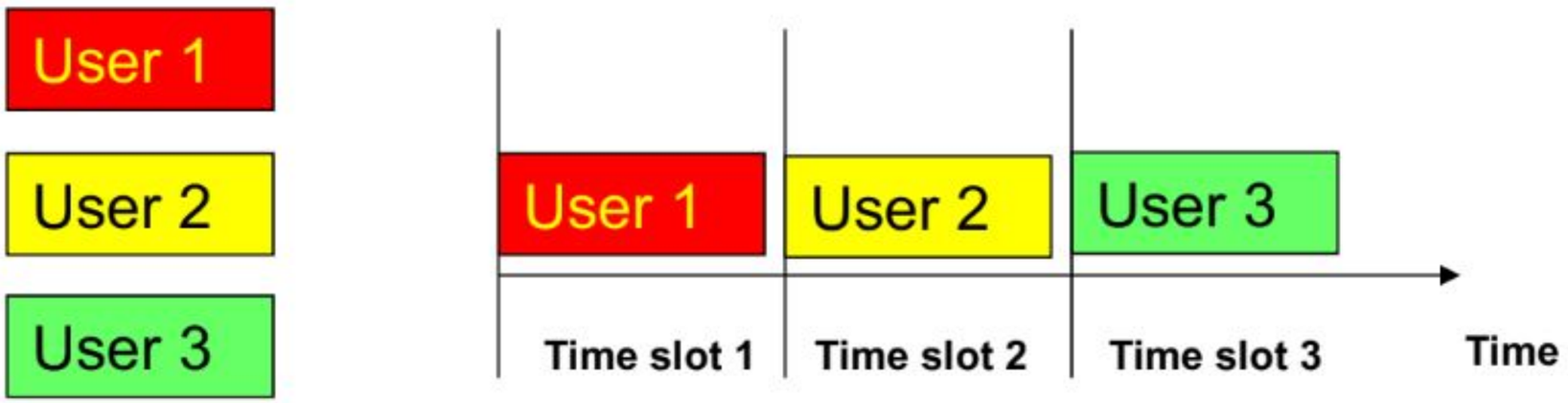
Physical Layers of Networks

Modulation

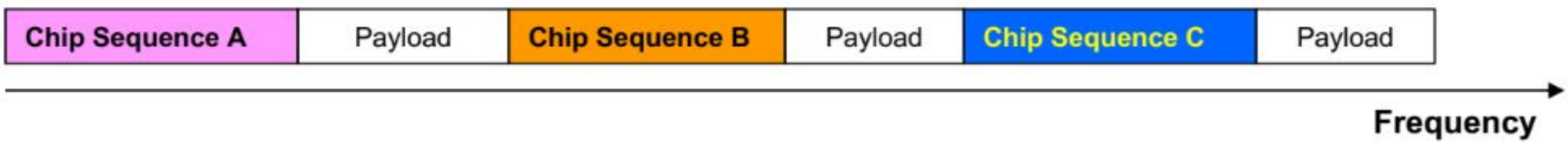
TDM (Time Division Multiplexing):

- The users will use time slots to transmit the information.
- Is used in telephone networks PSTN (Public Switched Telephone Network)



Code Division Multiplexing:

One frequency is shared by multiple users.



Is used in cellular and satellite communications

Physical Layers of Networks

➢ PSTN (Public Switched Telephone Network)

❑ TDM (Time Division Multiplexing)

T1 and E1 Structures and Formats:

DS-n : DS (Digital Signal) is digital transmission hierarchy scheme.
n is Digital multiplexing level.

