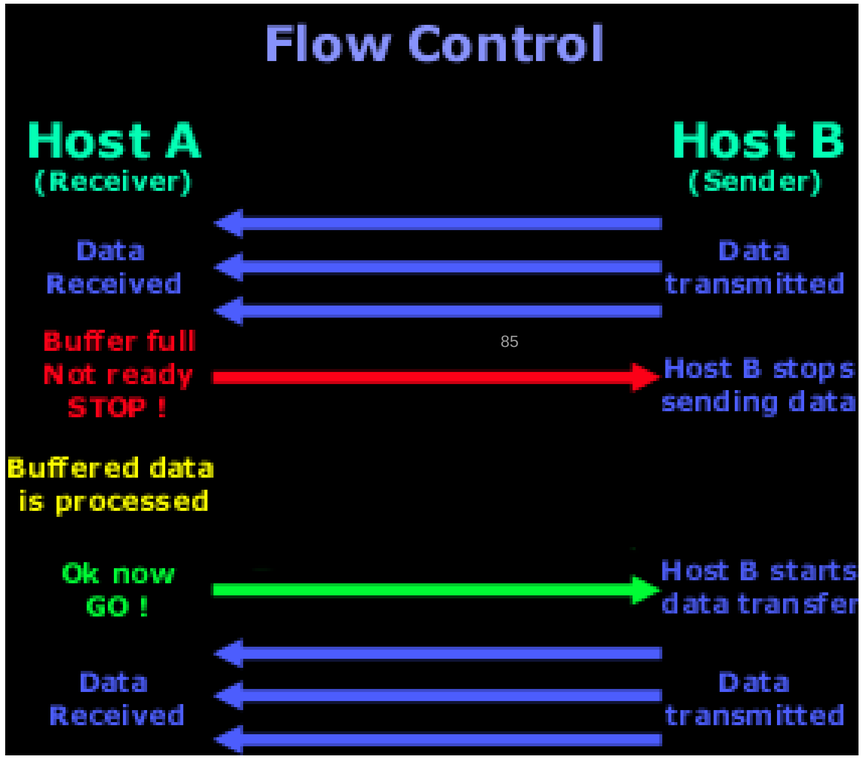
STEP 1: Host A sends a packet to Host B. This packet has the "SYN" bit enabled and when Host B receives it and reads the packet, it sees the "SYN" bit which has a value of "1" (in binary, this means ON) so it knows that Host A is trying to synchronise with it.

STEP 2: Host B then sends a packet back to Host A and within this packet, the "SYN and ACK" bits are enabled (value =1). The SYN that Host B sends means 'I want to synchronise with you' and the ACK means 'I acknowlege your previous SYN request'.

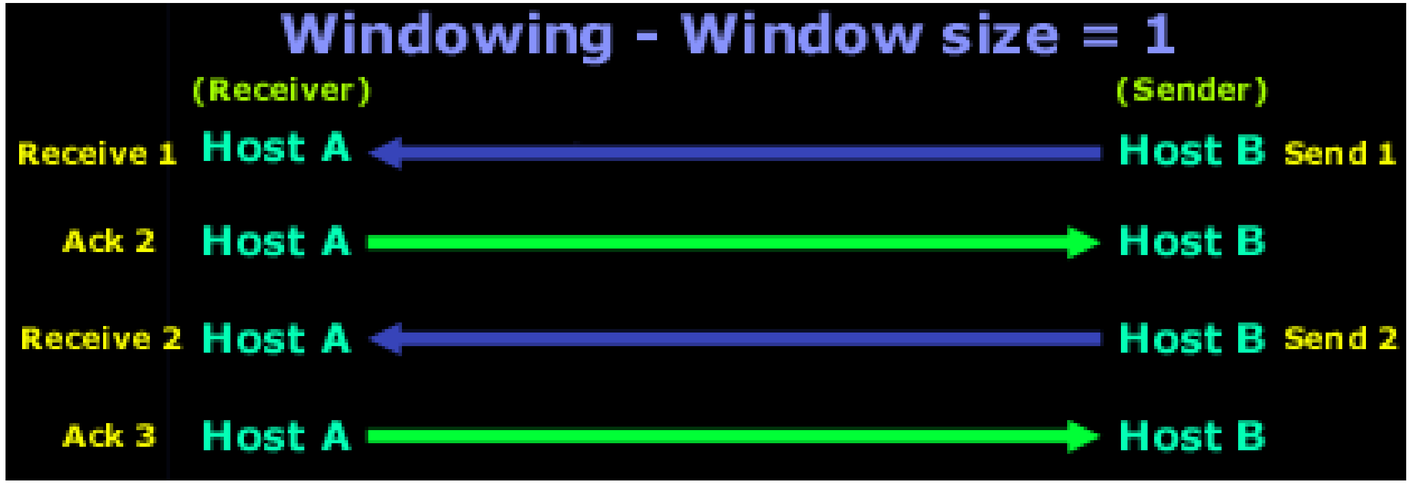
STEP 3: So... after all that, Host A sends another packet to Host B and has the "ACK" bit set to 1, which tells Host B 'Yes, I acknowlege your previous request'.

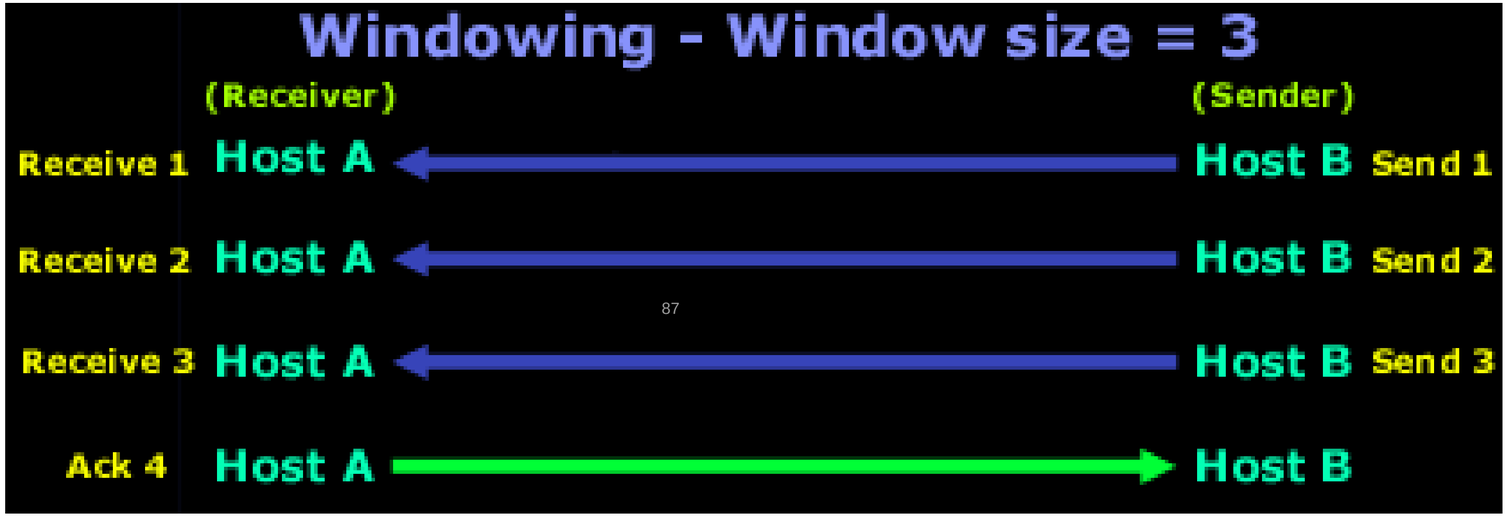
And after all that, the connection is established (virtual circuit) and the data transfer begins, and should end without any errors!

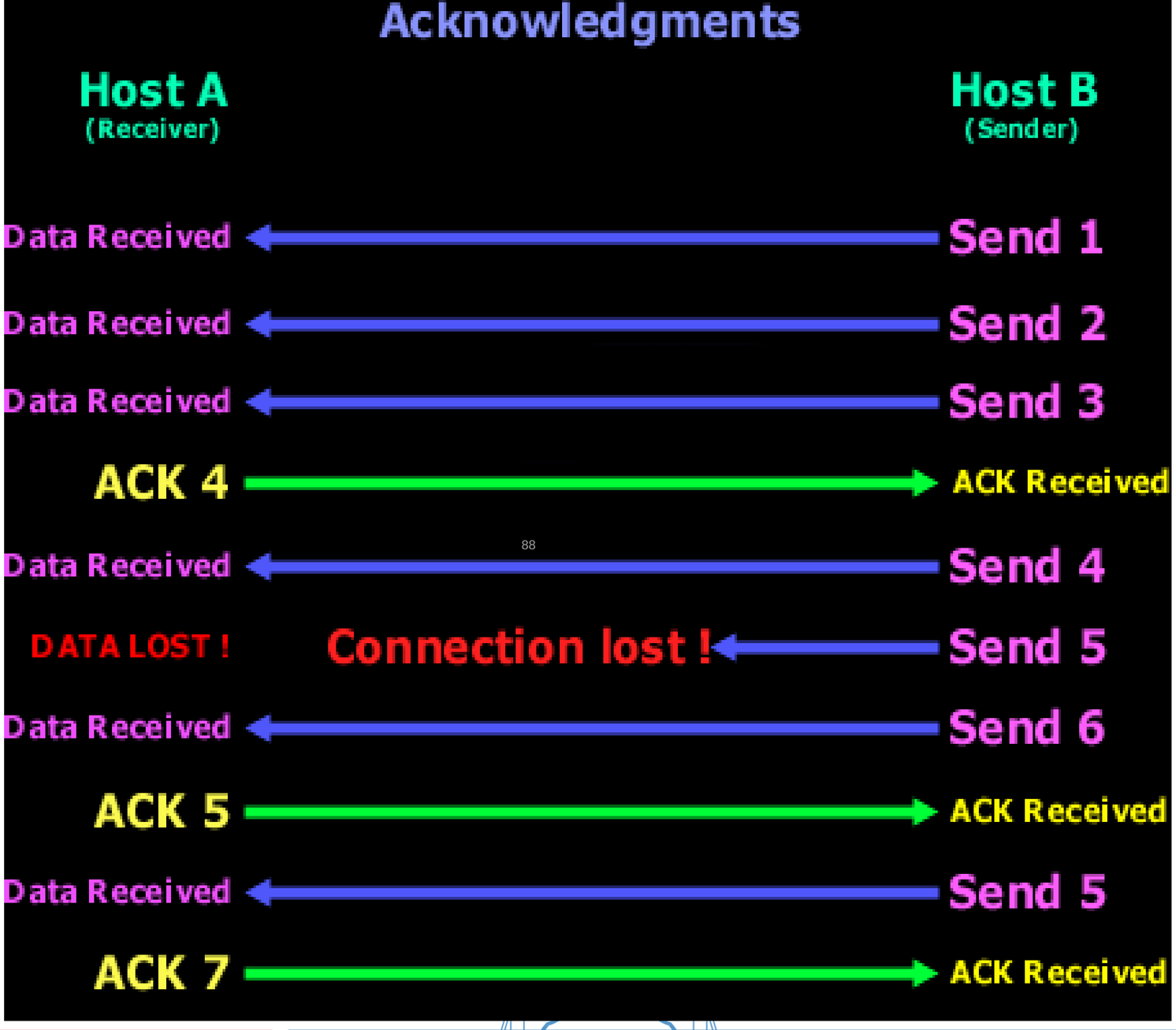
Below is a diagram which will help you understand all this jargon about flow control :



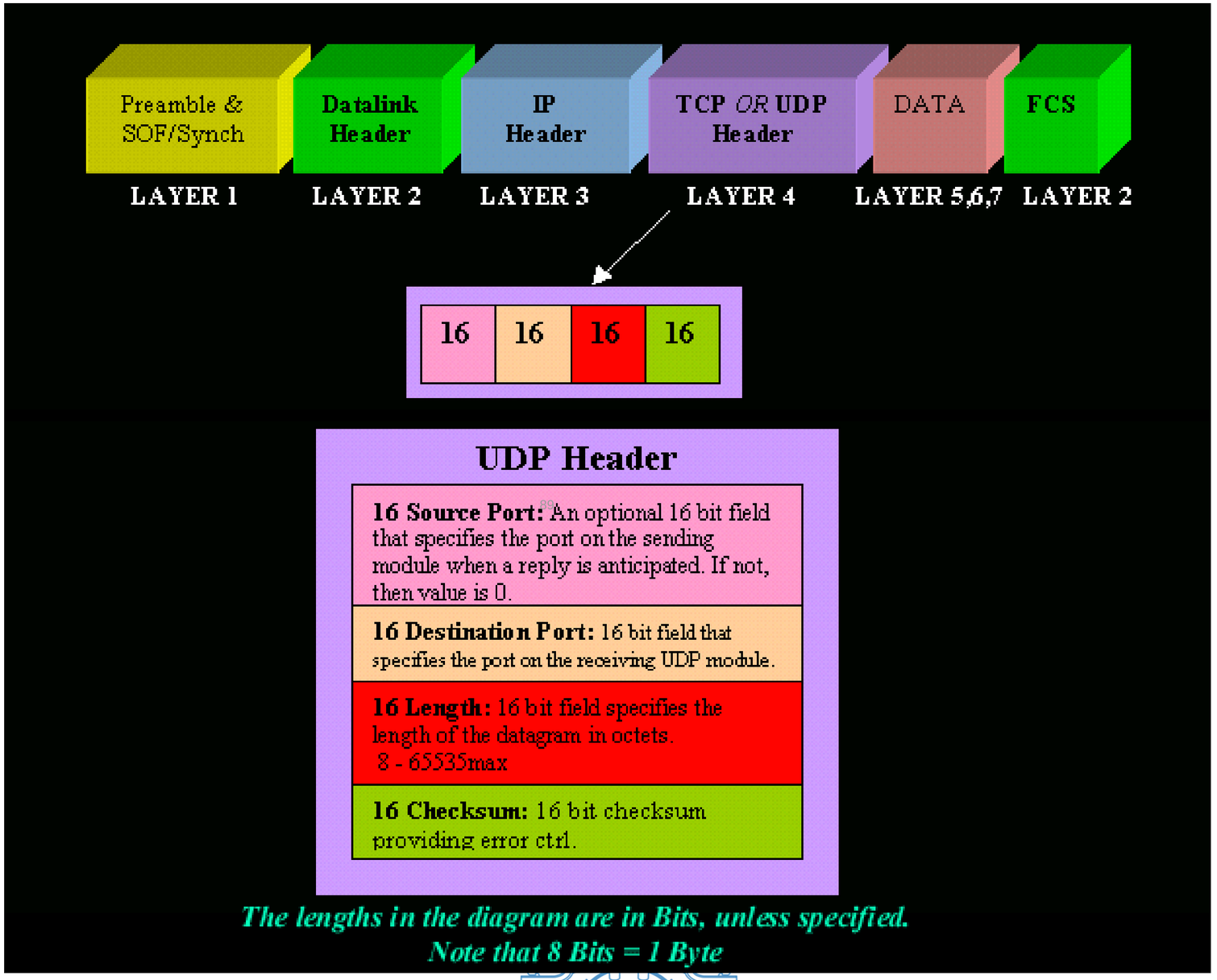
Windowing controls how much information is transferred from one end to the other. While some protocols quantify information by observing the number of packets, TCP/IP measures it by counting the number of bytes.



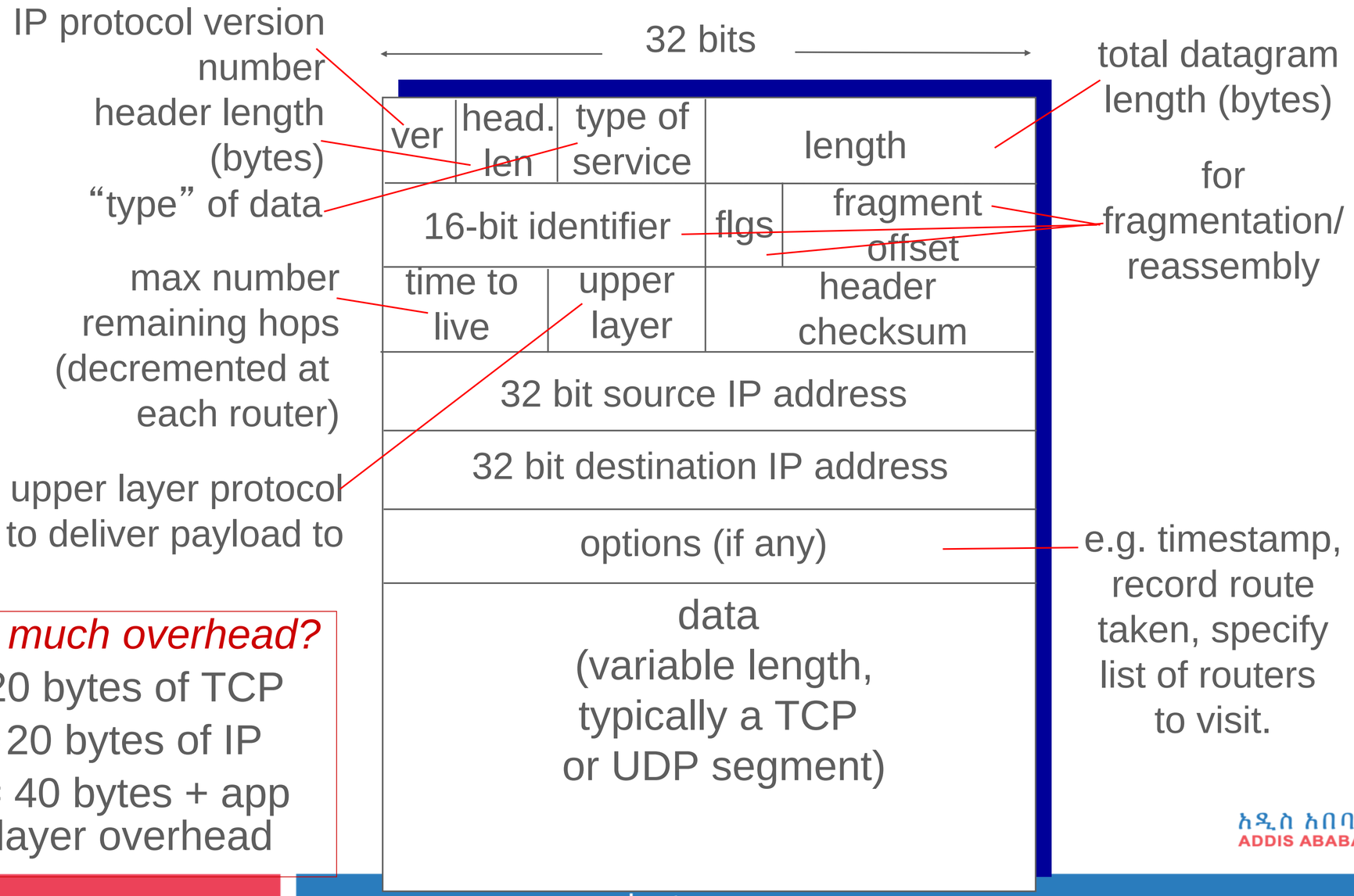

Windowing - Window size = 3
(Receiver)
(Sender)
Receive 1
Host A
Host B
Send 1
Receive 2
Host A
Host B
Send 2
87
Receive 3
Host A
Host B
Send 3
Ack 4
Host A
Host B


Acknowledgments
Host A
(Receiver)
Host B
(Sender)
Data Received
Send 1
Data Received
Send 2
Data Received
Send 3
ACK 4
ACK Received
88
Data Received
Send 4
DATA LOST !
Connection lost !
Send 5
Data Received
Send 6
ACK 5
ACK Received
Data Received
Send 5
ACK 7
ACK Received

UDP


Preamble & SOF/Synch
Datalink Header
IP Header
TCP OR UDP Header
DATA
FCS
LAYER 1
LAYER 2
LAYER 3
LAYER 4
LAYER 5,6,7
LAYER 2
16
16
16
16
UDP Header
16 Source Port: An optional 16 bit field that specifies the port on the sending module when a reply is anticipated. If not, then value is 0.
16 Destination Port: 16 bit field that specifies the port on the receiving UDP module.
16 Length: 16 bit field specifies the length of the datagram in octets. 8 - 65535max
16 Checksum: 16 bit checksum providing error ctrl.
The lengths in the diagram are in Bits, unless specified.
Note that 8 Bits = 1 Byte

IP datagram format



how much overhead?

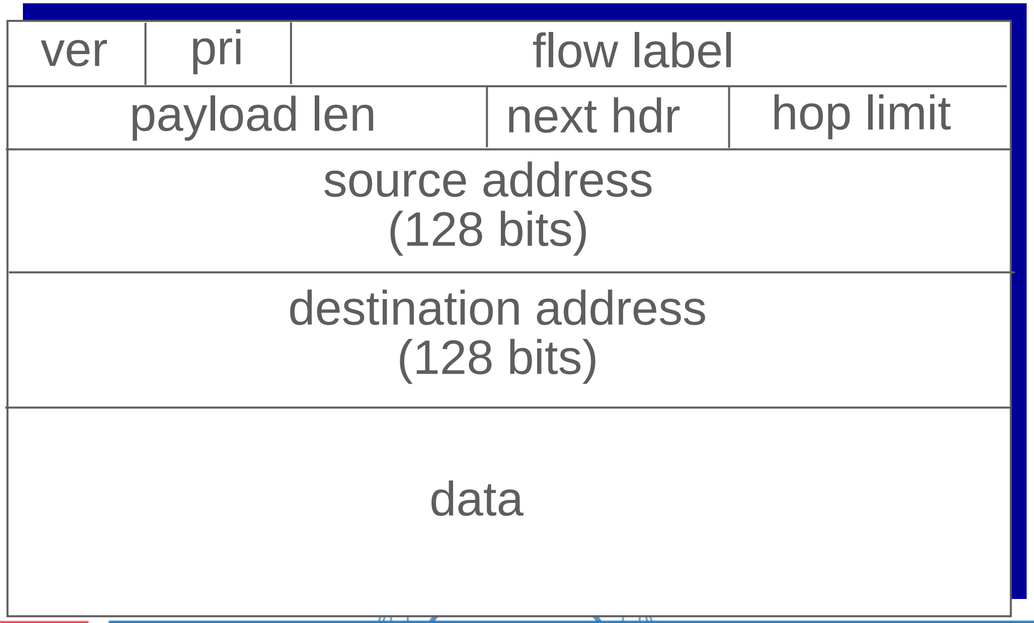
- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

IPv6 datagram format

priority: identify priority among datagrams in flow

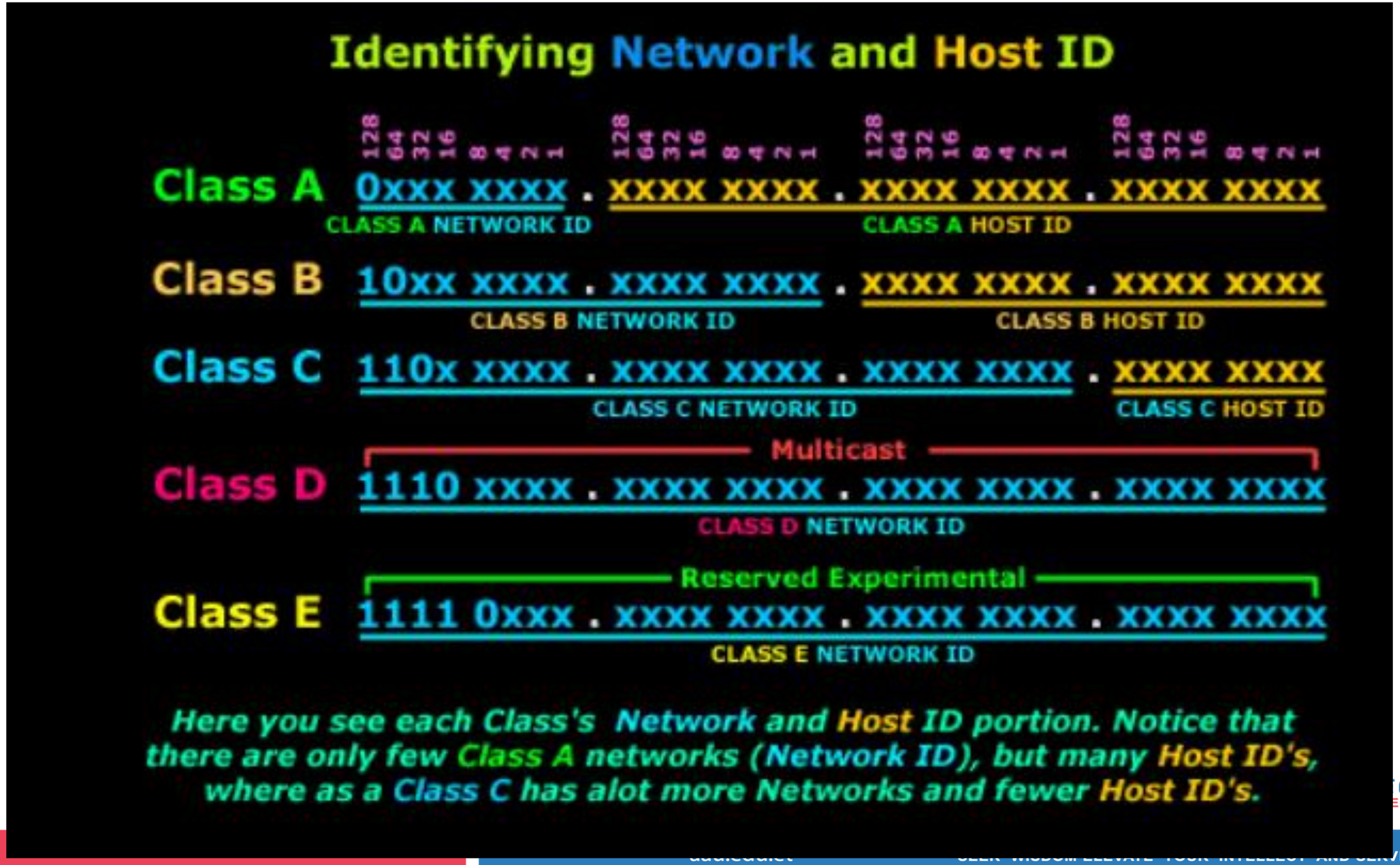
flow Label: identify datagrams in same "flow." (concept of"flow" not well defined).

next header: identify upper layer protocol for data



IP Address

- MAC address is flat and portable
- IP address is hierarchical and routable
- 32 bit addresses
- Class A, B, C, D, E, and default subnetmask
- Subnetting
  - Classfull and classless
  - Variable length subnetmask (VLSM)
- Supernetting


Identifying Network and Host ID
128 64 32 16 8 4 2 1
Class A
0xxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS A NETWORK ID
CLASS A HOST ID
Class B
10xx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS B NETWORK ID
CLASS B HOST ID
Class C
110x xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS C NETWORK ID
CLASS C HOST ID
Multicast
Class D
1110 xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS D NETWORK ID
Reserved Experimental
Class E
1111 0xxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
CLASS E NETWORK ID
Here you see each Class's Network and Host ID portion. Notice that there are only few Class A networks (Network ID), but many Host ID's, where as a Class C has alot more Networks and fewer Host ID's.