T1: 24 channels each 8 bits, 24 x 8 = 192 +1(for control or framing)= 193

T1 rate: 1.544 Mbps

E1: 0-31 channels each 8 bits, 32 x 8 = 256, 8 bits at the beginning for control or framing

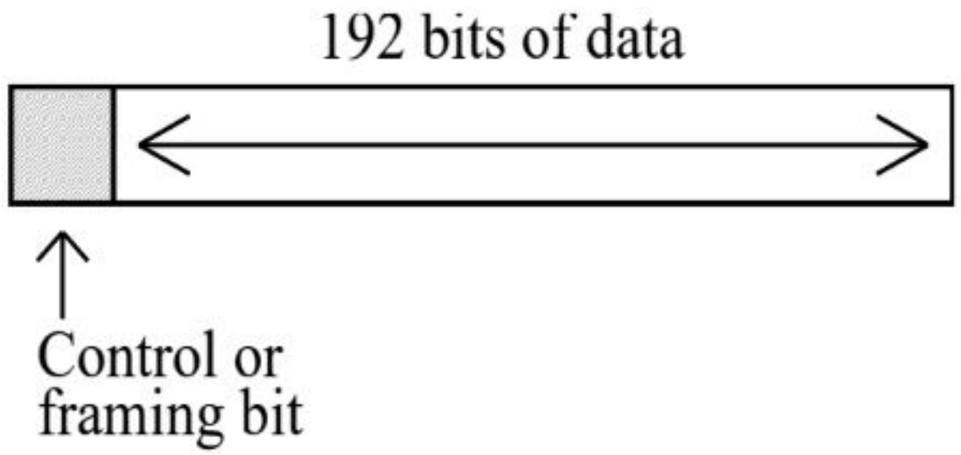
E1 rate: 2.048 Mbps

T1: 8000 slots/sec X 7 bits per slot = 56000 (clear channel)
8 x 24 = 192 bits 8000 x (192 +1) = 1.544 Mbps

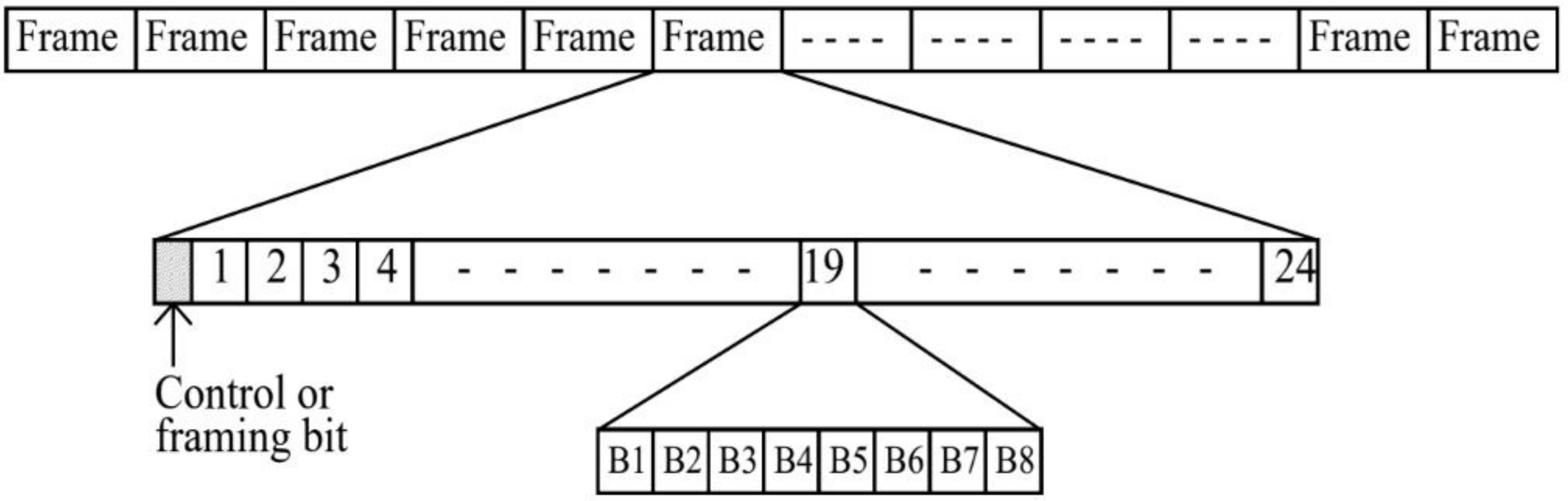
Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
  - **TDM (Time Division Multiplexing)**

T1 and E1 Structures and Formats:



8000 frames per second 1.544 Mbps



Physical Layers of Networks

PSTN (Public Switched Telephone Network)

TDM (Time Division Multiplexing)

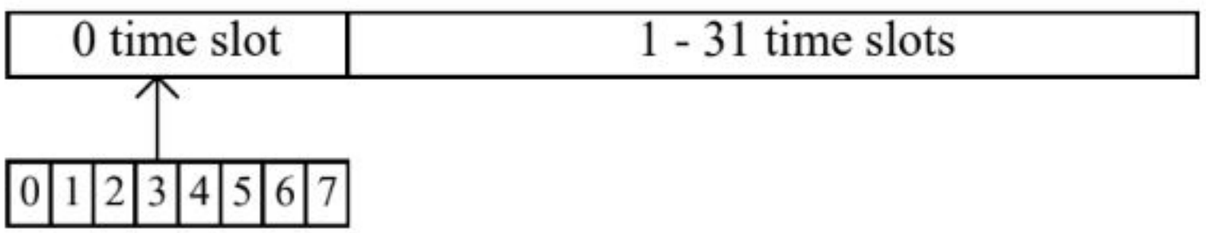
T1 and E1 Structures and Formats:

T1:

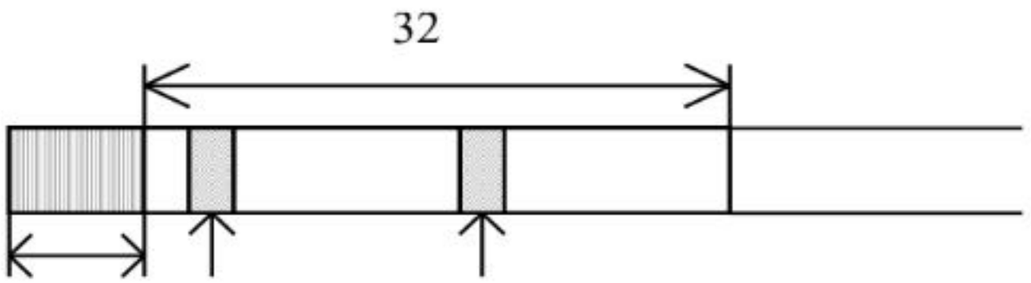
- It has 8000 frames per second and operates at 1.544 Mbps.
- The fractional trunks use only as many 64 Kbps channels as needed.
- In fractional T1 or E1, will use the 64 Kbps increments, not using the whole T1 channel capacity.
- **Synchronization:** In time slots **4, 8, *12*, 16, 20, and 24th** the six altering (110100) bits are used for synchronization, the rest of 12 bits used for OA&M.
- **In-Band signaling:** Robbed bits signaling the **A, B, C, and D** bits overwrite the least significant bit of every time slot in the **6, 12, 18, and 24th** of T1 frame.
  Only 7 bits could be used, in new version of T1 the signaling is **out of band** all 8 bits could be used.

E1:

- E1 is defined from CEPT (Previous ITU), it has a rate of 2.048 Mbps.
- It has 32 channels.
- Channel 1 is used for frame alignment and CRC-error checking
- Channel 16 is used to carry circuit signaling
- E1 frame size is 32 channels x 8 bits = 256 bits



8-bits used for frame alignment



Physical Layers of Networks

➢ Modulation

Adding information to a carrier signal.

Processing the source signal to be transmitted on the media.

The modulator will vary properties of Carrier signal with a signal that has the information and to be transported.

The properties of carrier signal are phase, amplitude, and frequency.

❑ Passband:

The passband is the range of frequencies or wavelengths that can pass through a filter.