The 5 Different Classes Of IP Address

Class A : 1.0.0.0 to 127.255.255.255

Class B : 128.0.0.0 to 191.255.255.255

Class C : 192.0.0.0 to 223.255.255.255

Class D : 224.0.0.0 to 239.255.255.255

Class E : 240.0.0.0 to 255.255.255.255

The IP Classes listed above are not all usable by hosts!
Here we are simply looking at the range each Class covers

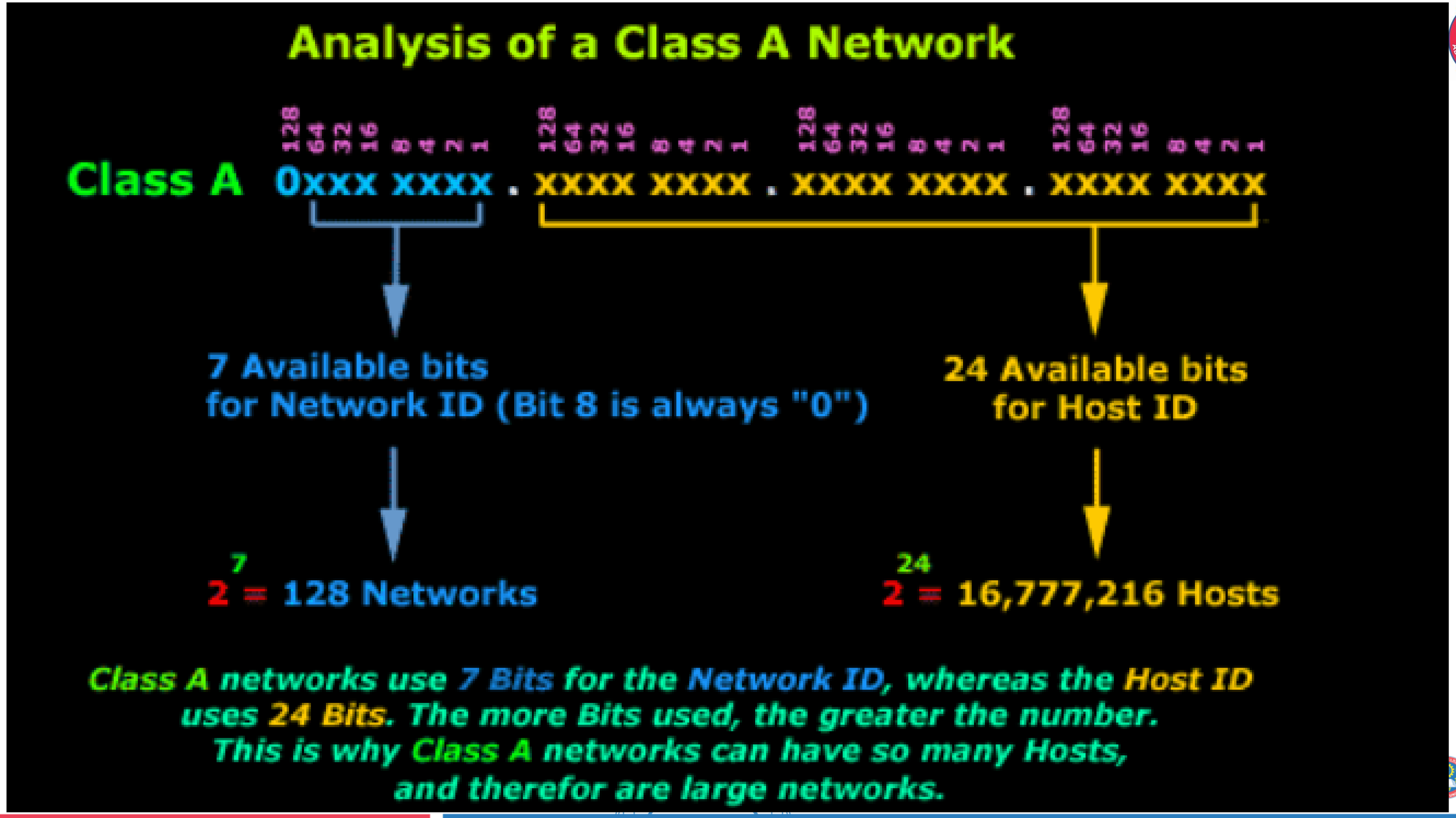
Network Classes with their respective Default Subnet Masks

CLASS TYPE	NETWORK RANGE	DEFAULT SUBNET MASK
Class A	1.0.0.0 to 127.255.255.255	255.0.0.0
Class B	128.0.0.0 to 191.255.255.255	255.255.0.0
Class C	192.0.0.0 to 223.255.255.255	255.255.255.0

Here you can see each Network Class with its range of IP Addresses followed by the default subnet mask for the particular Class. Remmeber that we can modify the default subnet mask to meet our needs

IP Configuration on hosts

- IP address
- Subnetmask
- Default gateway
- DNS


Analysis of a Class A Network
128 64 32 16 8 4 2 1
Class A 0xxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
7 Available bits
for Network ID (Bit 8 is always "0")
24 Available bits
for Host ID
2^7 = 128 Networks
2^24 = 16,777,216 Hosts
Class A networks use 7 Bits for the Network ID, whereas the Host ID
uses 24 Bits. The more Bits used, the greater the number.
This is why Class A networks can have so many Hosts,
and therefor are large networks.

Analysis of a Class C Network

Class C networks use 21 Bits for the Network ID and 8 Bits for the Host ID. This is why Class C networks have a large number of networks but with only 256 hosts per network

Subnetting

- In order to subnet a network, **extend** the subnet mask using some of **the bits from the host ID portion** of the address to create a subnetwork ID (address).
- Subnetting allows you to create **multiple logical networks (subnets)** that exist within a single Class A, B, or C network.
- ***If you do not subnet***, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

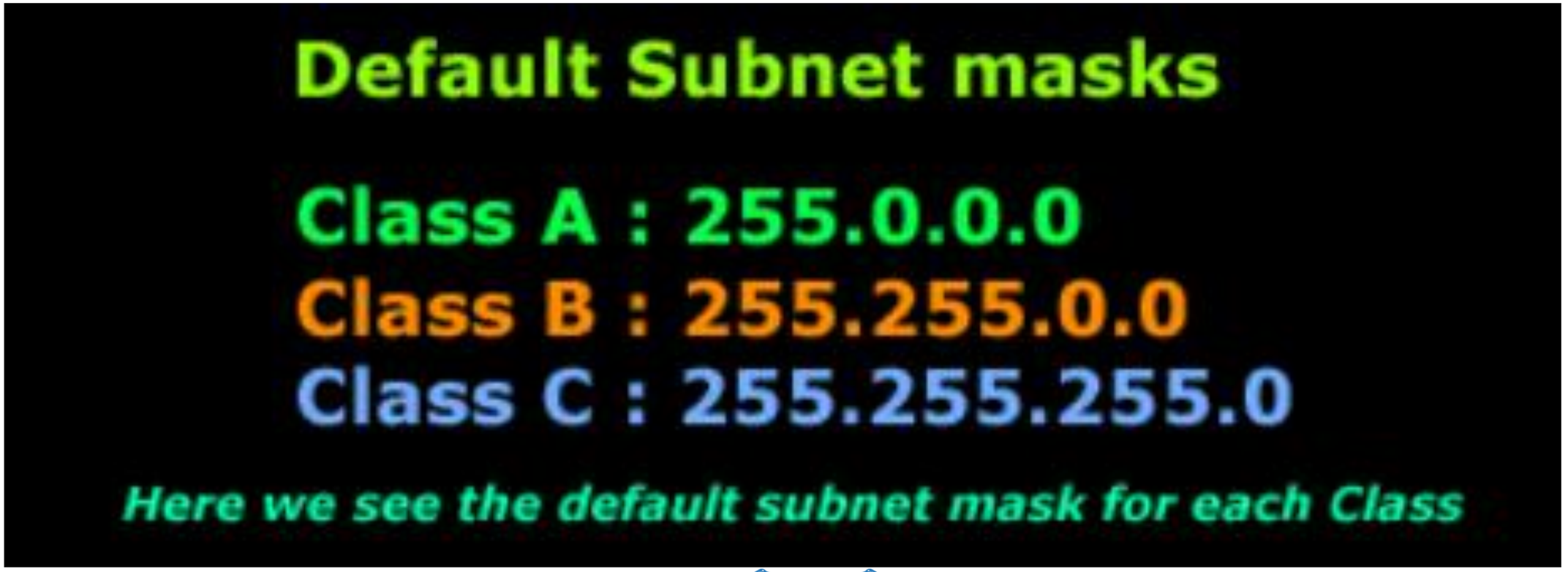
Subnetting

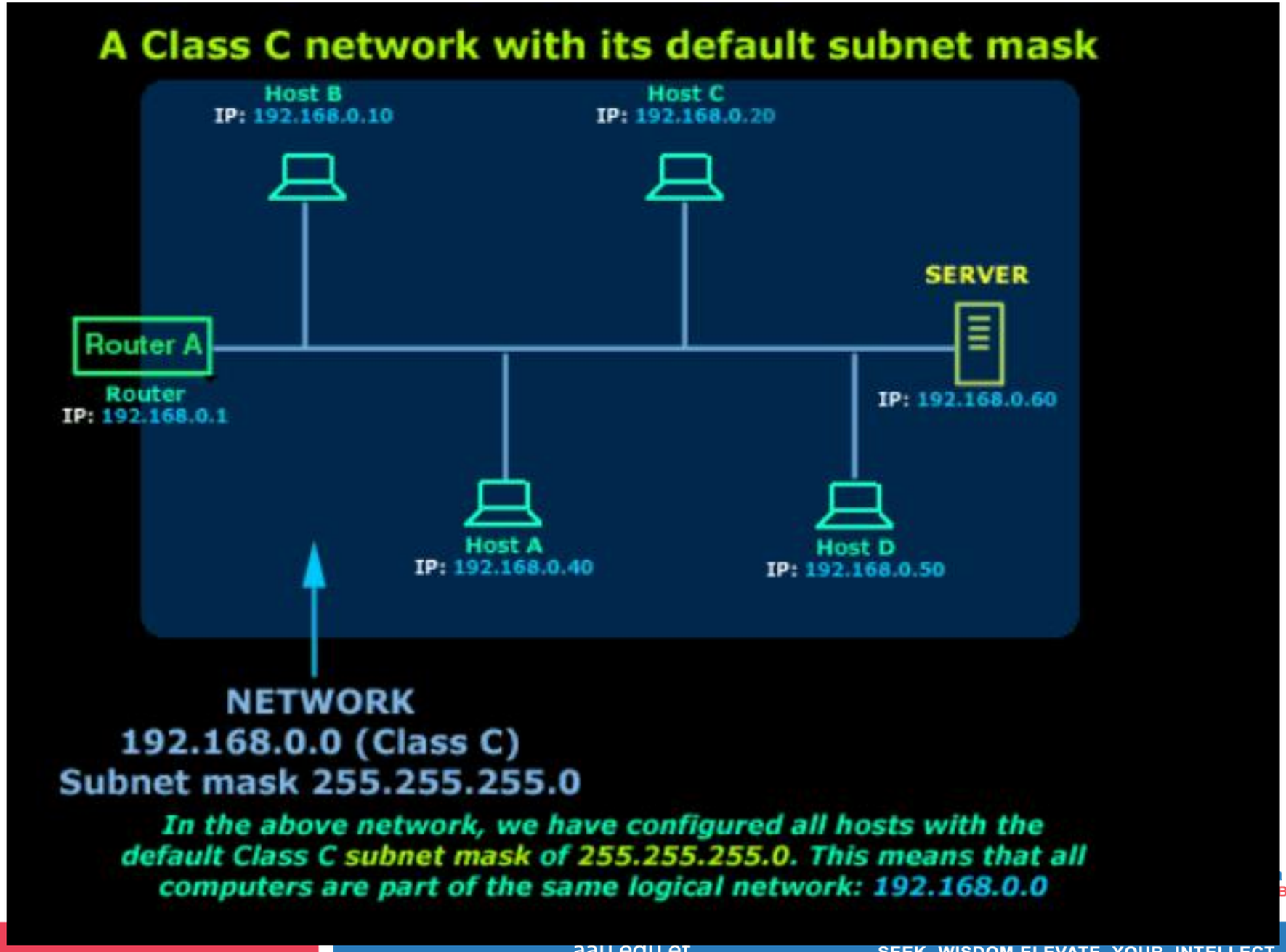
- Subnets are connected to the rest of the network through address-resolving devices called routers.
- Subnets can be freely assigned within the organization
  - Internally, subnets are treated as separate networks
  - Subnet structure is not visible outside the organization

Advantages of Subnetting

- Improves efficiency of IP addresses by not consuming an entire address space for each physical network.
- Reduced network traffic and optimized network performance
- Simplified management

Subnetting


Default Subnet masks
Class A : 255.0.0.0
Class B : 255.255.0.0
Class C : 255.255.255.0
Here we see the default subnet mask for each Class


A Class C network with its default subnet mask
Host B
IP: 192.168.0.10
Host C
IP: 192.168.0.20
SERVER
Router A
Router
IP: 192.168.0.1
IP: 192.168.0.60
Host A
IP: 192.168.0.40
Host D
IP: 192.168.0.50
NETWORK
192.168.0.0 (Class C)
Subnet mask 255.255.255.0
In the above network, we have configured all hosts with the default Class C subnet mask of 255.255.255.0. This means that all computers are part of the same logical network: 192.168.0.0

Home take and class exercises

1. show with diagram the three way handshaking at time of connection establishment. Which transport protocol is used for such purpose.

2. Assume there are 5 networks in an organization each consisting of a maximum number of 50, 24, 16, 5 and 3 computers respectively. You are given IP address 192.168.1.0/24. Using VLSM subnetting allocate IP addresses for each network. Determine also the network, broadcast, subnetmask and default gateway addresses for each network.

Home take and class exercises

1. A given organization needs to establish independent networks for its 10 branches. Assume it has been decided to use two class C IP addresses 200.200.22.0/24 and one 200.200.33.0/24. Use VLSM (Variable Length Subnetmask) to subnet and allocate IP addresses for all branches.

Branch name	Maximum number of computers
Branch 1	49
Branch 2	58
Branch 3	42
Branch 4	119
Branch 5	37
Branch 6	25
Branch 7	3
Branch 8	4
Branch 9	5
Branch 10	5

Cont …

At the same time assume it has been decided that branch 1 and branch 2, are to be connected with a router, say Router 1, and branch 3 and branch 4 are to be connected with a router, say Router 2, etc. as indicated below.

Router 1 connects branch 1 and branch 2, Router 2 connects branch 3 and branch 4, Router 3 connects branch 5 and branch 6, Router 4 connects branch 7 and branch 8, Router 5 connects branch 9 and branch 10

In addition Router 1 is supposed to be connected with Router 2 and Router 3. Router 2 is also supposed to be connected to Router 4, while Router 3 is to be connected to Router 5. Finally Router 4 is required to be connected to Router 5. Allocation of IP addresses to the connections between the routers is mandatory. You are now requested to do so.

a. Draw a diagram that shows all the networks and the interfaces of the routers.

b. Write for all networks the network, broadcast, subnetmask addresses.

c. Assume RIP is configured on all routers. Write the routing table formed at Router 1 after convergence.

4. Internetworking

- Introduction to Internetworking
- Introduction to Routing
- Routing Protocols
  - Interior Gateway Routing Protocols
  - Border Gateway Routing Protocols
- VLAN and Inter VLAN Routing
- Software Defined Networks

Internetworking

- What is a network?
- Internetworking
- The Internet

- Compare and contrast switching and routing
- Explain the process of routing

Switching & Routing

- *Similarity:*
  - *they are both store-and-forward devices.*
- *Differences:*
  - *routers are network layer (or layer-3) devices whereas switches are link layer (or layer-2) devices;*
  - *routers forward packets using network-layer (IP) addresses but switches forward packets (frames) using MAC addresses;*
  - *routers maintain routing tables by implementing routing algorithms whereas switches maintain switch tables, implement filtering, and learning algorithms.*

Routing

- Routing is used for taking a packet (data) from one device and sending it through the network to another device on a different network.
- To be able to route packets, a router must know the following :
  - Destination address
  - Neighbor routers from which it can lean about remote networks
  - Possible routes to all remote networks
  - The best route to each remote network
  - How to maintain and verify routing information

Routing

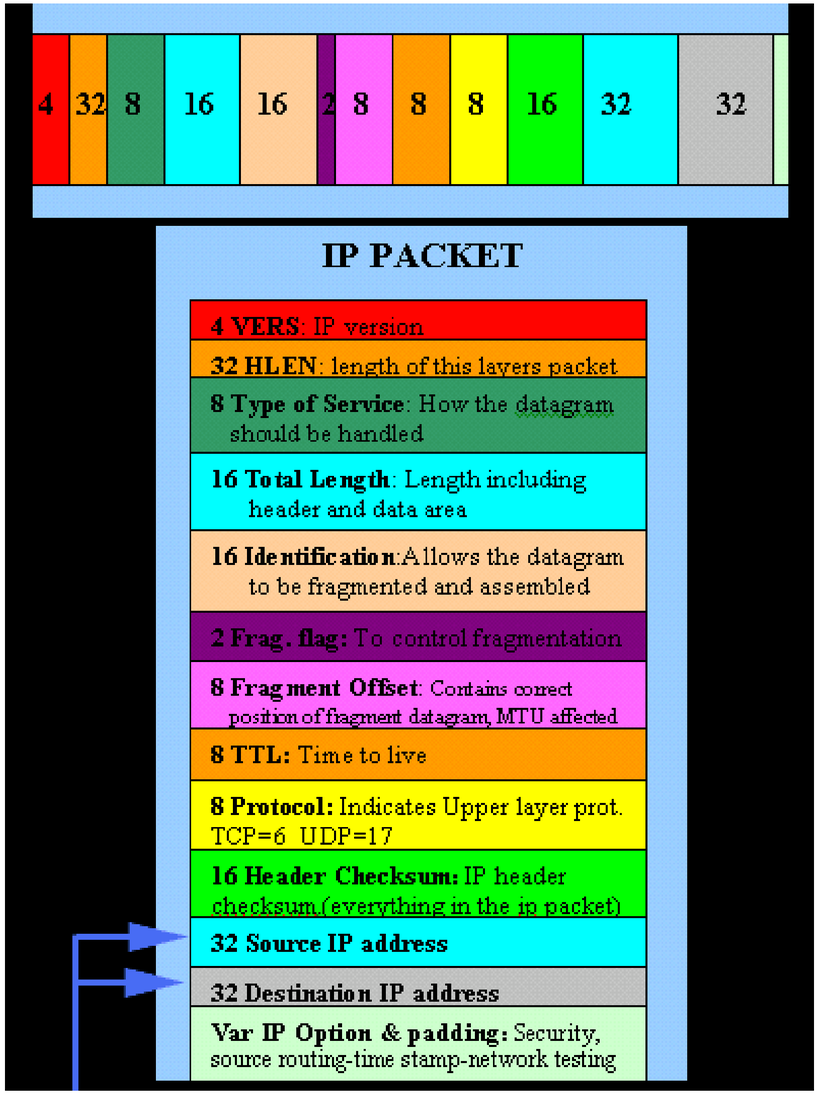
- Convergence: The process required for all routers in an internetwork to update their routing tables and create a consistent view of the network, using the best possible paths.

- Default Route: A "standard" route entry in a routing table which is used as a first option. Any packets sent by a device will be sent first to the default route. If that fails, it will try alternative routes.

Routing

- Static Route: A permanent route entered manually into a routing table. This route will remain in the table, even if the link goes down. It can only be erased manually.

- Dynamic Route: A route entry which is dynamically (automatically) updated as changes to the network occur. Dynamic routes are basically the opposite to static routes.