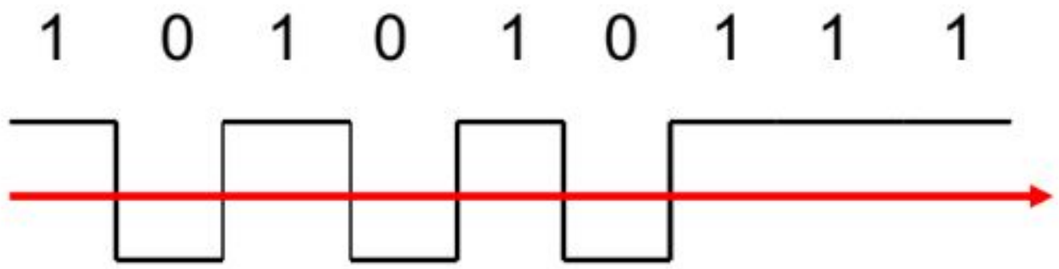
Car radio receiver has a band pass filter to tune to desired frequency signal from all radio frequencies received by antenna.

❑ Modulation Types:

NRZ (Non-Return-to-Zero)

Positive voltage 1

Negative voltage 0



Physical Layers of Networks

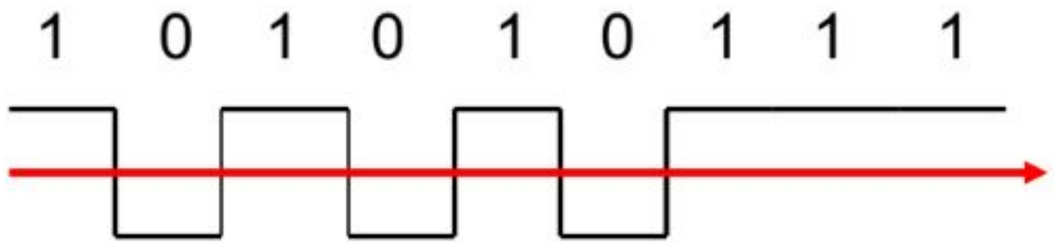
- **Modulation**

- **Modulation Types:**

NRZ (Non-Return-to-Zero)

Positive voltage 1

Negative voltage 0



Number of bits per signal transition is 2, requires two signal transitions to transmit 1,0 transitions.

No. of bits can be transmitted is B/2

Efficiency:

Send more bits per transition. The transition is half the bit rate.

The two bits are one symbol that we transmit.

bit rate = symbol rate * number of bits per symbol

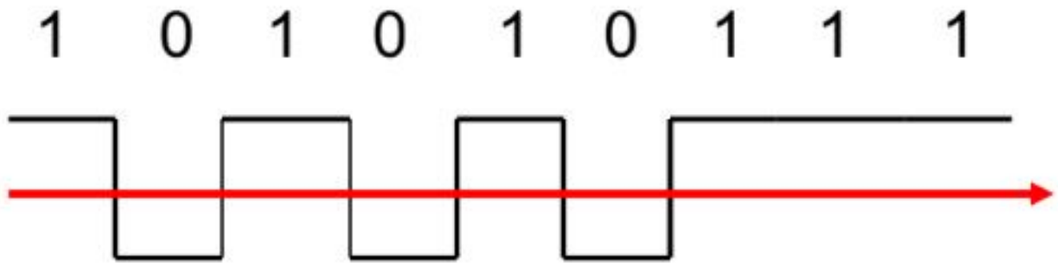
Baud rate in telephony is symbol rate

Physical Layers of Networks

➢ Modulation

❖ Modulation Types:

NRZ (Non-Return-to-Zero):



❑ Too Many 1 or 0 bits received:

If many 0s and 1s transmitted in NRZ encoding the clock recovery will be difficult.

NRZI will provide some solution, but not complete.

❑ 4B/5B (4 Bit/5 Bit):

4 bits are transmitted as 5 bits.

The 5 bits provide more transition to bit patterns.

❑ Scrambling bits XOR with random pseudo number:

TX: bits XOR random pseudo number

RX: bits XOR with the same TX random pseudo number

Physical Layers of Networks

- **Modulation**

- Modulation Types:

Balanced signal:

- Provides equal number of positive and negative volts over defined period of time.
- The DC (Direct Current) is filtered before transmission.

AMI (Alternate Mark Inversion):

- **Bipolar encoding:** provides equal number +/- volts.
- **AMI** uses 4B/5B or 8B/10B to add voltage.
- 0000 is mapped to 10101.