4
32
8
16
16
2
8
8
8
16
32
32
IP PACKET
4 VERS: IP version
32 HLEN: length of this layers packet
8 Type of Service: How the datagram should be handled
16 Total Length: Length including header and data area
16 Identification: Allows the datagram to be fragmented and assembled
2 Frag. flag: To control fragmentation
8 Fragment Offset: Contains correct position of fragment datagram, MTU affected
8 TTL: Time to live
8 Protocol: Indicates Upper layer prot. TCP=6 UDP=17
16 Header Checksum: IP header checksum (everything in the ip packet)
32 Source IP address
32 Destination IP address
Var IP Option & padding: Security, source routing-time stamp-network testing

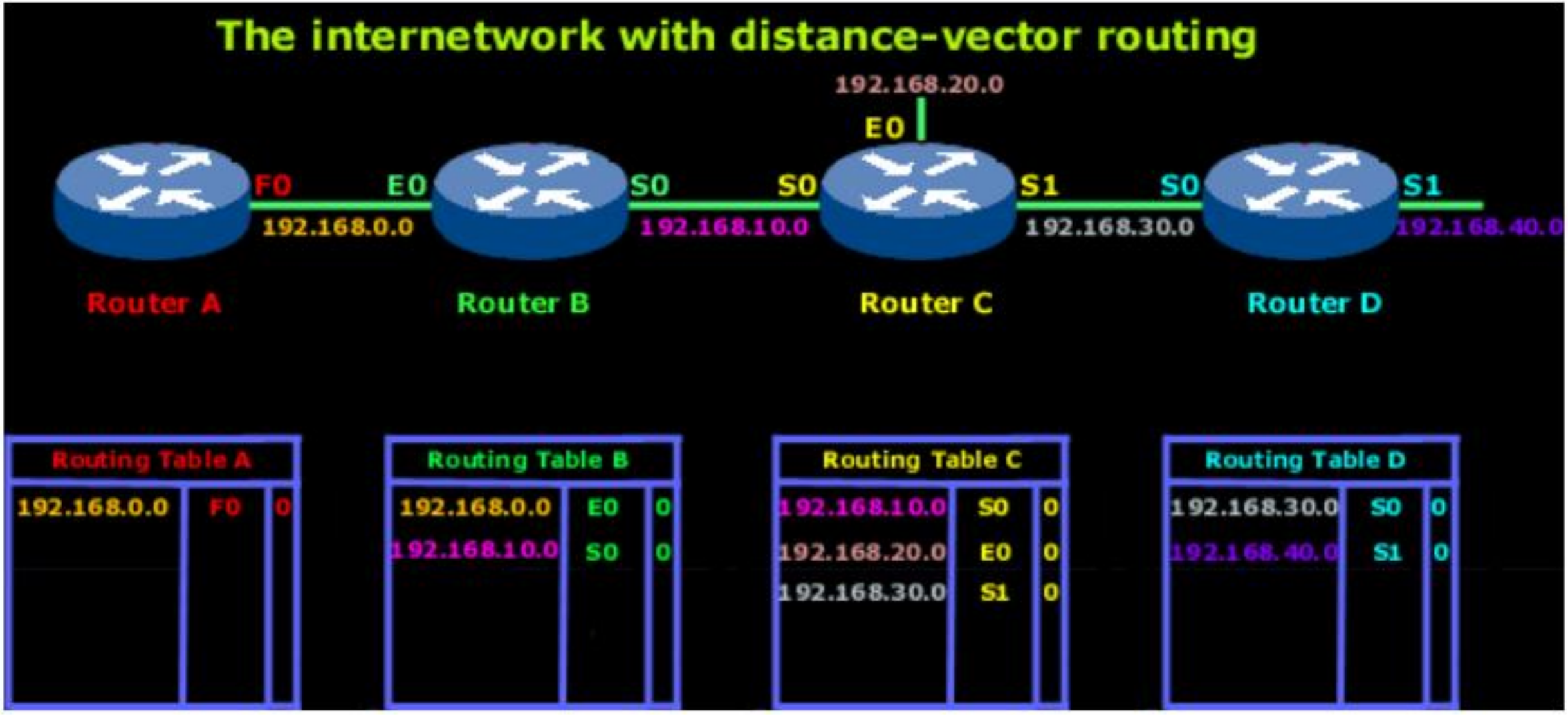
Static and Dynamic Routing

- Only Dynamic routing uses routing protocols, which enable routers to:
  - Dynamically discover and maintain routes
  - Calculate routes
  - Distribute routing updates to other routers
  - Reach agreement with other routers about the network topology

Routing Protocols

- Interior Gateway Protocol
  - Distance vector
    - RIP, IGRP
  - Link state
    - OSPF
  - Hybrid
    - EIGRP
- Exterior Gateway Protocol
  - Border Gateway Protocol (BGP)

The internetwork with distance-vector routing

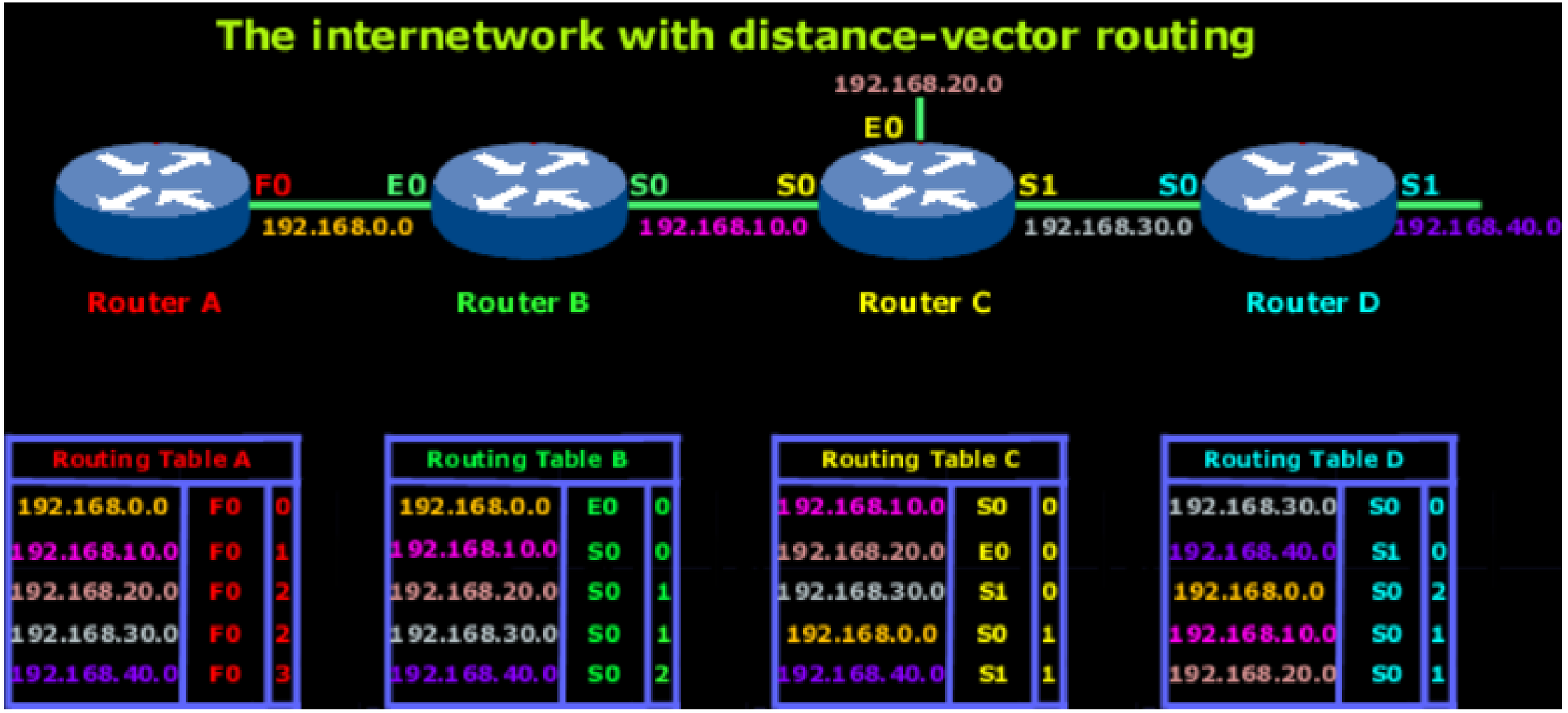


Routing Table A		
192.168.0.0	F0	0

Routing Table B		
192.168.0.0	E0	0
192.168.10.0	S0	0

Routing Table C		
192.168.10.0	S0	0
192.168.20.0	E0	0
192.168.30.0	S1	0

Routing Table D		
192.168.30.0	S0	0
192.168.40.0	S1	0


The internetwork with distance-vector routing
192.168.20.0
E0
F0
E0
S0
S0
S1
S0
S1
192.168.0.0
192.168.10.0
192.168.30.0
192.168.40.0
Router A
Router B
Router C
Router D
Routing Table A
192.168.0.0 F0 0
192.168.10.0 F0 1
192.168.20.0 F0 2
192.168.30.0 F0 2
192.168.40.0 F0 3
Routing Table B
192.168.0.0 E0 0
192.168.10.0 S0 0
192.168.20.0 S0 1
192.168.30.0 S0 1
192.168.40.0 S0 2
Routing Table C
192.168.10.0 S0 0
192.168.20.0 E0 0
192.168.30.0 S1 0
192.168.0.0 S0 1
192.168.40.0 S1 1
Routing Table D
192.168.30.0 S0 0
192.168.40.0 S1 0
192.168.0.0 S0 2
192.168.10.0 S0 1
192.168.20.0 S0 1

OSPF – Link state protocol

- *OSPF will listen to neighbors and gather all link state data*

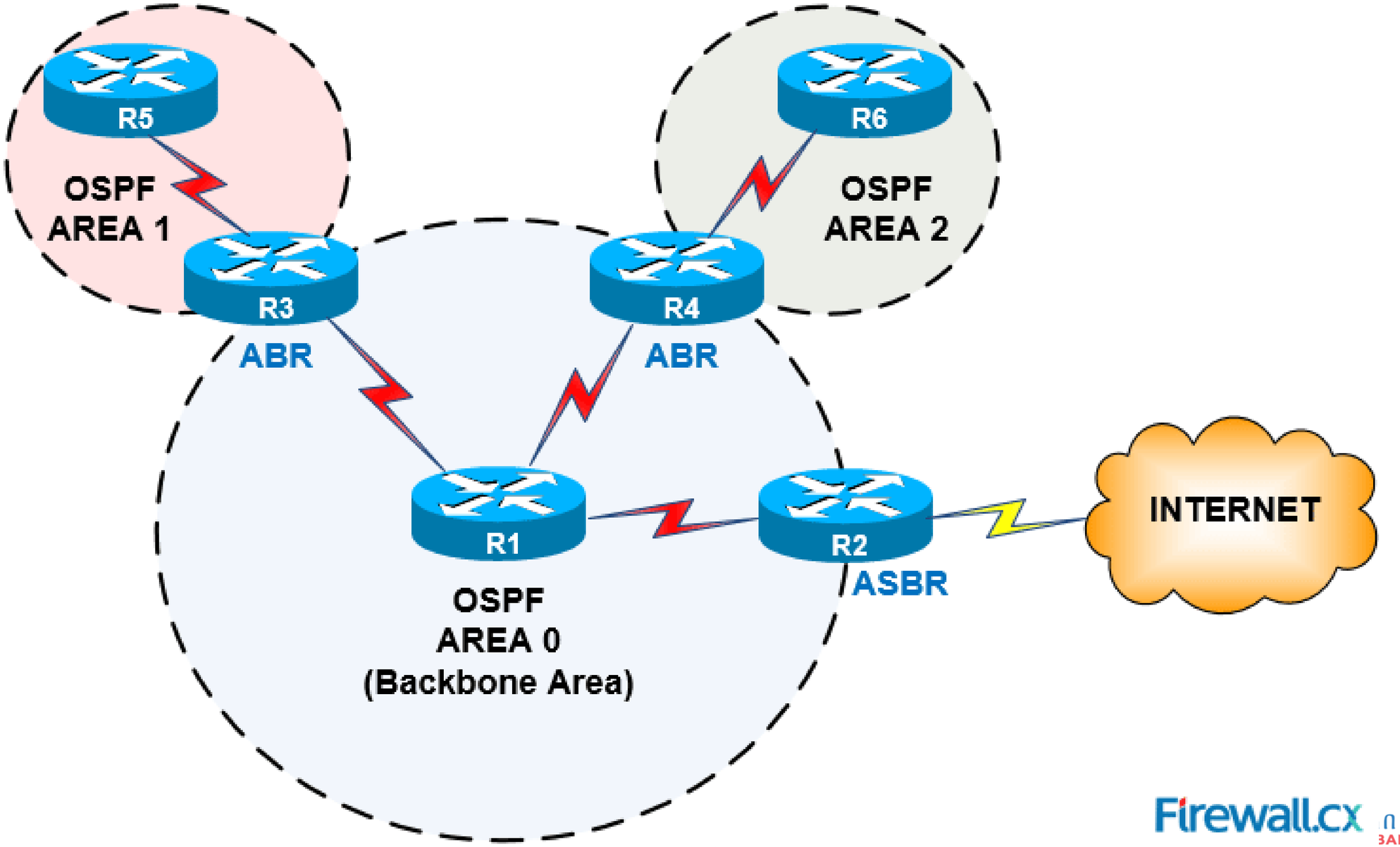
- *Build a topology map of all available paths in its network*

- *Save the information in its topology database, also known as its Link-State Database (LSDB).*

- *Uses Shortest Path First (SFP) Algorithm that was developed by the computer scientist Edsger W. Dijkstra*

OSPF – Link state protocol

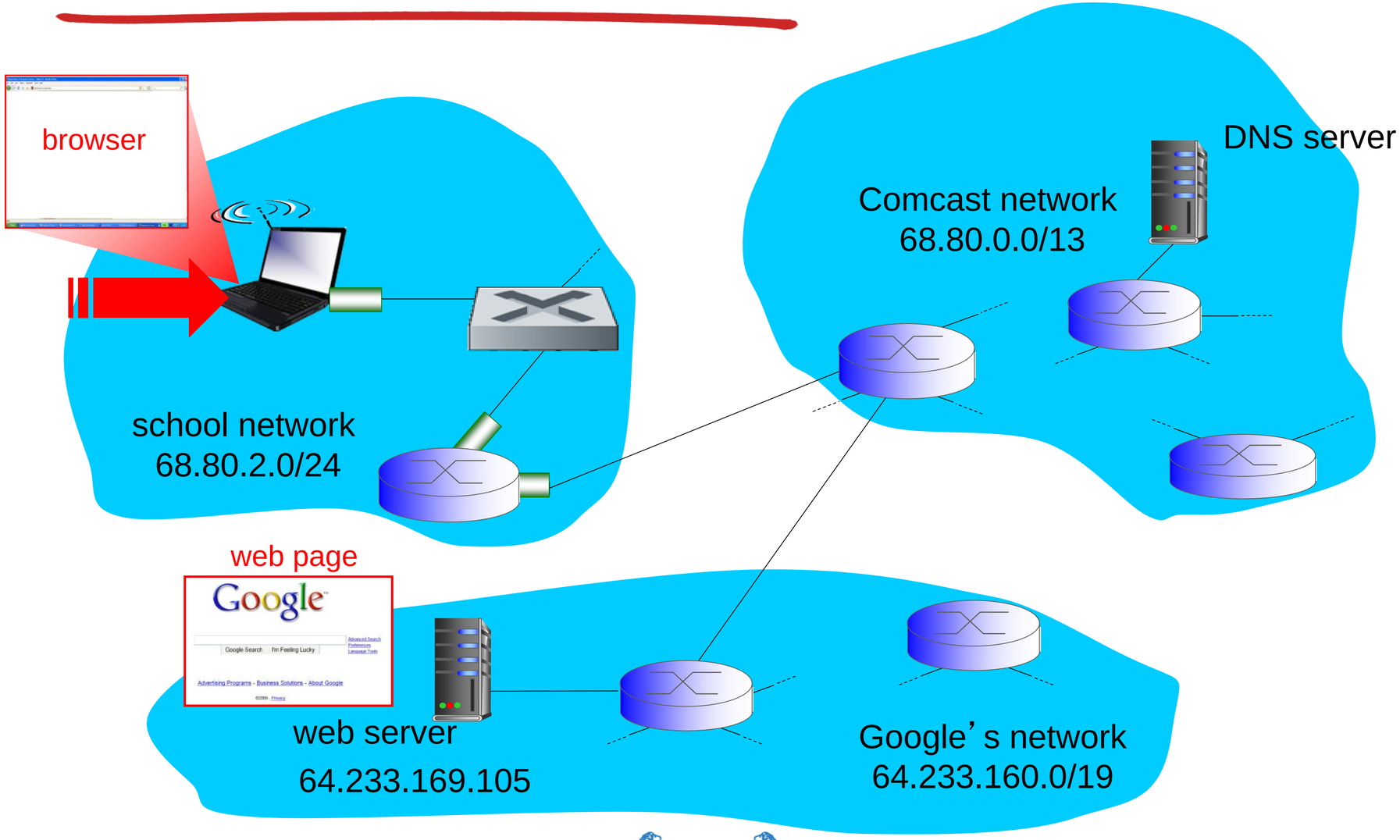
- *OSPF will then construct three tables to store the following information:*
  - *Neighbor Table: Contains all discovered OSPF neighbors with whom routing information will be interchanged*
  - *Topology Table: Contains the entire road map of the network with all available OSPF routers and calculated best and alternative paths.*
  - *Routing Table: Contain the current working best paths that will be used to forward data traffic between neighbors.*


R5
OSPF
AREA 1
R6
OSPF
AREA 2
R3
ABR
R4
ABR
R1
R2
ASBR
INTERNET
OSPF
AREA 0
(Backbone Area)

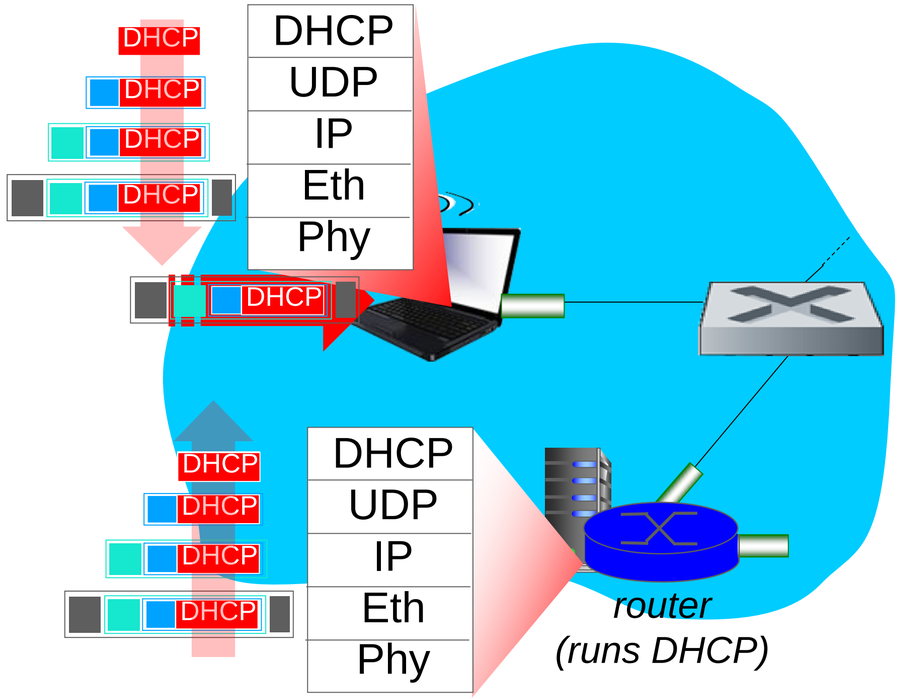
Synthesis: a day in the life of a web request

- journey down protocol stack complete!
  - application, transport, network, link
- putting-it-all-together: synthesis!
  - *goal:* identify, review, understand protocols (at all layers) involved in seemingly simple scenario: requesting www page
  - *scenario:* student attaches laptop to campus network, requests/receives www.google.com

A day in the life: scenario

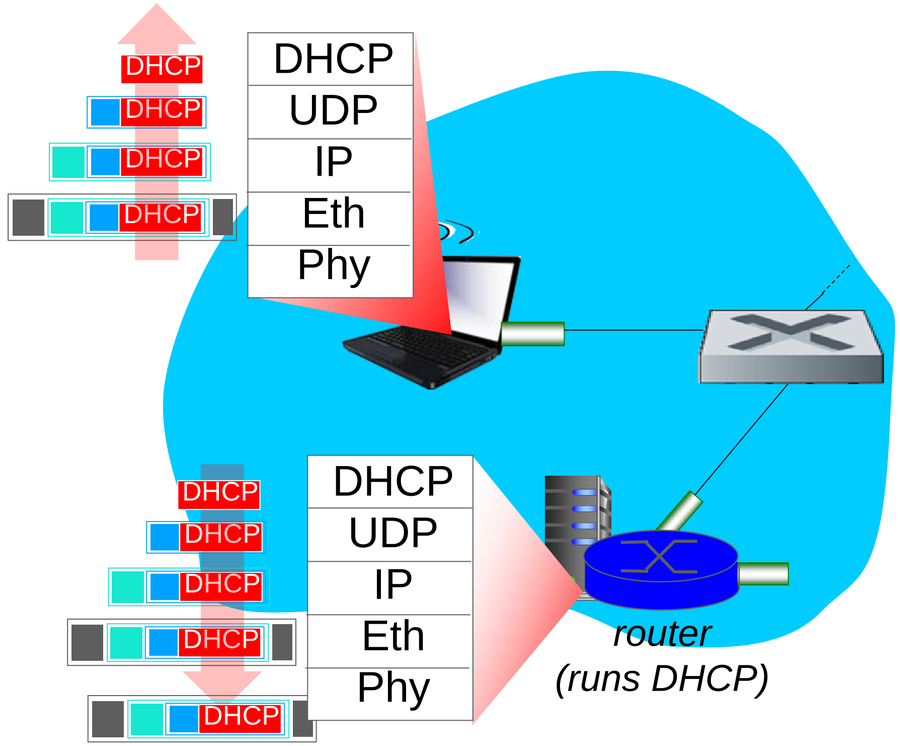


A day in the life… connecting to the Internet



- connecting laptop needs to get its own IP address, addr of first-hop router, addr of DNS server: use *DHCP*
  - DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.3 Ethernet
  - Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
    - Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

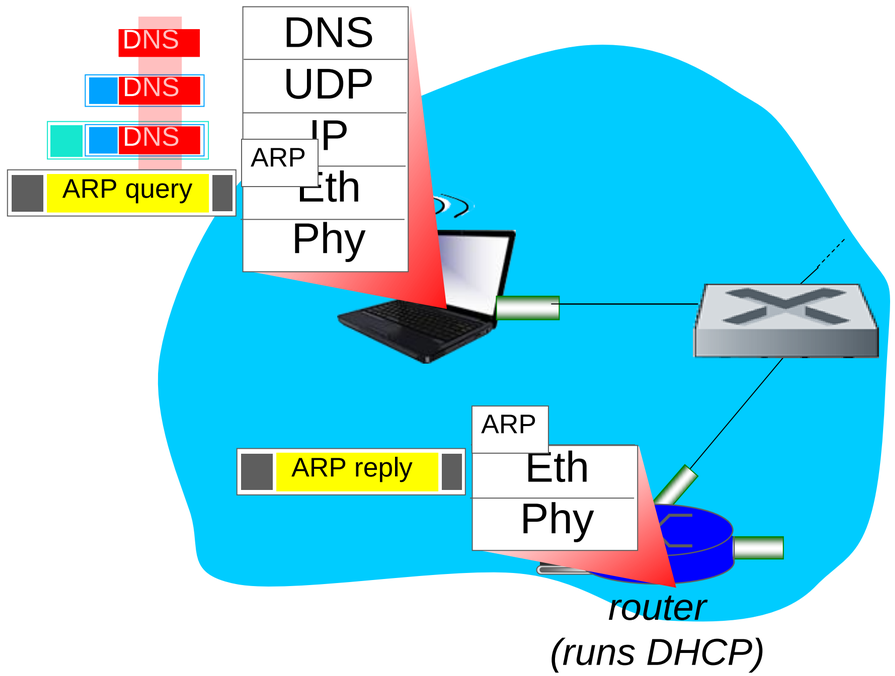
A day in the life… connecting to the Internet



- DHCP server formulates *DHCP ACK* containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
  - encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client
  - DHCP client receives DHCP ACK reply

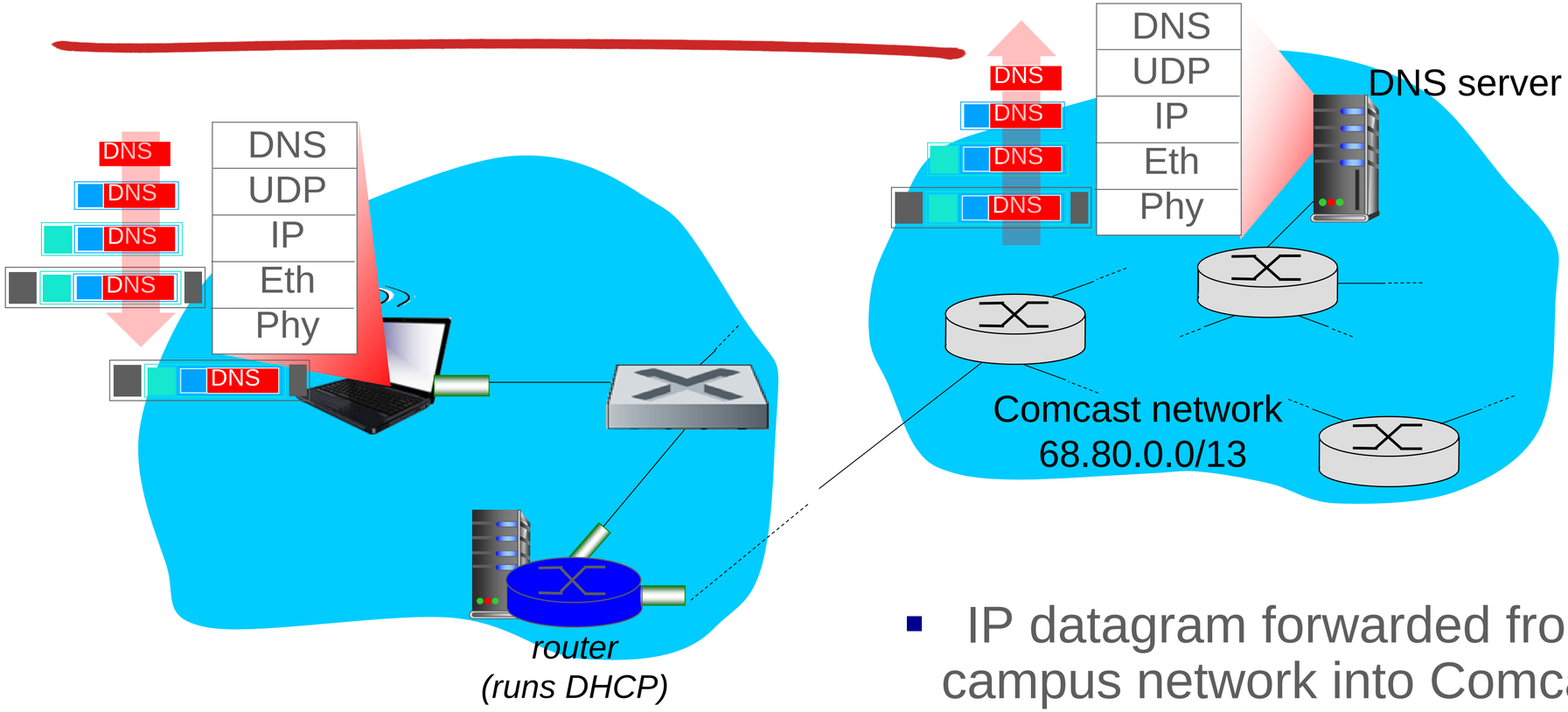
Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