Passband:

In one physical channel multiple frequencies can be used for transmission

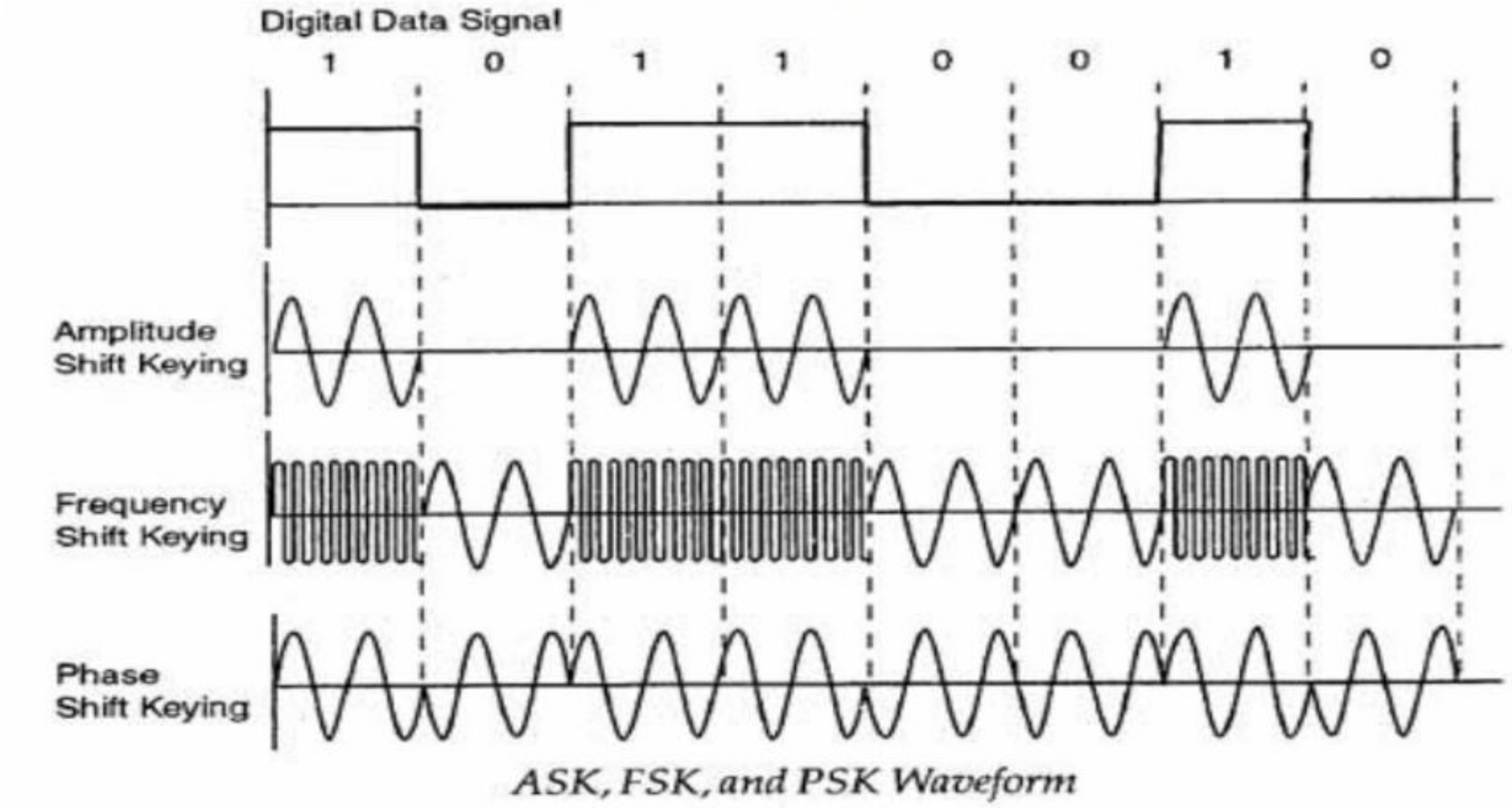
Physical Layers of Networks

➢ Modulation

Adding information to a carrier signal.
The baseband signal will be included in a passband, the result will be = Baseband + passband