A day in the life… ARP (before DNS, before HTTP)



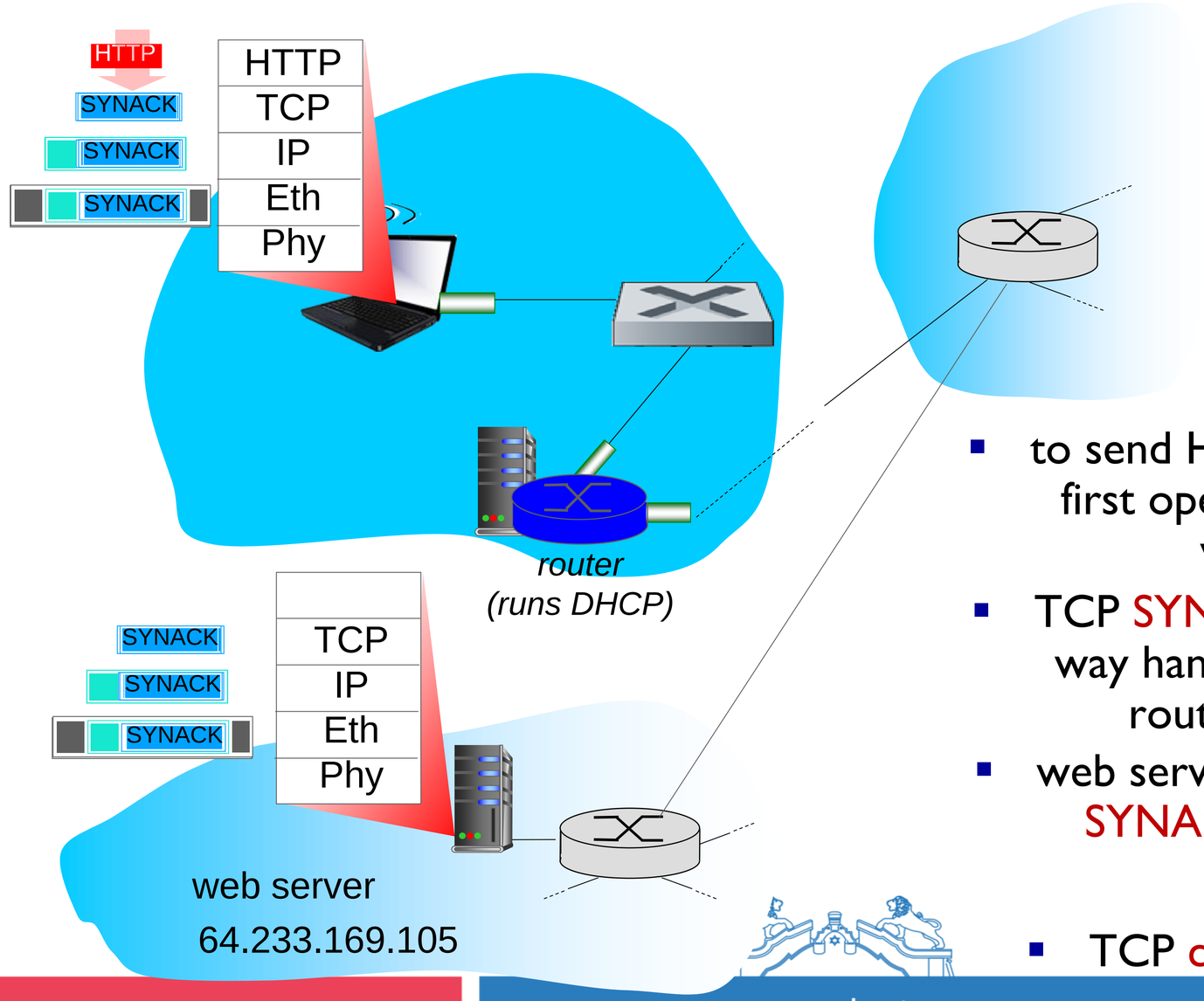
- before sending *HTTP* request, need IP address of www.google.com: *DNS*
  - DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: ARP
  - ARP query broadcast, received by router, which replies with ARP reply giving MAC address of router interface
  - client now knows MAC address of first hop router, so can now send frame containing DNS query

A day in the life… using DNS



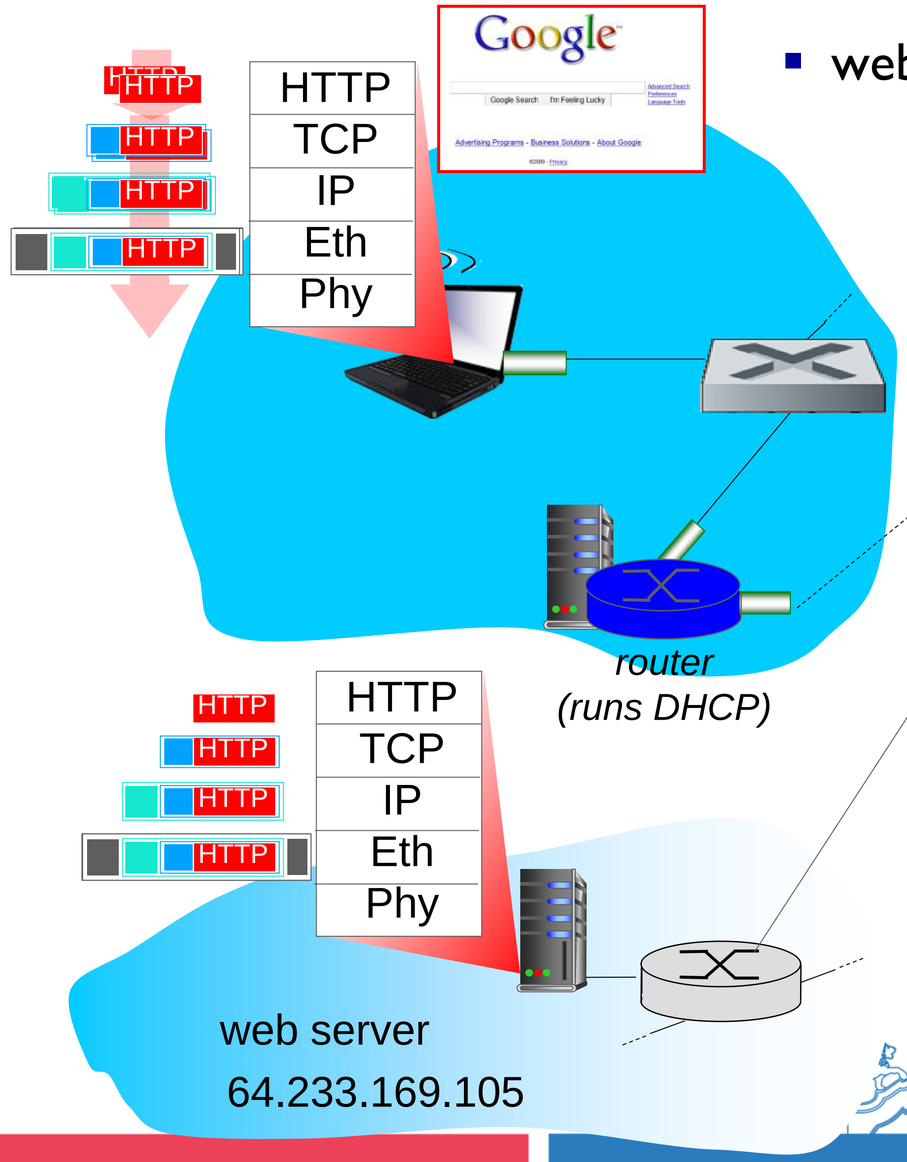
- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router
- IP datagram forwarded from campus network into Comcast network, routed (tables created by RIP, OSPF, IS-IS and/or BGP routing protocols) to DNS server
- demuxed to DNS server
- DNS server replies to client with IP address of www.google.com

A day in the life…TCP connection carrying HTTP



- to send HTTP request, client first opens TCP socket to web server
- TCP SYN segment (step 1 in 3-way handshake) inter-domain routed to web server
- web server responds with TCP SYNACK (step 2 in 3-way handshake)
- TCP connection established!

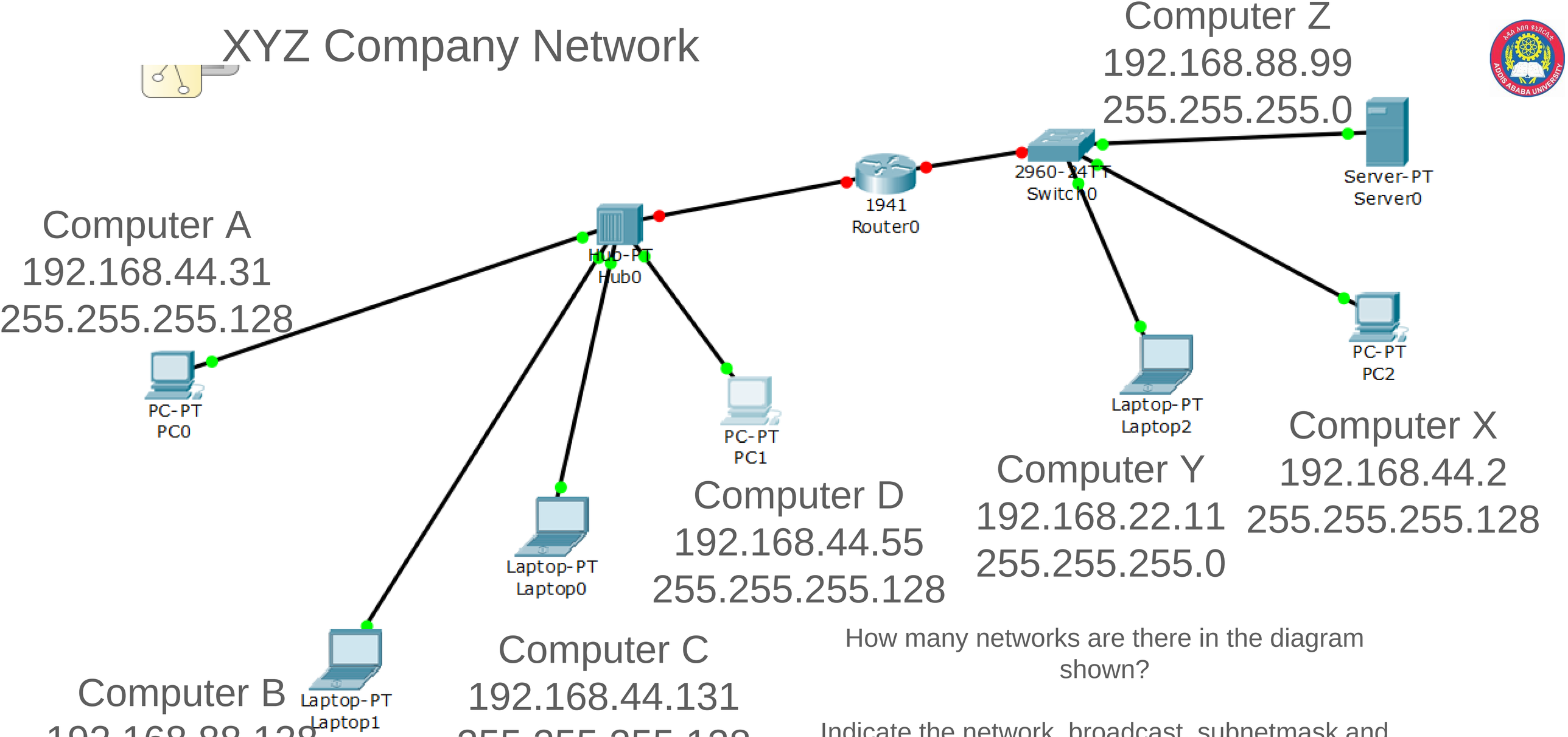
A day in the life… HTTP request/reply



- web page finally (!!!) displayed

- HTTP request sent into TCP socket
- IP datagram containing HTTP request routed to www.google.com
- web server responds with HTTP reply (containing web page)
- IP datagram containing HTTP reply routed back to client

XYZ Company Network



Computer A
192.168.44.31
255.255.255.128

Computer Z
192.168.88.99
255.255.255.0

Computer B
192.168.88.128
255.255.255.0

Computer C
192.168.44.131
255.255.255.128

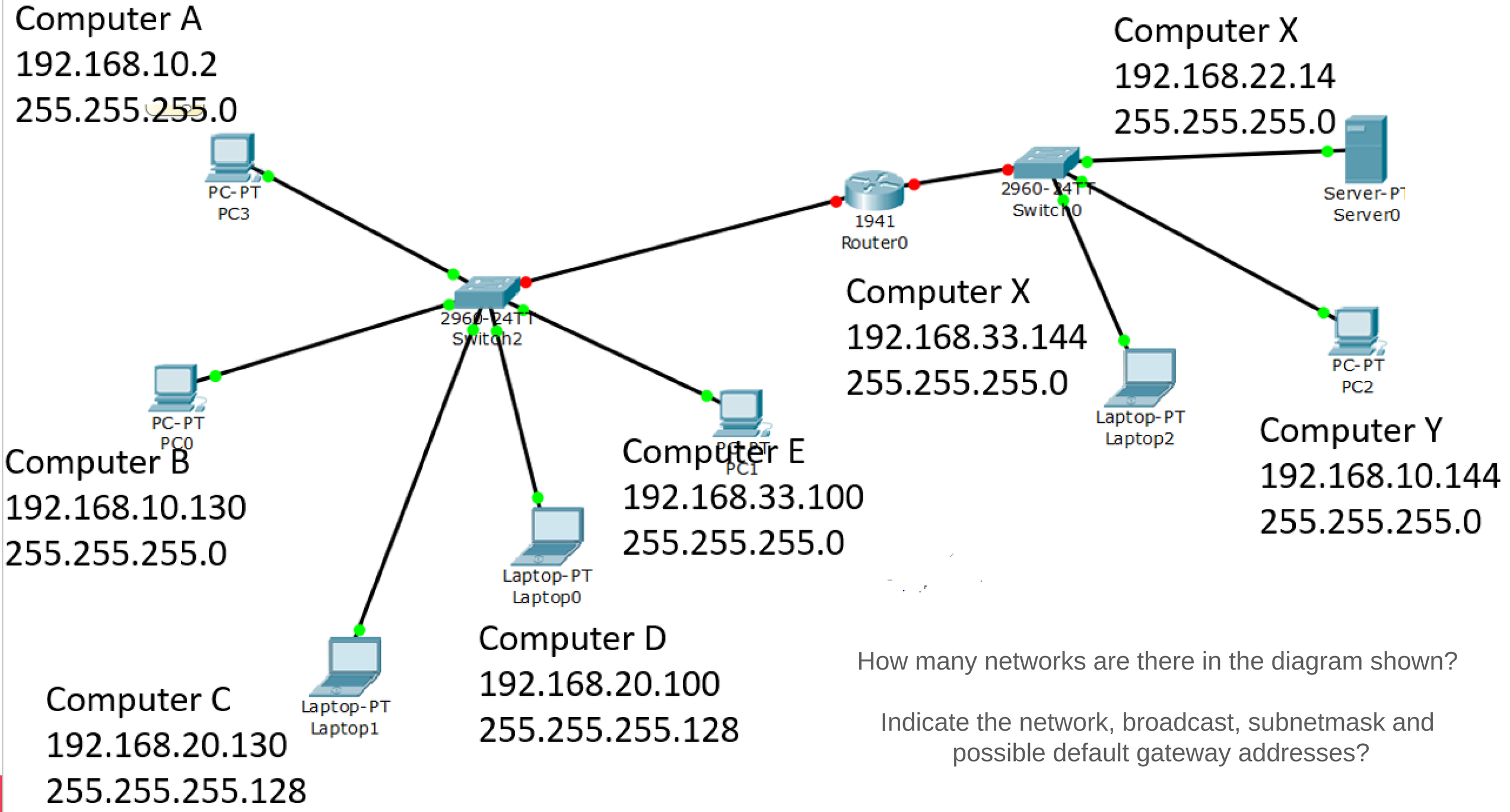
Computer D
192.168.44.55
255.255.255.128

Computer Y
192.168.22.11
255.255.255.0

Computer X
192.168.44.2
255.255.255.128

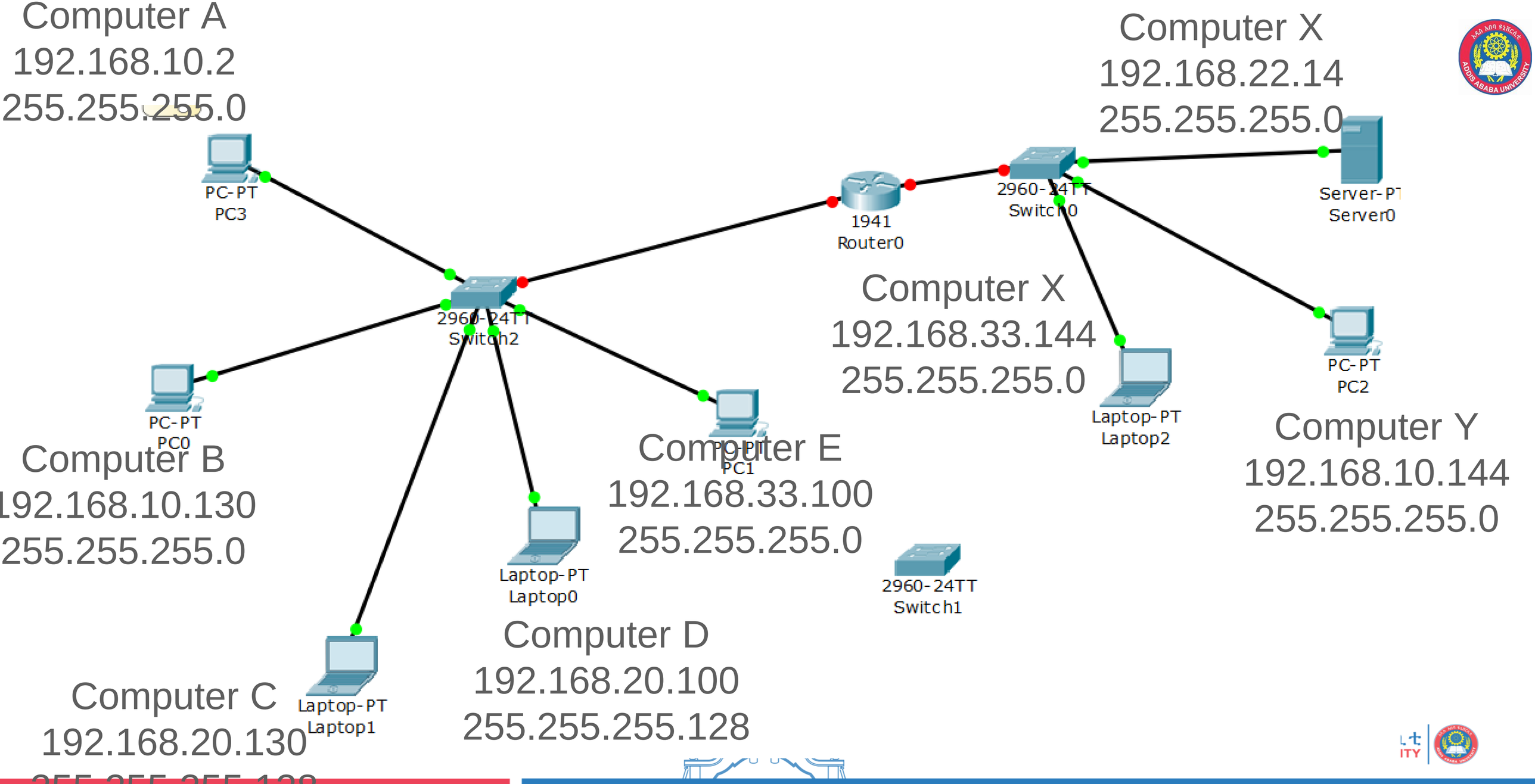
How many networks are there in the diagram shown?

Indicate the network, broadcast, subnetmask and possible default gateway addresses?



How many networks are there in the diagram shown?

Indicate the network, broadcast, subnetmask and possible default gateway addresses?


Computer A
192.168.10.2
255.255.255.0
PC-PT
PC3
2960-24TT
Switch2
1941
Router0
2960-24TT
Switch0
Server-PT
Server0
Computer X
192.168.22.14
255.255.255.0
Computer X
192.168.33.144
255.255.255.0
PC-PT
PC2
Laptop-PT
Laptop2
Computer Y
192.168.10.144
255.255.255.0
PC-PT
PC0
Computer B
192.168.10.130
255.255.255.0
PC-PT
PC1
Computer E
192.168.33.100
255.255.255.0
Laptop-PT
Laptop0
2960-24TT
Switch1
Computer D
192.168.20.100
255.255.255.128
Laptop-PT
Laptop1
Computer C
192.168.20.130
255.255.255.128

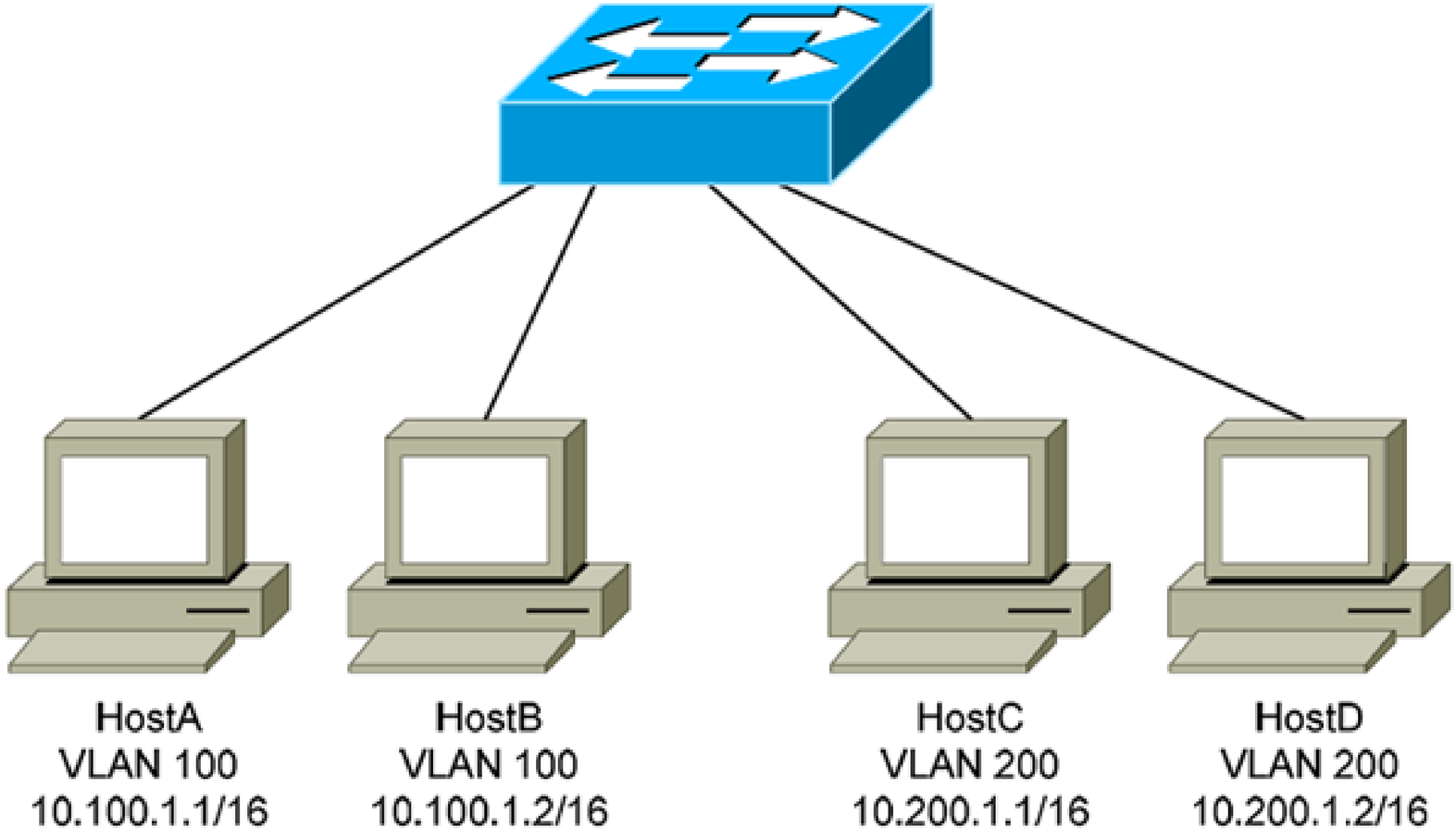
VLAN and Inter-VLAN Routing

- A Virtual Local Area Network (VLAN) is a virtual local area network that is created by grouping devices together based on their logical relationships, rather than their physical location within a network.
- By dividing a physical network into multiple logical networks, VLANs can help organizations to simplify network management, control network access, and increase the efficiency of network resources

.