❖ Digital Modulation Types:

- ❑ ASK (Amplitude Shift Keying) Modulation
- ❑ FSK (Frequency Shift Keying) Modulation
- ❑ PSK (Phase Shift Keying) Modulation



ASK, FSK, and PSK Waveform

Physical Layers of Networks

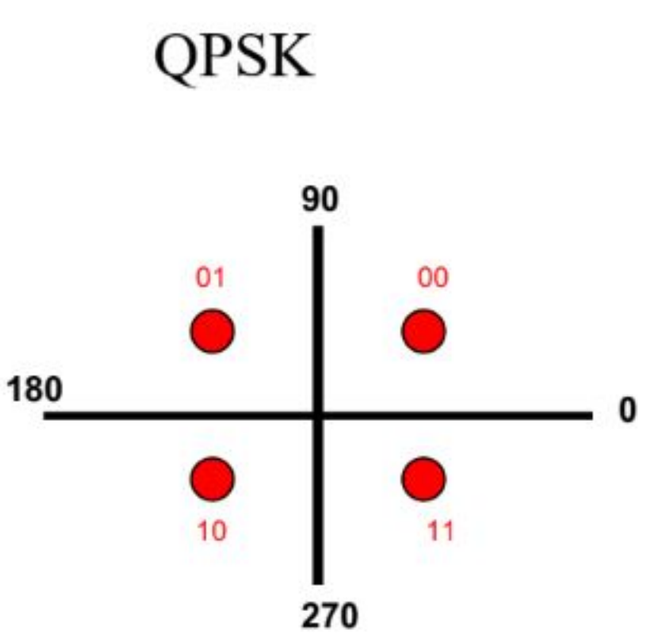
Modulation

Combining phase and amplitude or frequency and phase for modulation.

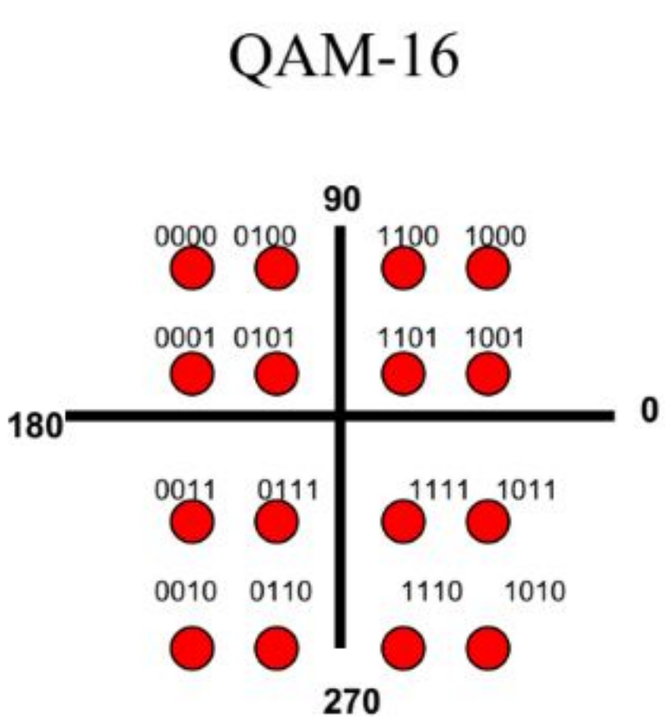
- Modulation Types:
  - QPSK (Quadrature Phase Shift Keying) Modulation carries 2 bits per symbol
  - QAM-16 (Quadrature Amplitude-16) Modulation, carries 4 bits per symbol
  - QAM-64 (Quadrature Amplitude-64) Modulation, carries 6 bits per symbol

Constellations:

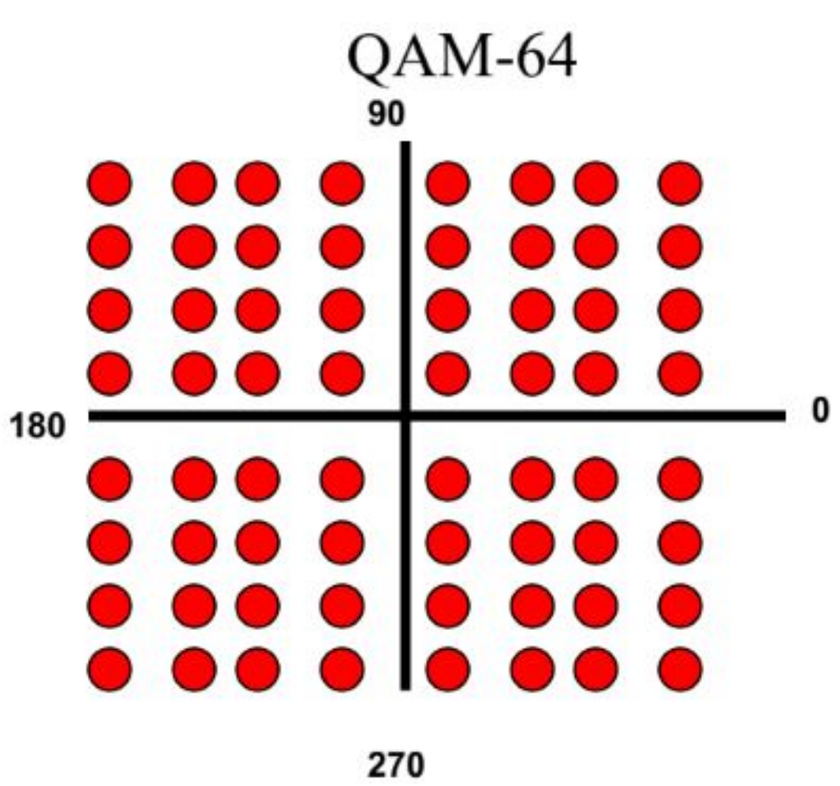
QPSK



QAM-16



QAM-64



Error correction: Gray code provides a method to make correction, neighbor symbols have only one bit that is different from each other.

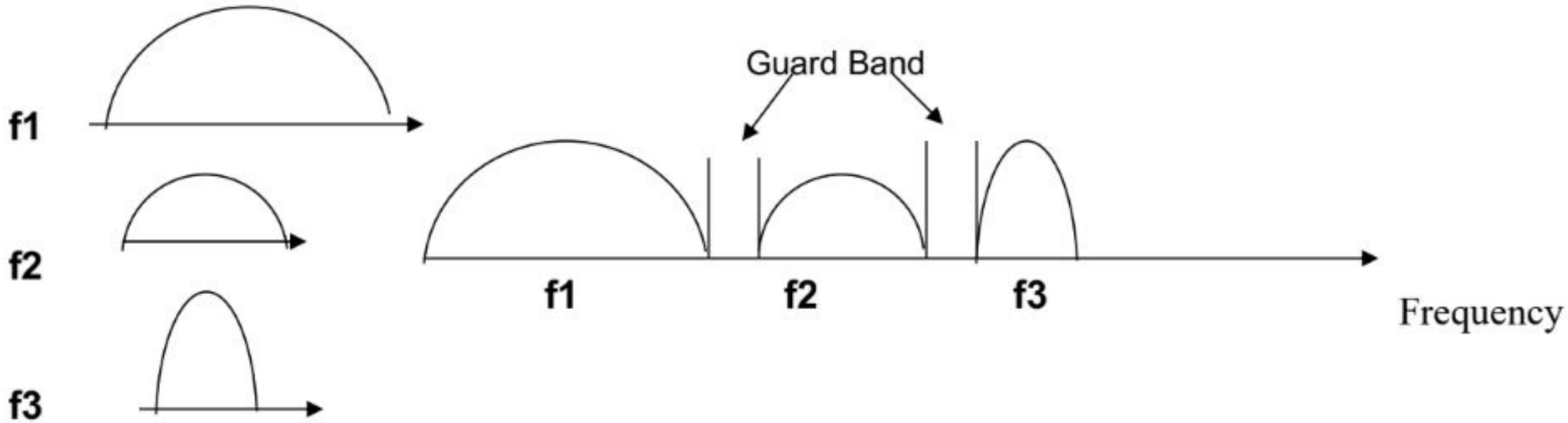
Physical Layers of Networks

Modulation

FDM (Frequency Division Multiplexing):

Individual users use different frequency to transmit.