VLAN and Inter-VLAN Routing

- VLANs provide the several benefits:
  - ***Broadcast Control*** – eliminates unnecessary broadcast traffic, improving network performance and scalability.
  - ***Security*** – logically separates users and departments, allowing administrators to implement access-lists to control traffic between VLANs.
  - ***Flexibility*** – removes the physical boundaries of a network, allowing a user or device to exist anywhere. VLANs are very common in LAN and campus networks. For example, user networks are often separated from server networks using VLANs. .


HostA
VLAN 100
10.100.1.1/16
HostB
VLAN 100
10.100.1.2/16
HostC
VLAN 200
10.200.1.1/16
HostD
VLAN 200
10.200.1.2/16

VLAN and Inter-VLAN Routing

- In a VLAN, devices that are part of the same VLAN can communicate with each other as if they were on the same physical network, even if they are physically located in different parts of the network.

- Devices that are part of different VLANs, however, cannot communicate directly with each other. This is where inter VLAN routing comes into play.

.

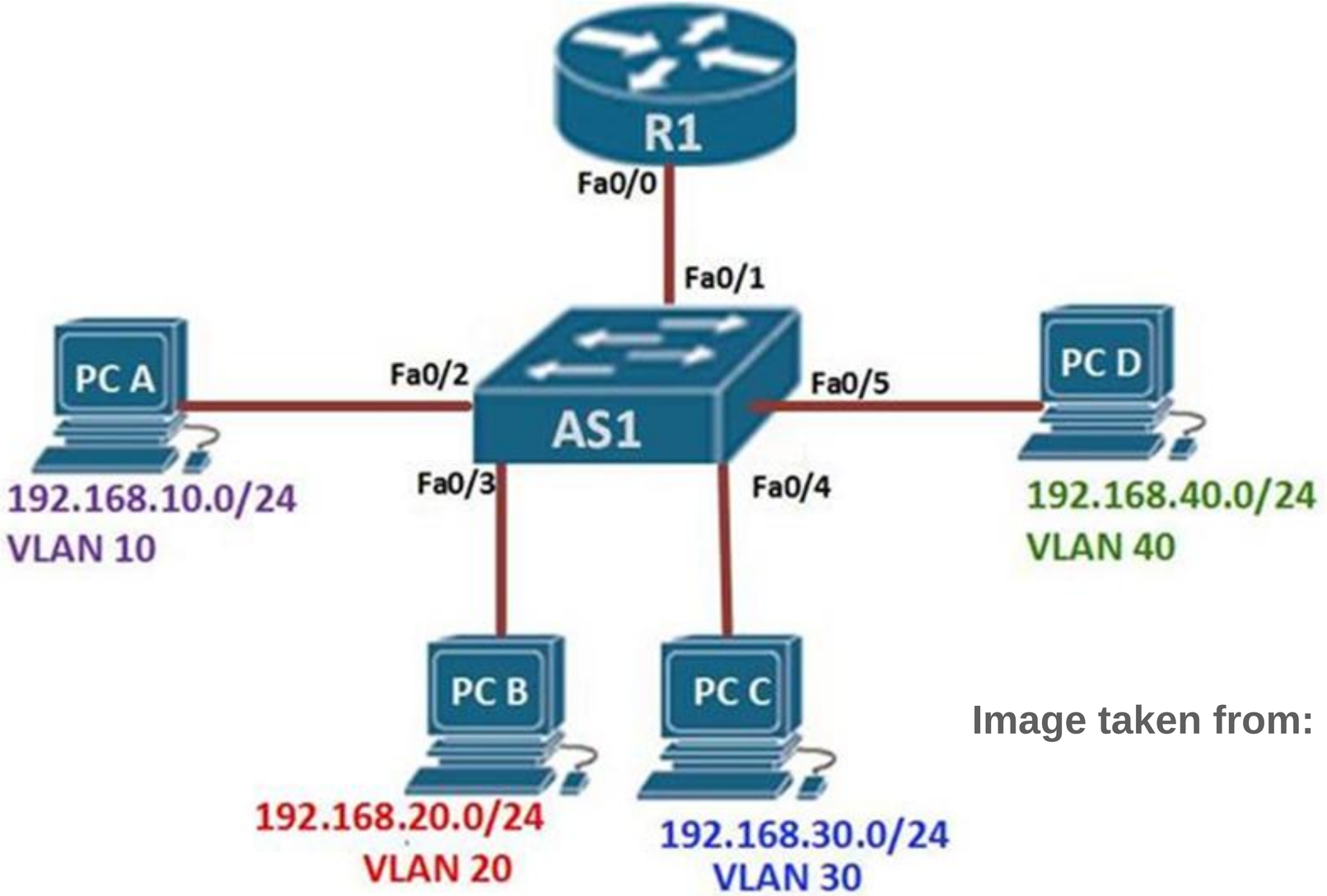


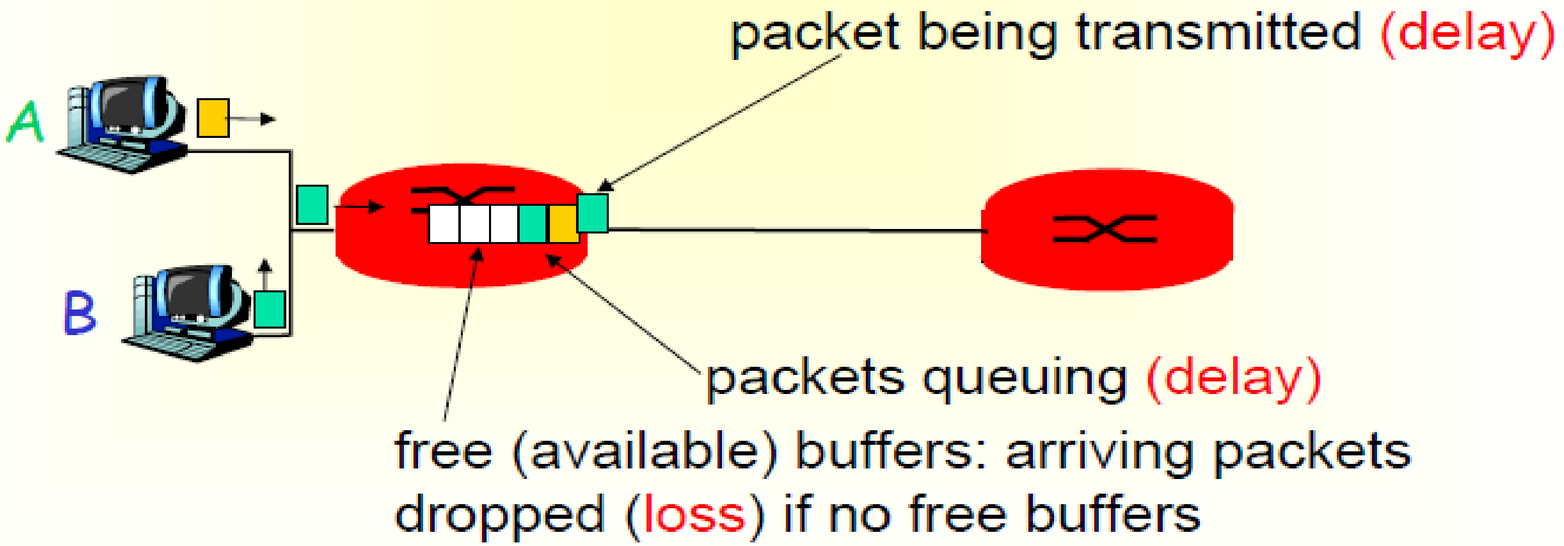
Image taken from: CCNA blog

5. Advanced Topics in Computer Networks

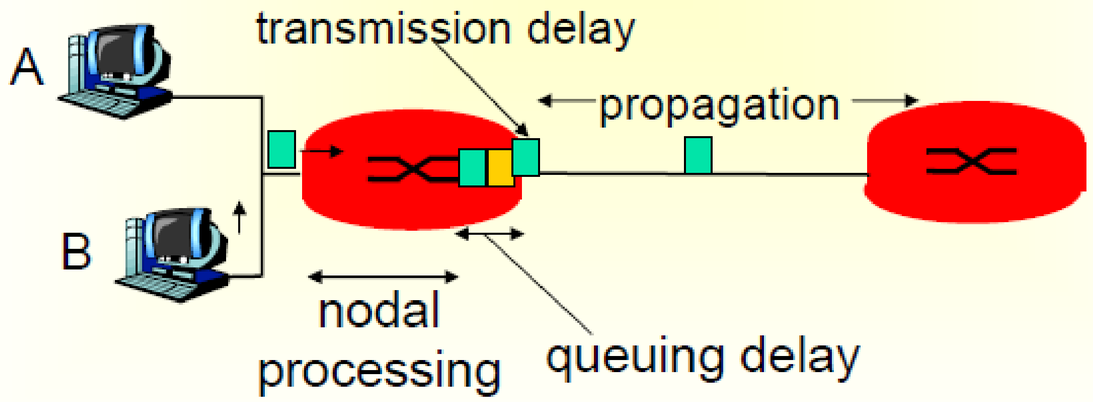
- Network Performance
- Wireless and Mobile Networks
- Linking to ISPs
- Security in Computer Networks (Preventing, Detecting, Recovery)

1. Performance: can be measured using transit time (amount of time required for a message to travel), response time (elapsed time between an inquiry and the response), and packet loss and delay

   - How do loss and delay occur?
     - packet arrival rate to link exceeds output link capacity
     - packets queue in router buffers, waiting for their turn



- Four sources of packet delay (in packet-switched networks)
  1. Nodal processing (d_{proc})
     - to check bit errors
     - to determine output link
  2. Queuing Delay (d_{queue})
     - time waiting at output link for transmission
     - depends on congestion level of router
     - if queue is empty, queue delay is zero



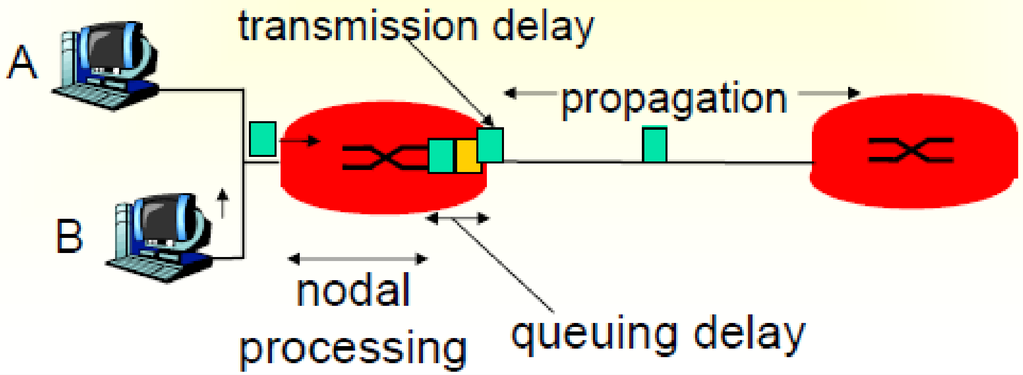
3. Transmission delay (d_{trans}) - assume FCFS

- R = link bandwidth (bps) e.g., for 10Mbps Ethernet link, R = 10Mbps (confusion in measurement units - 10Mbps vs. 10Mb)
- L = packet length (bits)
- time to send bits into link, $d_{trans} = L/R$

4. Propagation delay (d_{prop})

- d = length of physical link (distance between two routers)
- s = propagation speed in medium (depends on the type of link and is in the range of $2x10^8$ meters/sec to $3x10^8$)
- propagation delay, $d_{prop} = d/s$

- Note: s and R are very different quantities!
- $d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$

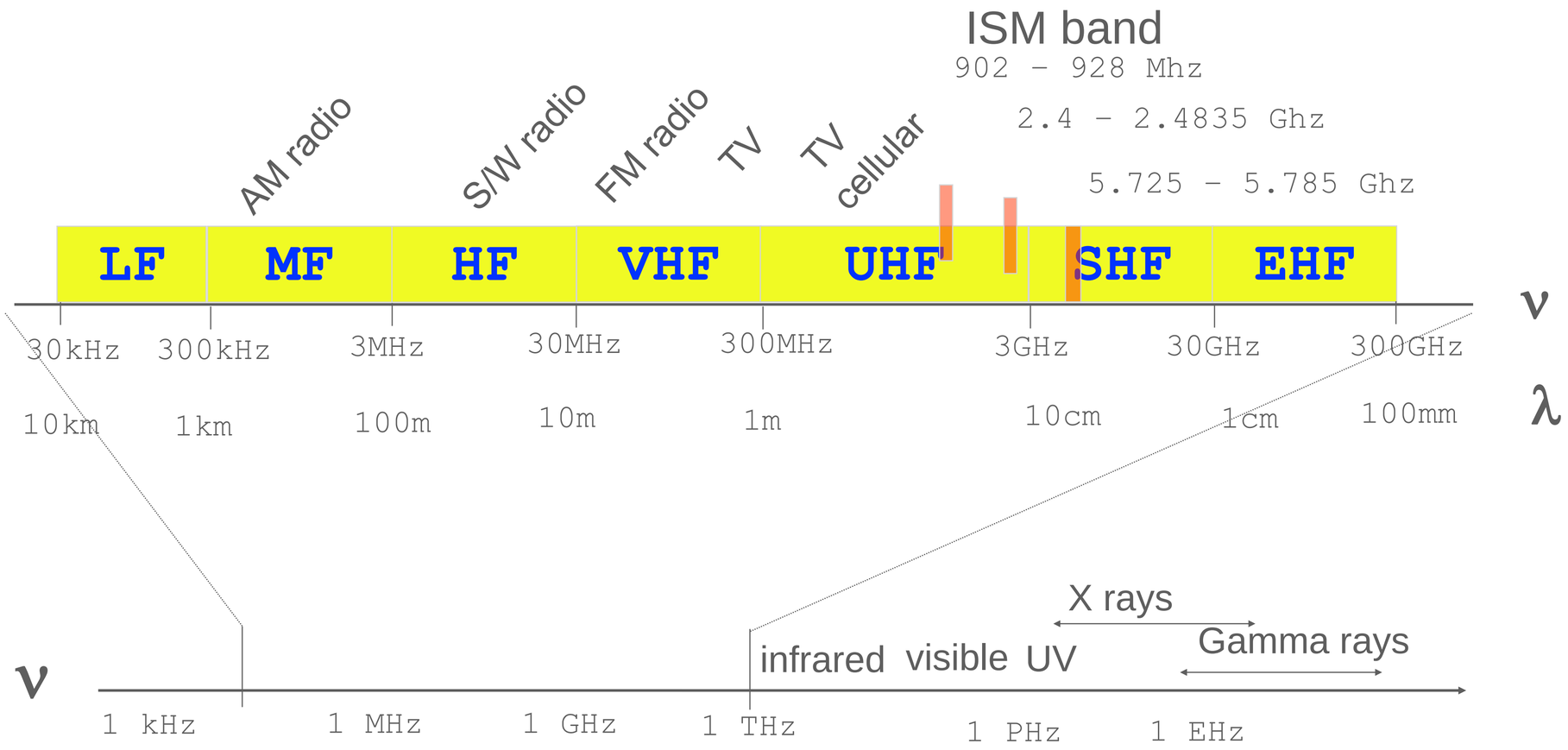


Wireless and Mobile Networks

- **Definition**
  - Wireless
    - refers to the transmission of voice and data over radio wave
    - allows communication without requiring physical connection to the network
    - wireless devices include anything that use wireless network to either send or receive data
    - a wireless network can be accessed from mobile or fixed devices
  - Mobile
    - a mobile device is anything that can be used on the move, ranging from laptops to mobile phones
  - Wireless does not always mean Mobile!

- Different types of wireless networks
  - elements of a wireless network can be combined in many way
  - Single-hop, infrastructure-based
    - host connects to base station (e.g., 802.11 WiFi, cellular) which connects to the larger Internet
  - Single-hop, Infrastructure-less
    - no base station, no connection to a larger Internet (e.g., Bluetooth, ad hoc networks)
  - Multi-hop, Infrastructure-based
    - some hosts may have to relay through several wireless nodes to connect to the base station (e.g., wireless mesh networks)
  - Multi-hop, Infrastructure-less
    - no base station, have to relay messages among several other nodes in order to reach a destination
    - nodes may also be mobile, a class of networks known as mobile ad hoc networks (MANETs)
  - multi-hop implies that each mobile node also acts as a router

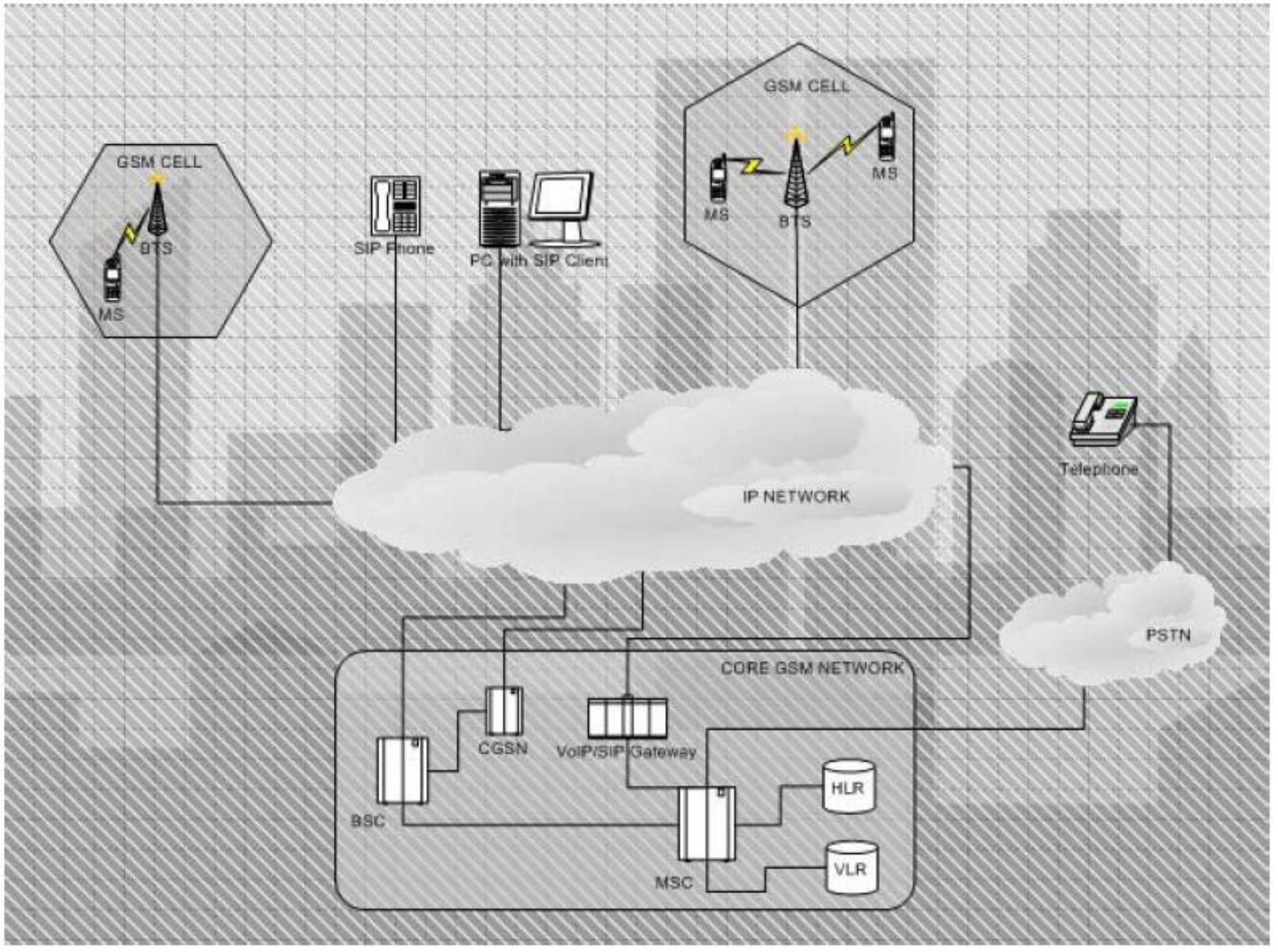
EM Spectrum

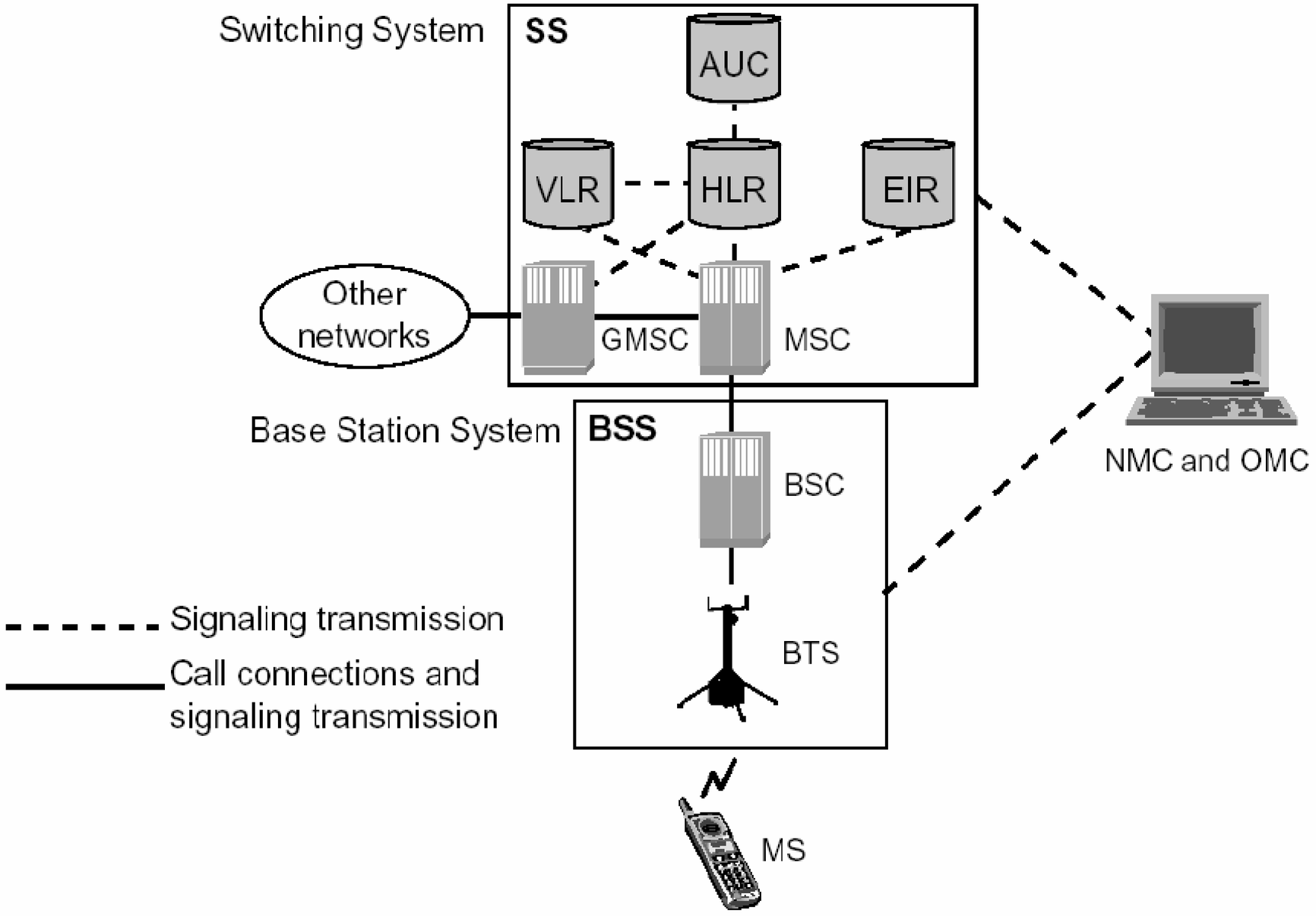

ISM band
902 – 928 Mhz
2.4 – 2.4835 Ghz
5.725 – 5.785 Ghz
AM radio
S/W radio
FM radio
TV
TV
cellular
LF
MF
HF
VHF
UHF
SHF
EHF
ν
λ
30kHz
300kHz
3MHz
30MHz
300MHz
3GHz
30GHz
300GHz
10km
1km
100m
10m
1m
10cm
1cm
100mm
X rays
infrared
visible
UV
Gamma rays
ν
1 kHz
1 MHz
1 GHz
1 THz
1 PHz
1 EHz

Wireless Networks

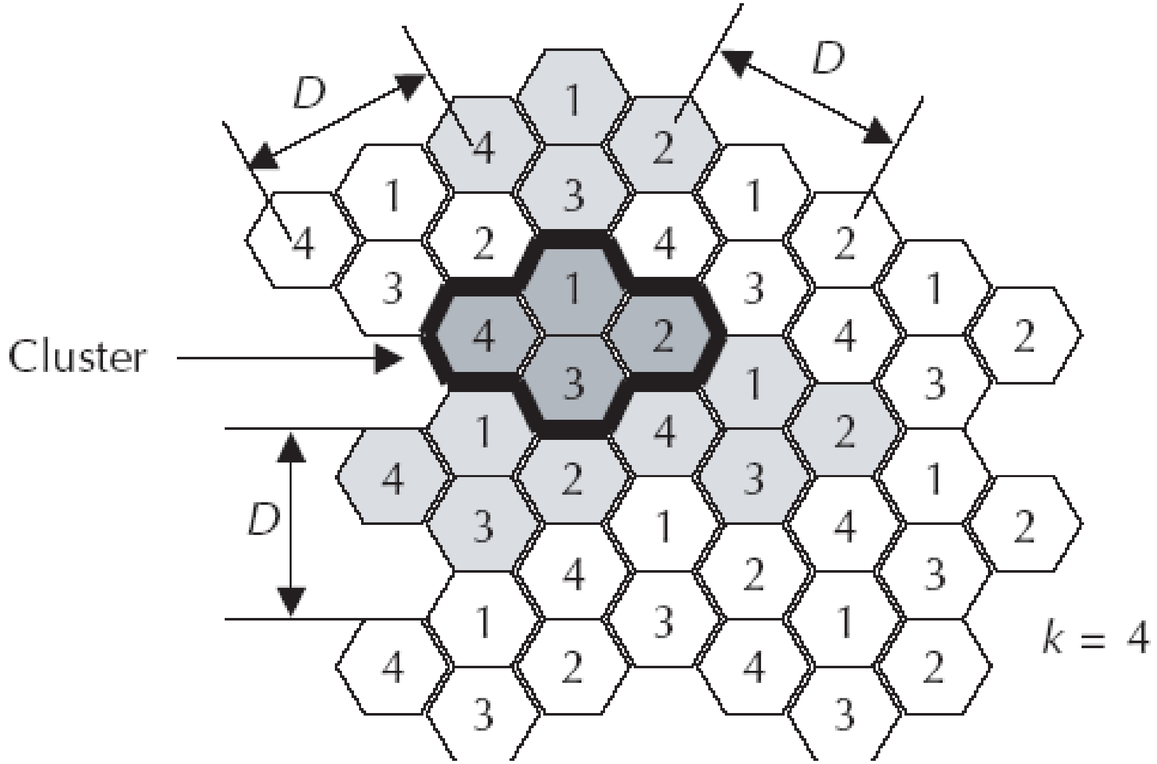
- PAN
- WLAN
  - Wi-Fi
- WWAN

- 802.11
  - 2.4-5 GHz
  - 1-2 Mbps (100m)
- 802.11a
  - 5.1-5.8 GHz
  - up to 54 Mbps (50m)
- 802.11b
  - 2.4-2.485 GHz
  - up to 11 Mbps (100m)
- 802.11g
  - 2.4-2.485 GHz
  - up to 54 Mbps (100m)
- 802.11n: multiple antennae (MIMO – Multiple Input Multiple Output)
  - 2.4-5 GHz
  - up to 200 Mbps
- 802.11n-2009: enhancement on (802.11 2007, 802.11k-2008, 802.11r-2008,802.11y-2008,802.11w-2009)
  - 600 Mbps

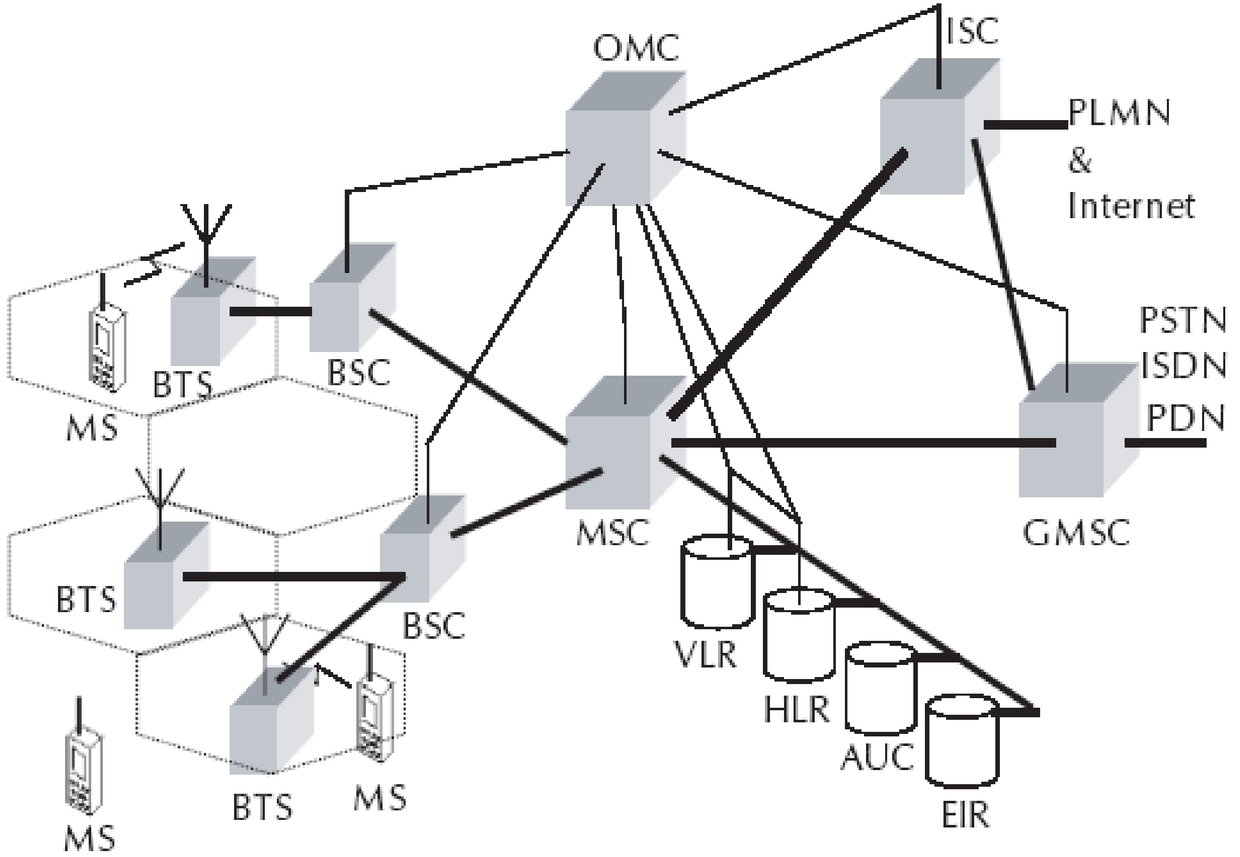

GSM CELL
BTS
MS
SIP Phone
PC with SIP Client
GSM CELL
MS
BTS
MS
IP NETWORK
Telephone
PSTN
CORE GSM NETWORK
CGSN
VoIP/SIP Gateway
HLR
BSC
MSC
VLR


Switching System
SS
AUC
VLR
HLR
EIR
Other networks
GMSC
MSC
Base Station System
BSS
BSC
BTS
NMC and OMC
MS
Signaling transmission
Call connections and signaling transmission

Cell clusters in GSM



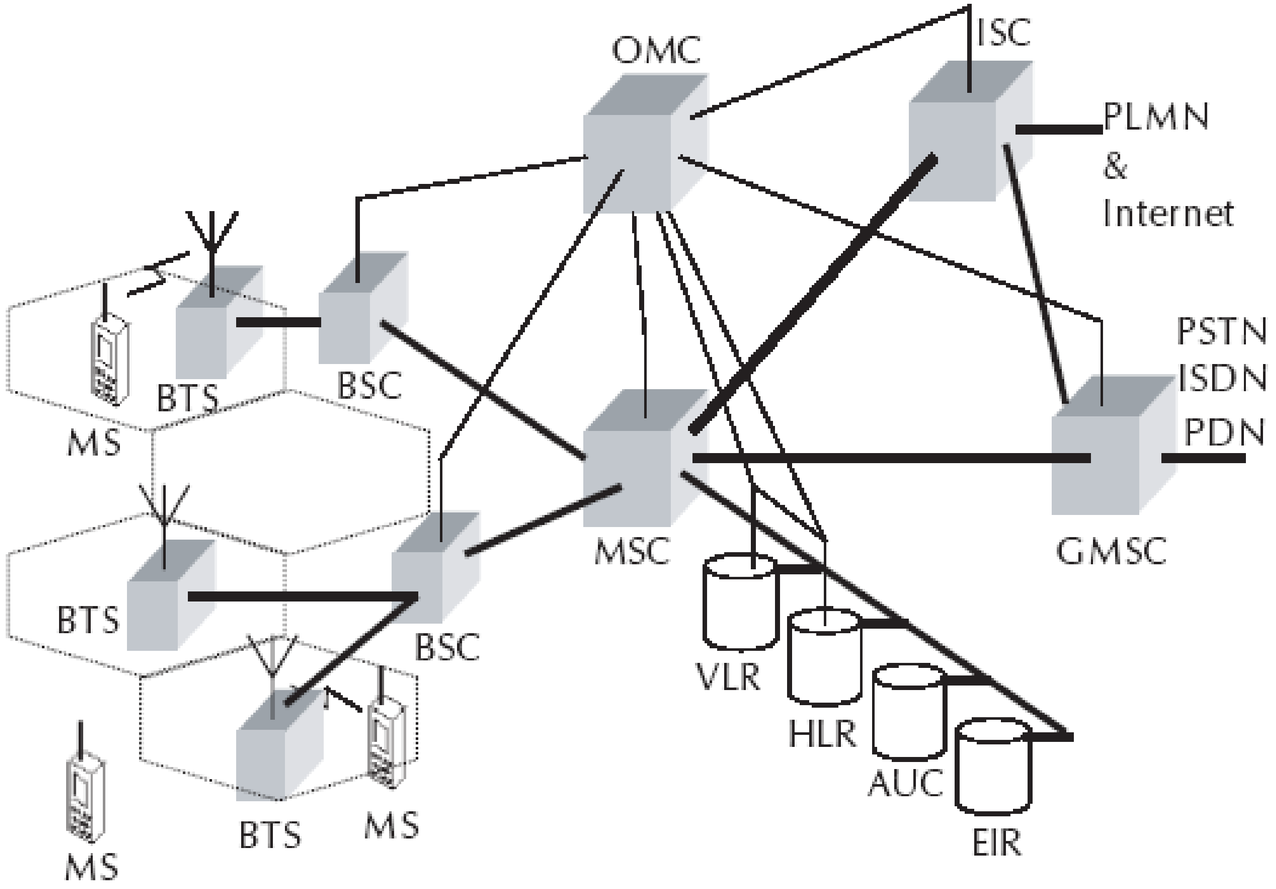
GSM Architecture



BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
ISC	International Switching Center

MS	Mobile Station
HLR	Home Location Register
VLR	Visitor Location Register
AUC	Authentication Center
EIR	Equipment Identity Register
OMC	Operation and Maintenance Center

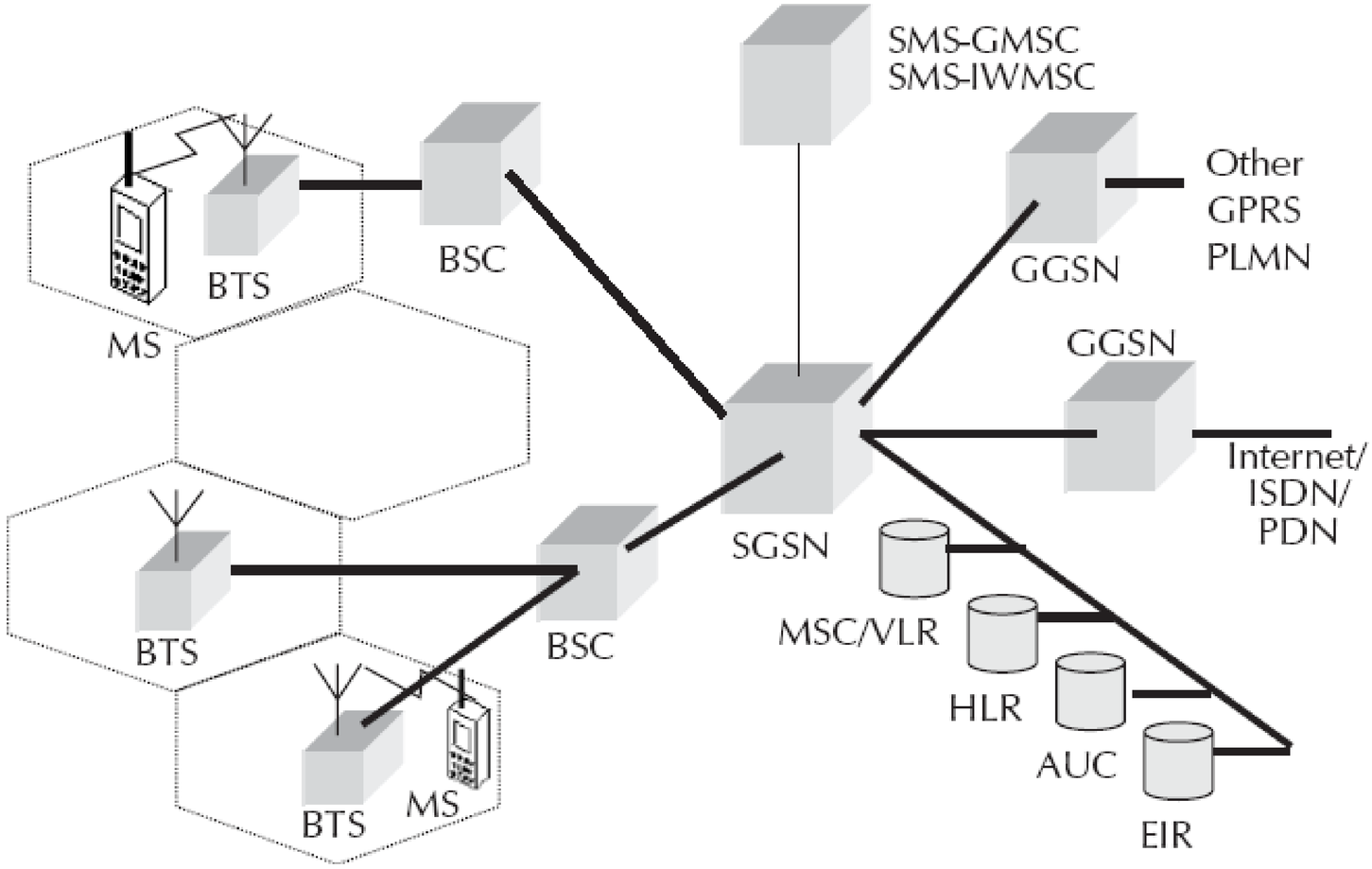
GSM Architecture



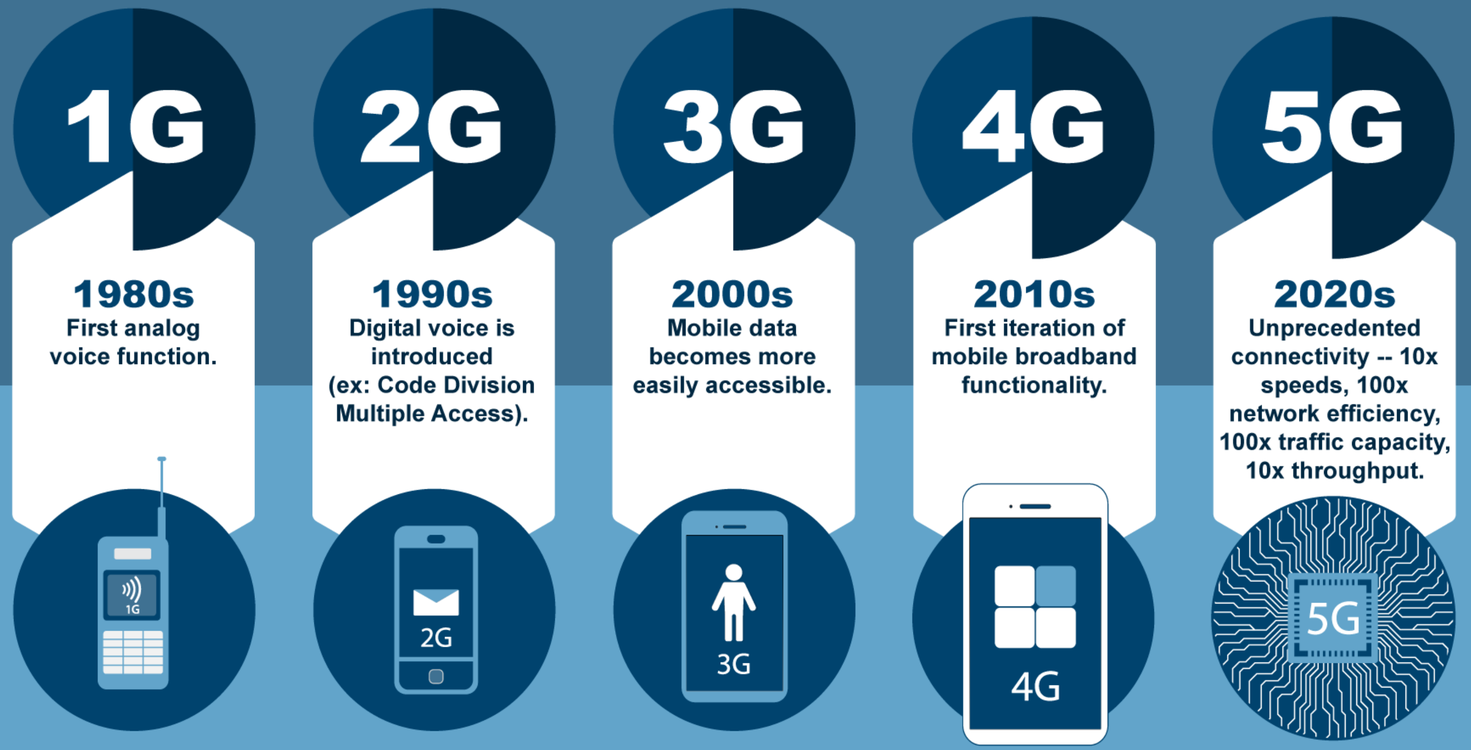
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
ISC	International Switching Center

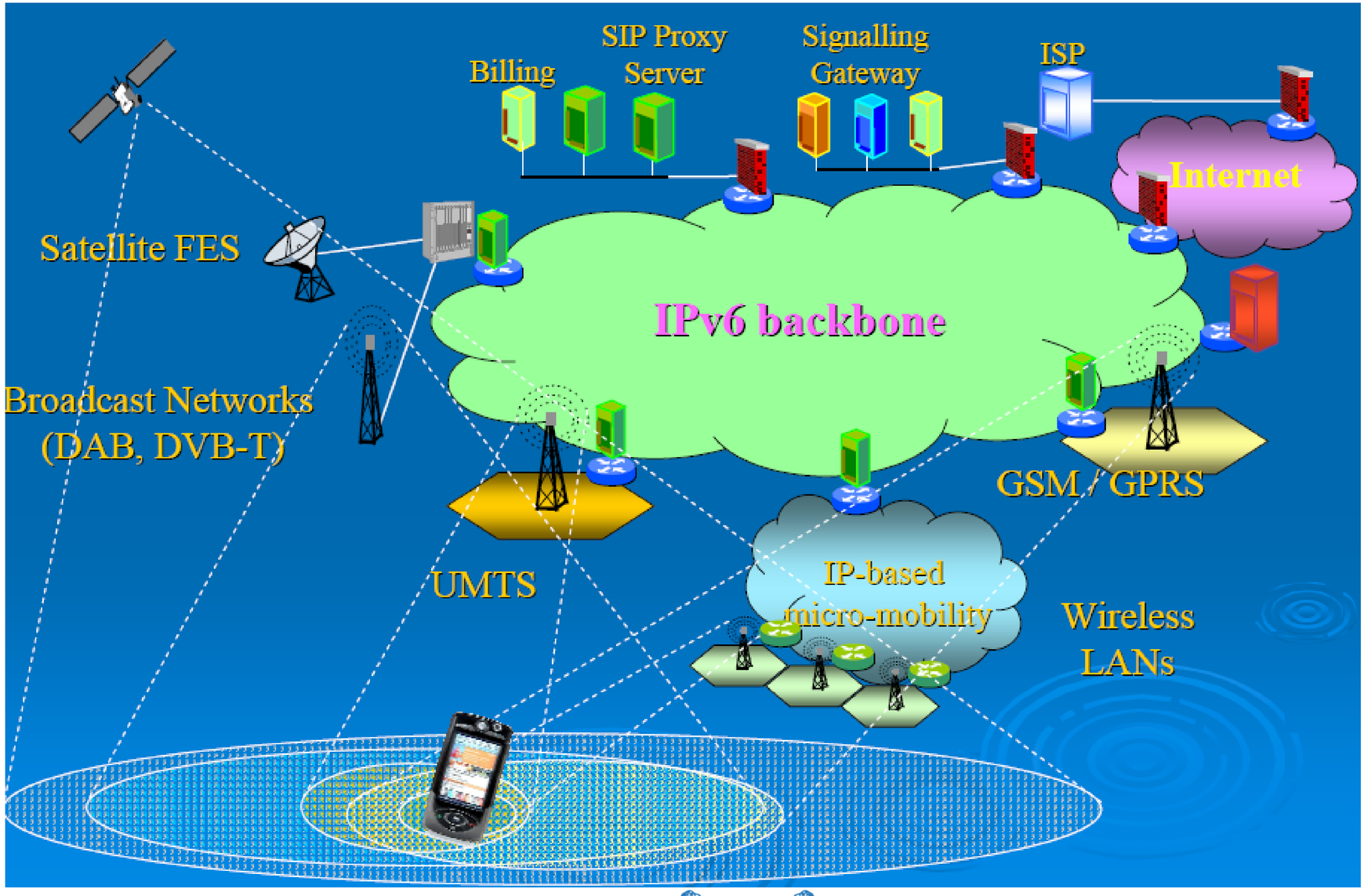
MS	Mobile Station
HLR	Home Location Register
VLR	Visitor Location Register
AUC	Authentication Center
EIR	Equipment Identity Register
OMC	Operation and Maintenance Center

GPRS System Architecture



Mobile Network Evolution




Billing
SIP Proxy Server
Signalling Gateway
ISP
Internet
Satellite FES
IPv6 backbone
Broadcast Networks (DAB, DVB-T)
GSM / GPRS
UMTS
IP-based micro-mobility
Wireless LANs

Linking to ISP

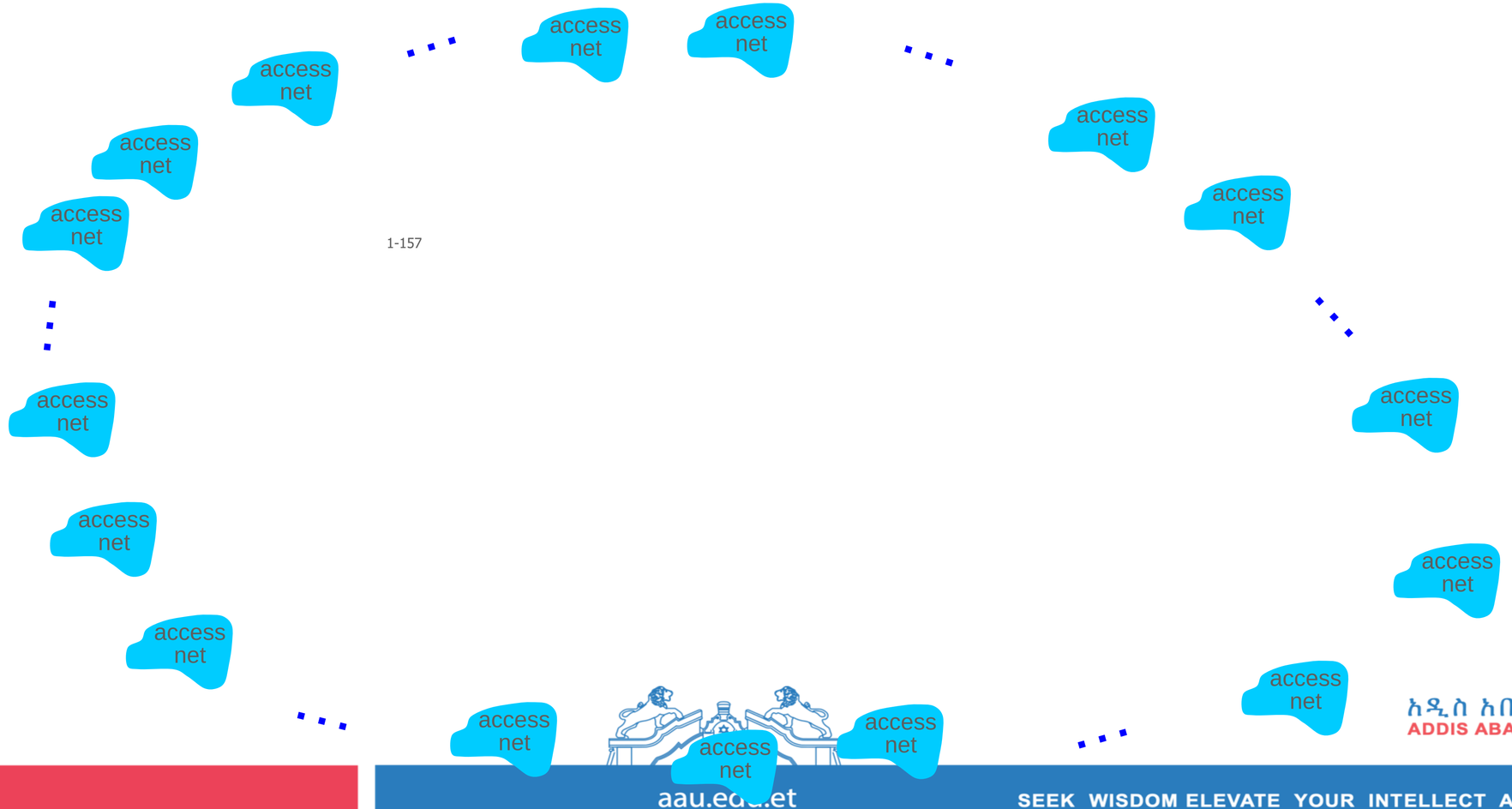
Adopted from Ross and Kurose (2017)

Internet structure: network of networks

- End systems connect to Internet via access ISPs (Internet Service Providers)
  - Residential, company and university ISPs
- Access ISPs in turn must be interconnected.
  - So that any two hosts can send packets to each other
- Resulting network of networks is very complex
  - Evolution was driven by economics and national policies
- Let's take a stepwise approach to describe current Internet structure

Internet structure: network of networks

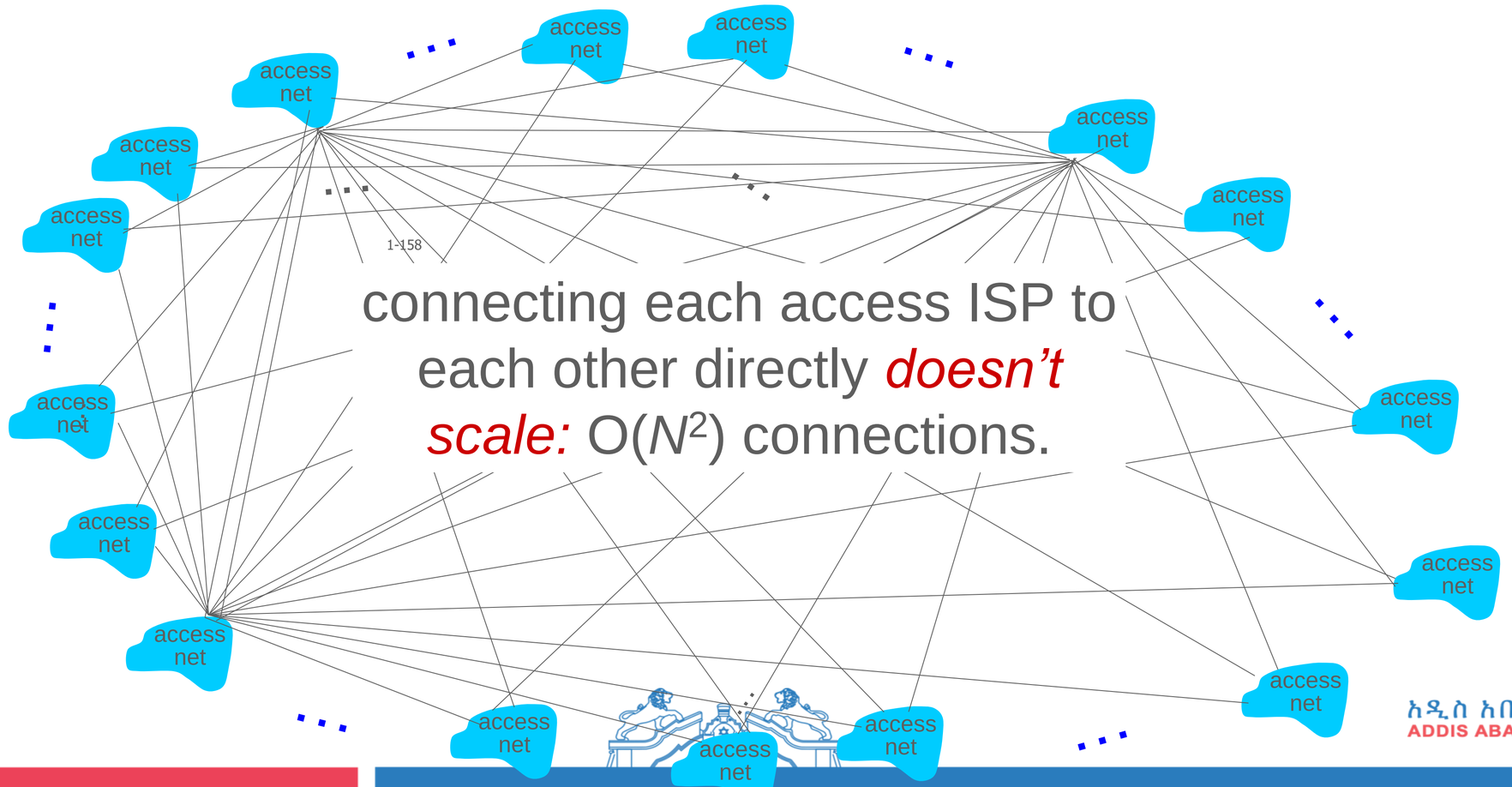
Question: given *millions* of access ISPs, how to connect them together?



1-157

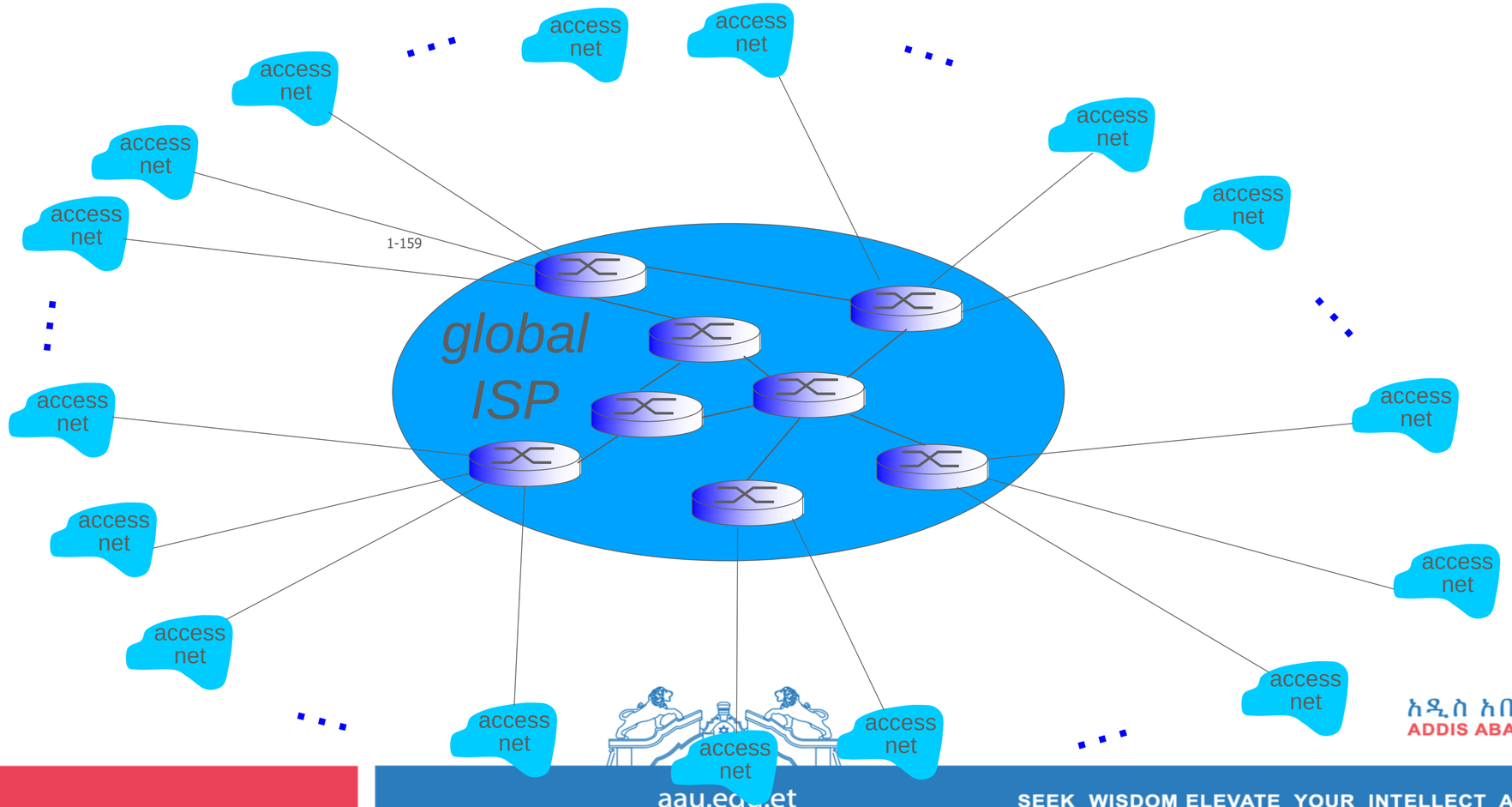
Internet structure: network of networks

Option: connect each access ISP to every other access ISP?



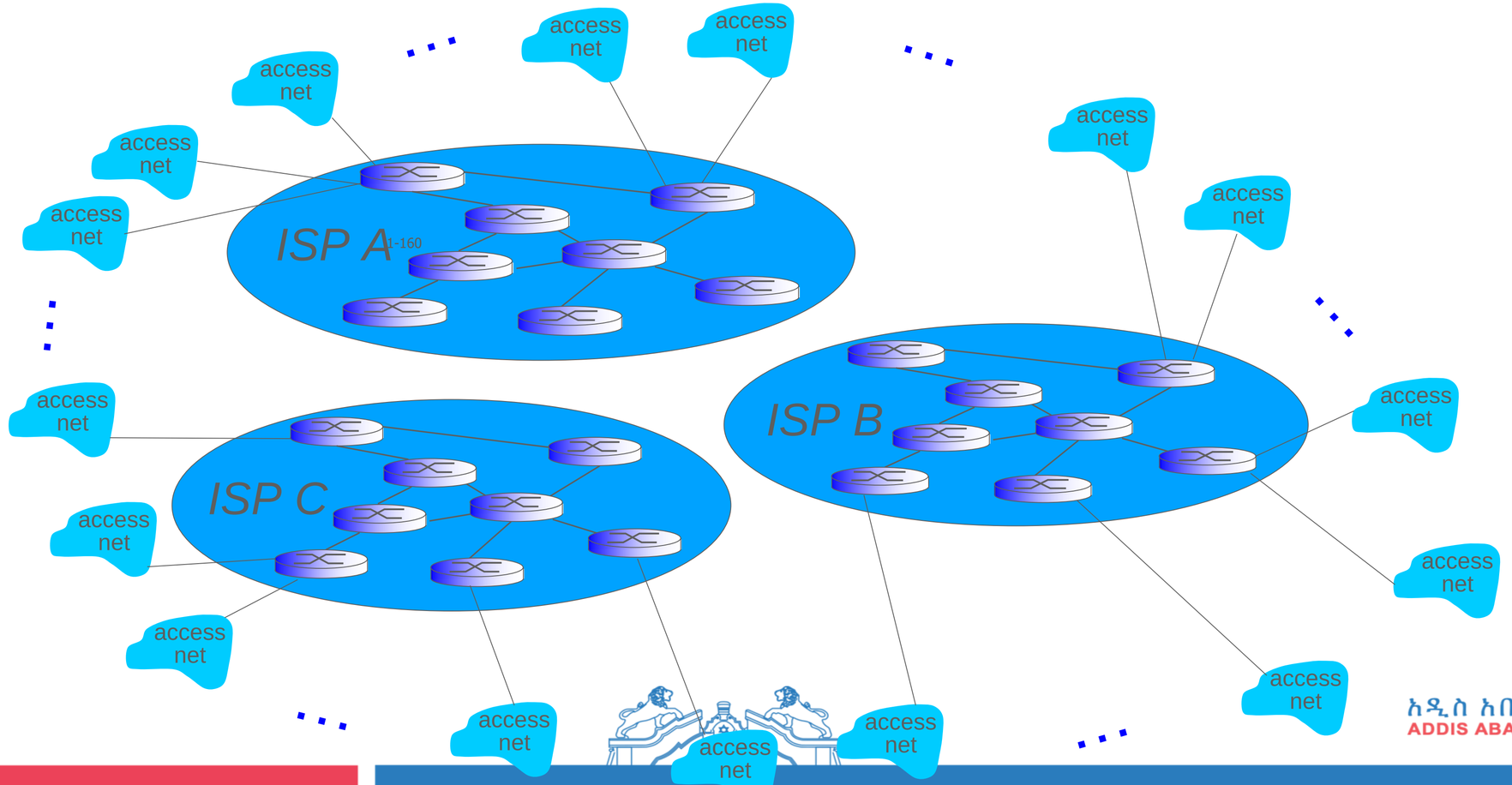
Internet structure: network of networks

Option: connect each access ISP to a global transit ISP? Customer and provider ISPs have economic agreement.



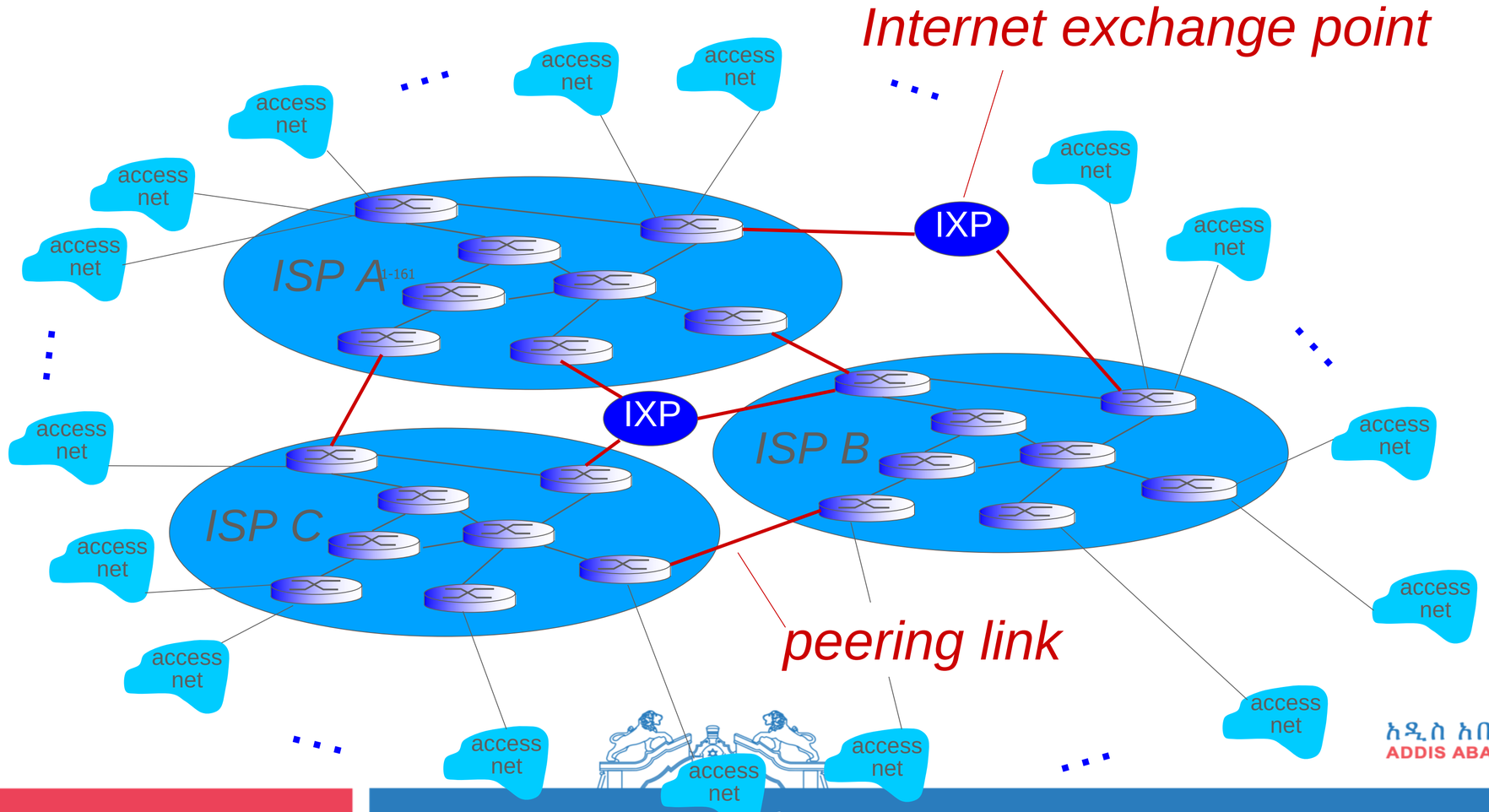
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors ….



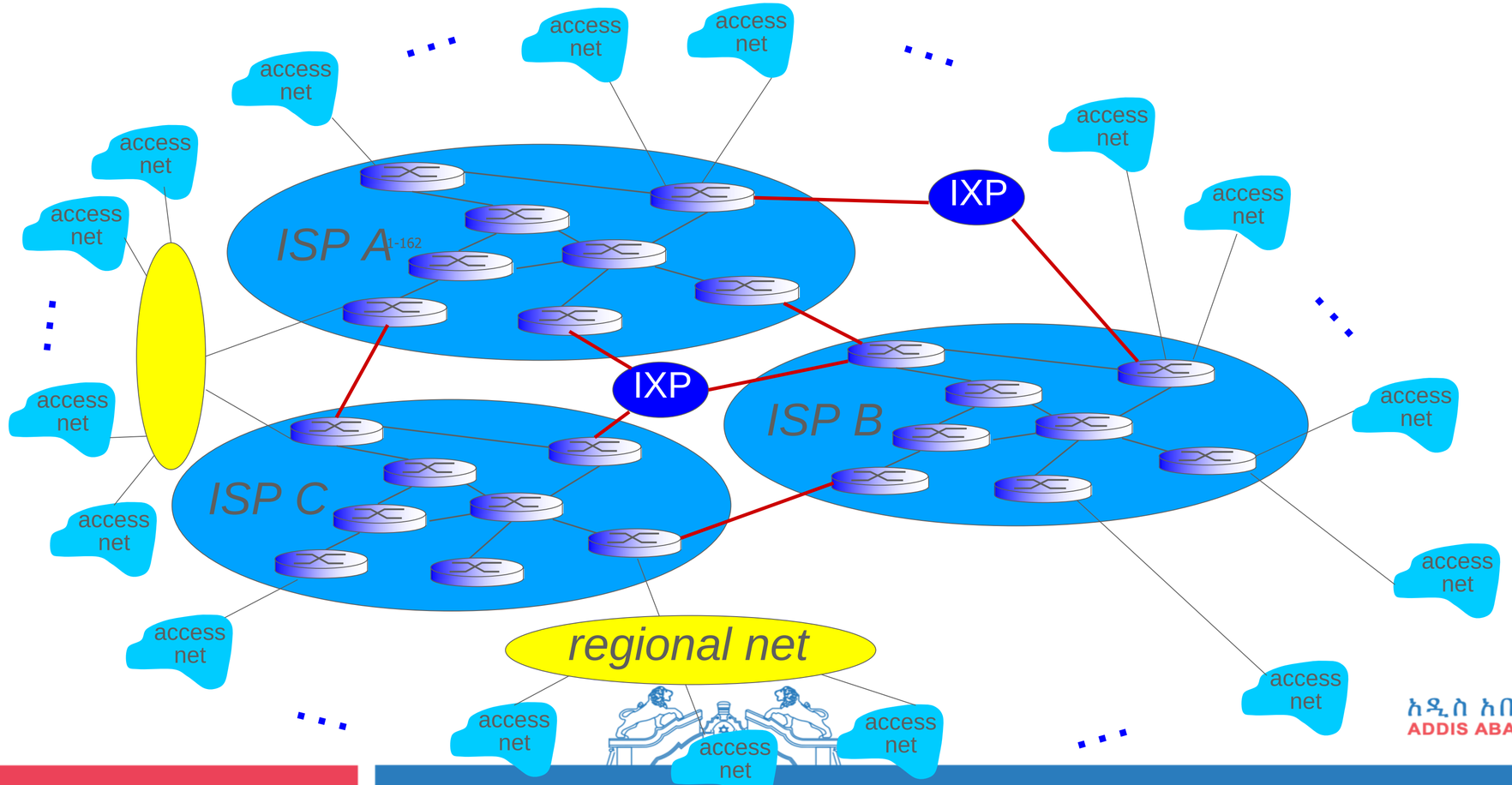
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors …. which must be interconnected



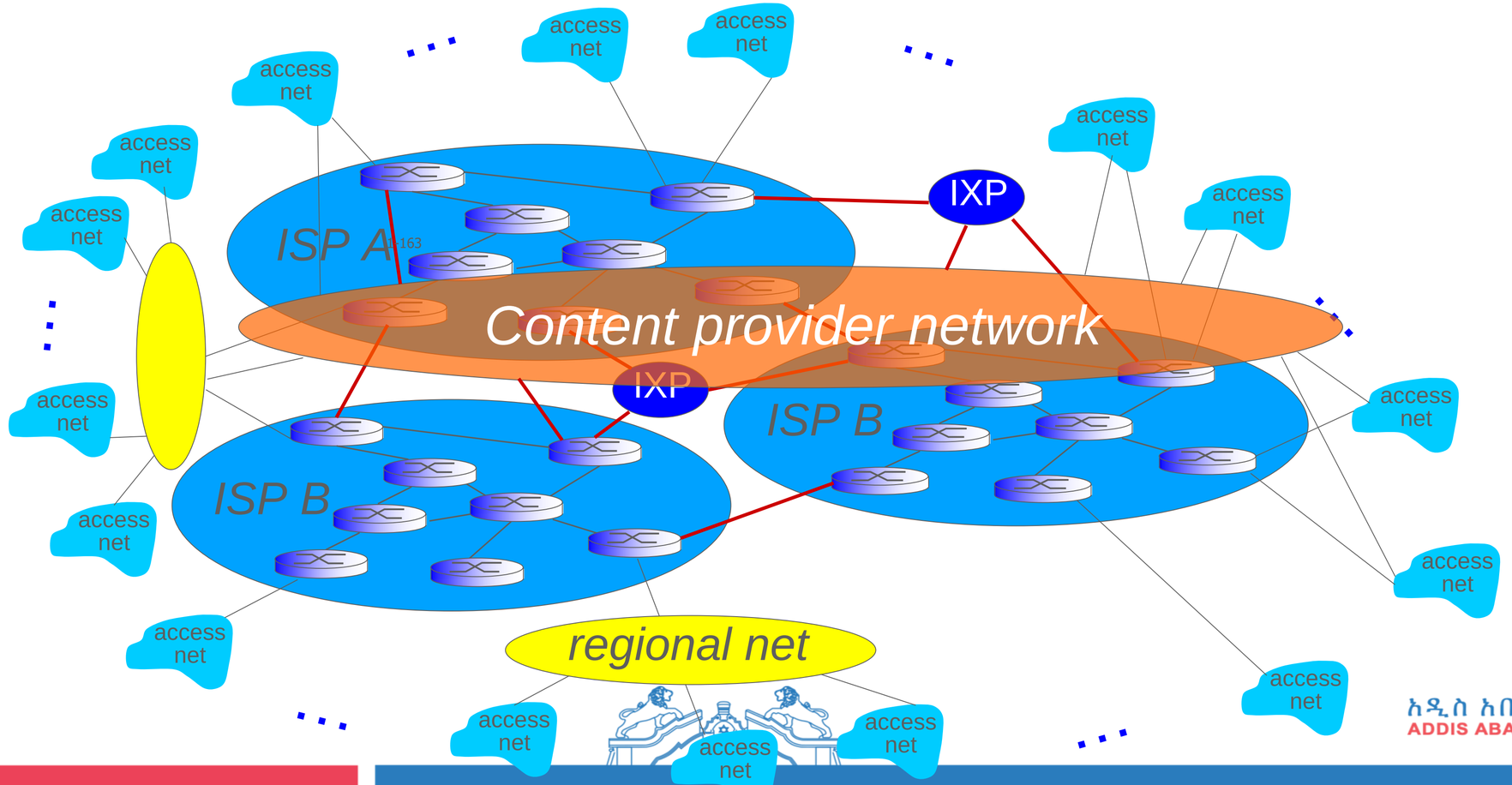
Internet structure: network of networks

… and regional networks may arise to connect access nets to ISPS

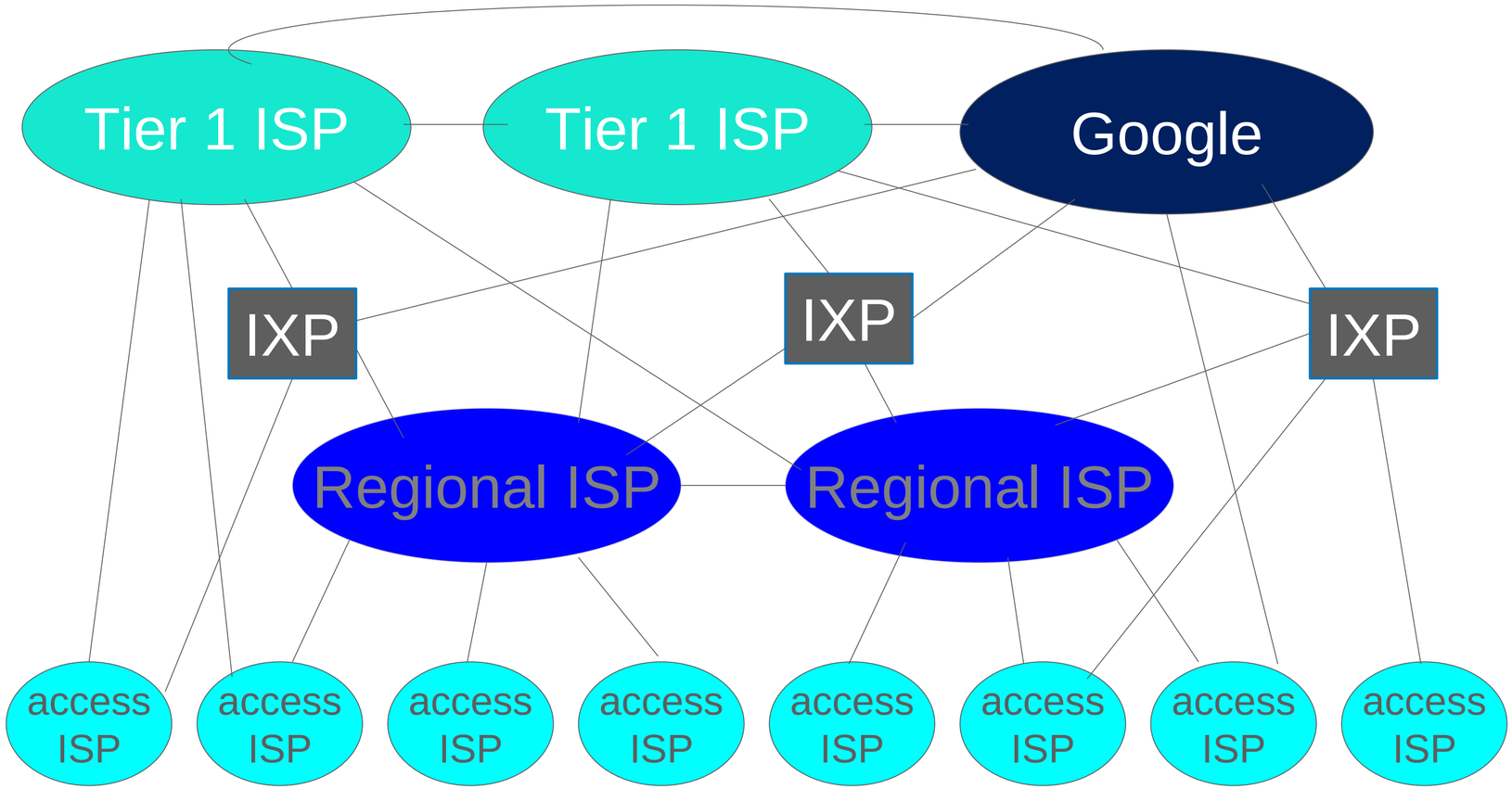


Internet structure: network of networks

… and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users



Internet structure: network of networks



- at center: small # of well-connected large networks
  - “tier-1” commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage
  - content provider network (e.g, Google): private network that

Security
IT Security
IS Security
Computer Security

Security - Overview

- What is security?
- Why do we need security?
- Who is vulnerable?

What is “Security”

- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.

  …etc.

Why do we need security?

- Protect vital information while still allowing access to those who need it – Privacy (Confidentiality)
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources -- Integrity
- Guarantee availability of resources
  - Ex: 5 9’s (99.999% reliability) -- Availability

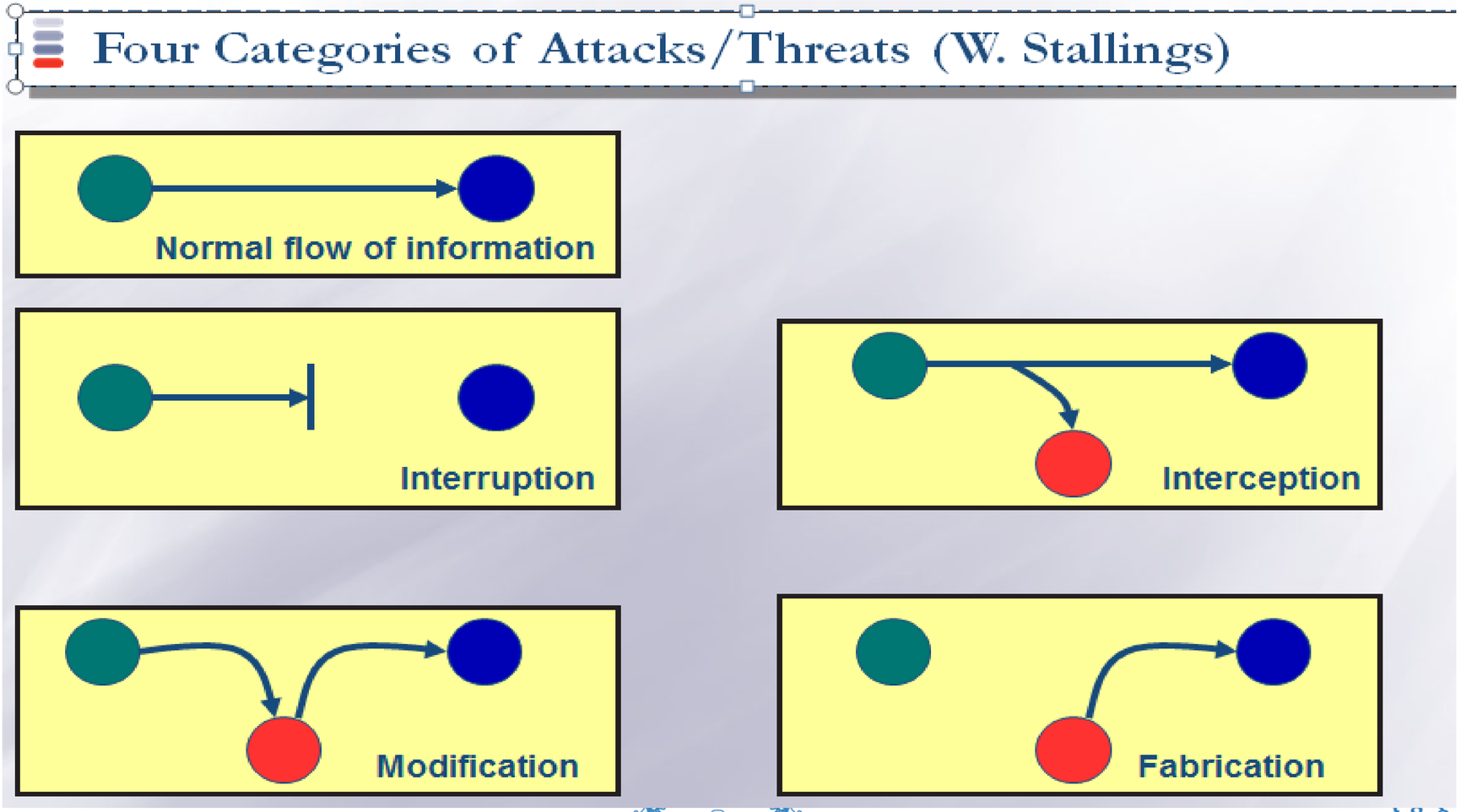
Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Security issues

- Computing in mobility is at a price
- Risk increase for sensitive critical information
- All systems are under attack
  - To build security system we need to know
    - The enemy
    - Vulnerability
    - Prevention (protection), detection, recovery

Categories of Network related attacks



Categorizing security

- Physical access
- Technological
  - Hardware & software - Application, OS and network
- Social & technological

Goals of security

- Prevention
- Detection
- Recovery

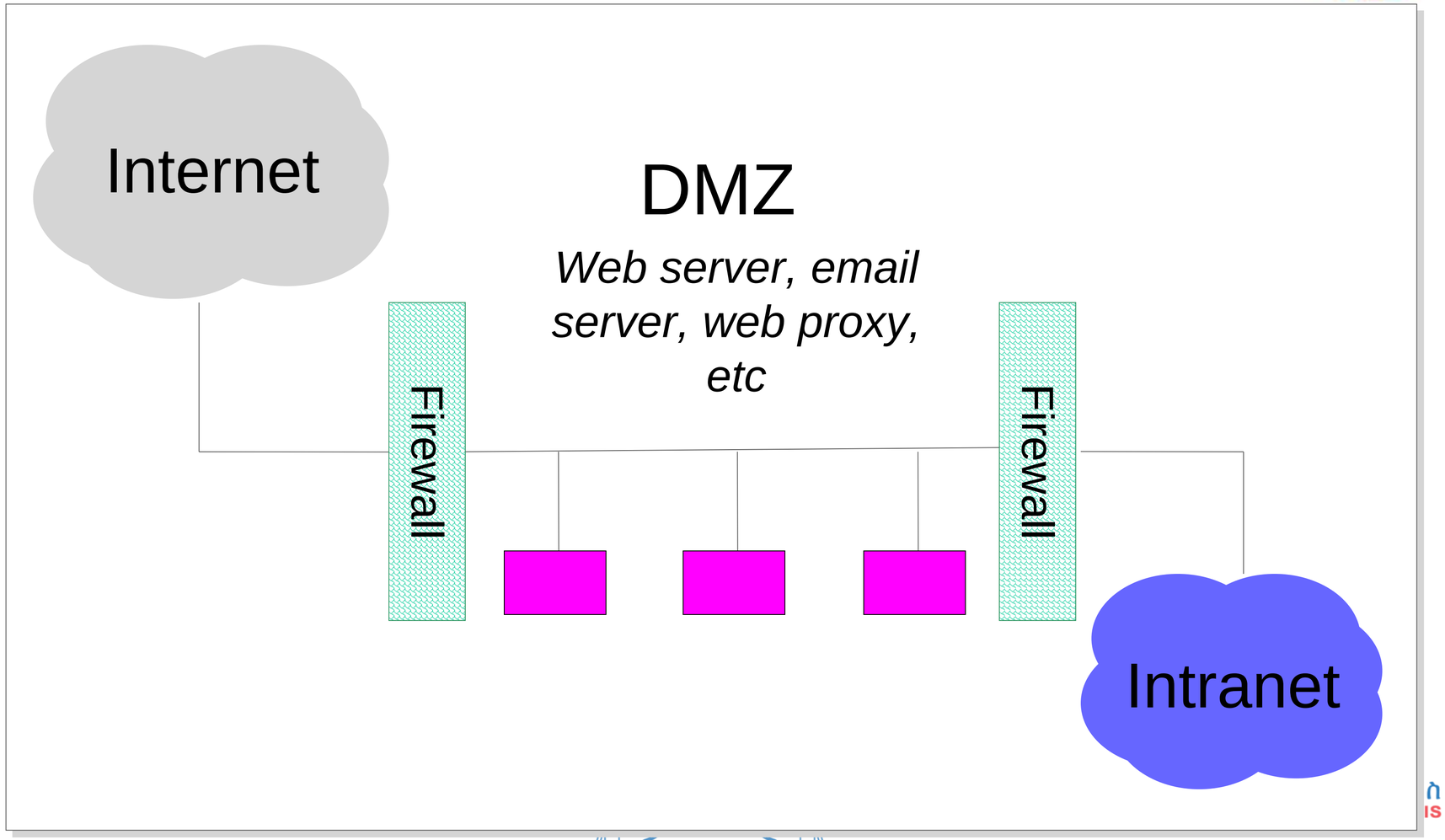
Solutions

- Firewall
- Intrusion Detection Systems (IDS)
- Cryptography

Firewall

- Packet Filtering
- Network Address Translation
- Demilitarized Zone (DMZ)

Firewalls


Internet
DMZ
Web server, email server, web proxy, etc
Firewall
Firewall
Intranet

IDS

- Network vs Host-based IDS
- Misuse vs Anomaly based IDS

Cryptography

- *Cryptography is the science of using mathematics to encrypt and decrypt data.*
- Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
- Is the science of sending messages secretly

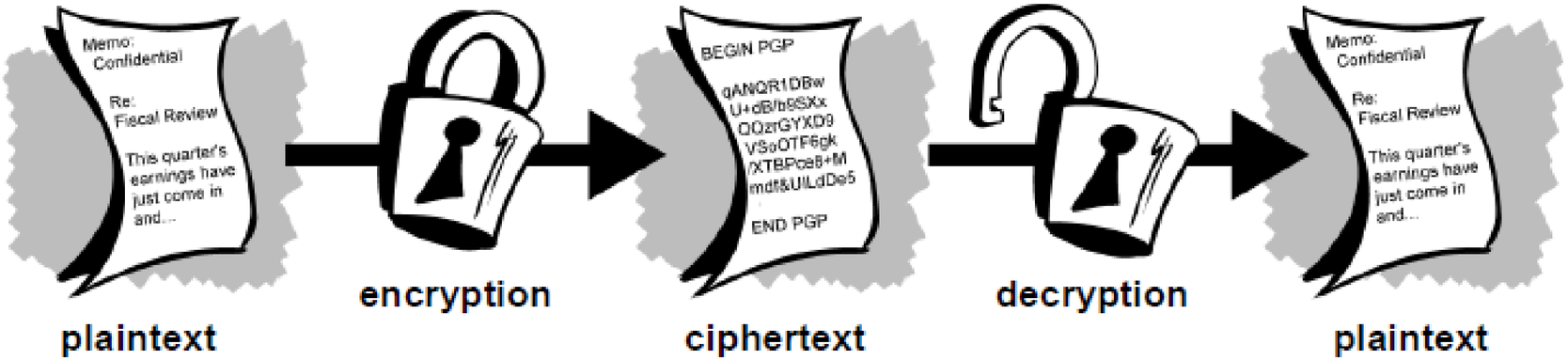


Figure 1-1. Encryption and decryption

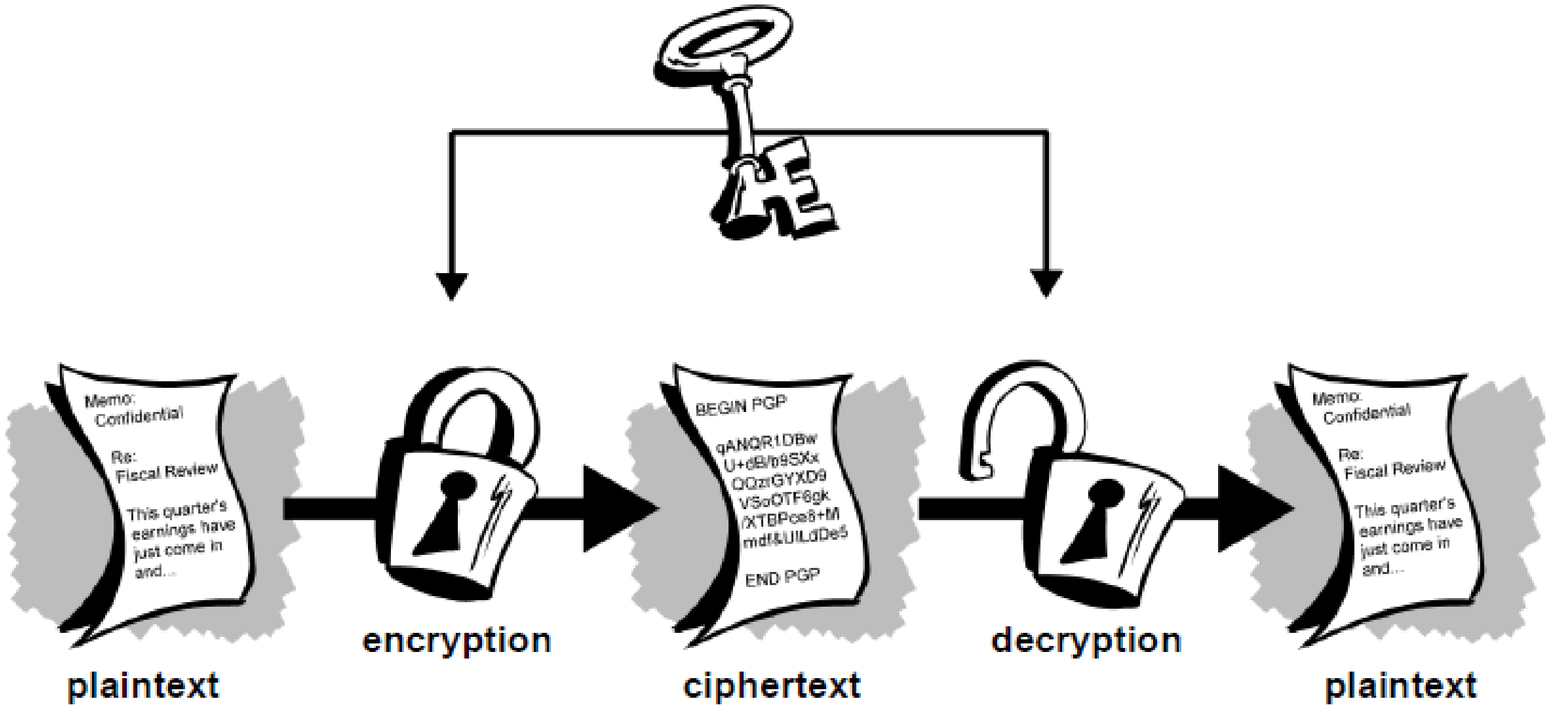


Figure 1-2. Conventional encryption

Caesar’s Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

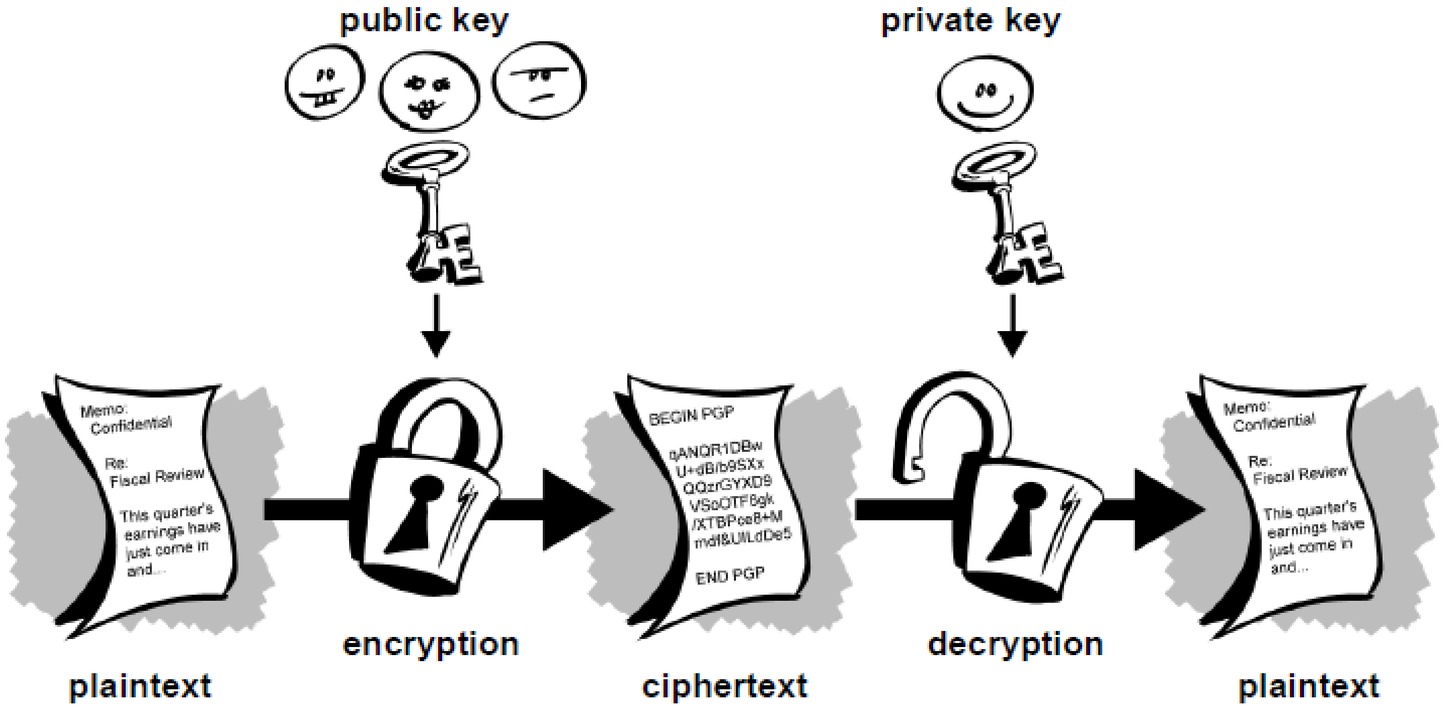


Figure 1-3. Public key encryption

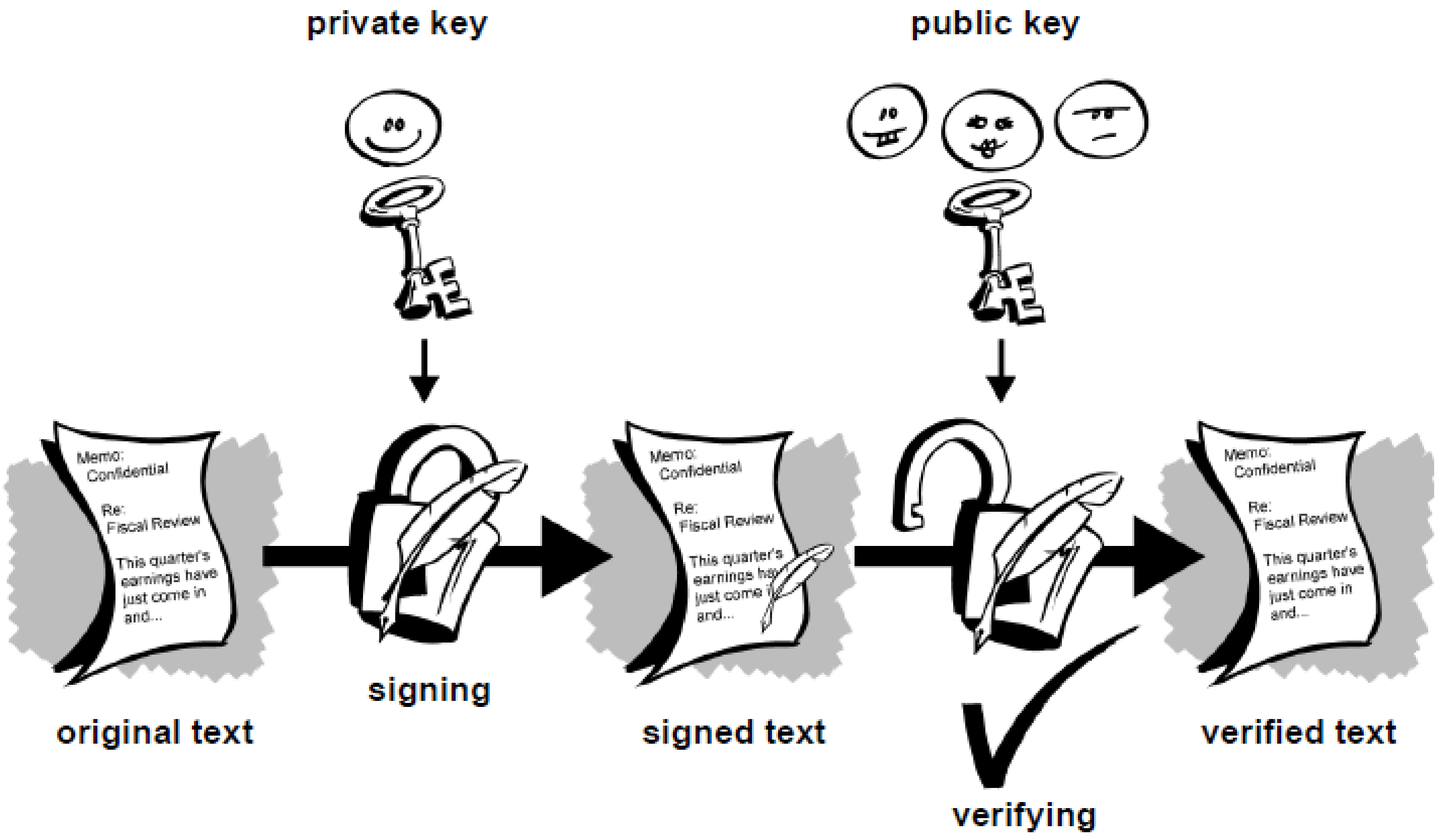


Figure 1-6. Simple digital signatures