All frequency channels are **multiplexed** together and transmitted.



OFDM (Orthogonal Frequency Multiplexing):

Provides solution with out guard band, the spectrum is subdivided in sub-channels.

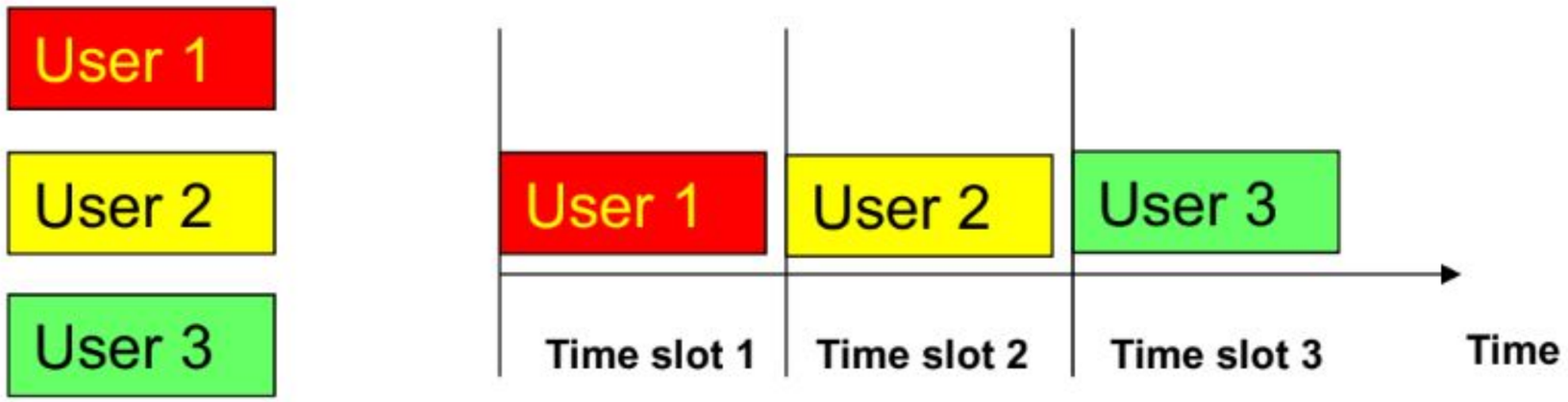
Using QAM (Quadrature Amplitude Modulation)

Physical Layers of Networks

Modulation

TDM (Time Division Multiplexing):

- The users will use time slots to transmit the information.
- Is used in telephone networks PSTN (Public Switched Telephone Network)



Code Division Multiplexing:

One frequency is shared by multiple users.

Is used in cellular and satellite communications

Physical Layers of Networks

- **PSTN (Public Switched Telephone Network):**
  - It provides services in the last mile.
  - Telephone was invented in 1876 and patented.

Structure of PSTN:

- **End office (local central office):** Connects subscriber with two copper wires (Cat 3) to network (distance 1-10 Km), analog signal.
- **Local loop:** Consists of the two wires connecting users to network, the local loop carries analog signal.
- **Toll Office:** Multiple local offices are connect to toll office, these lines are toll connecting trunks.
- **Toll trunks:** Toll offices are connected by inter toll trunks (analog signal) to intermediate switches
- **Intermediate switches:** connect toll offices to each other.
- **LATA (Local Access and Transport Area):** Coverage are of area code.
- **IXC (IntereXchange Carrier):** Provides connectivity between LATAs,

  IXCs have tandem offices.

Physical Layers of Networks

- **Physical Media types**

2) **Unguided Media**

- **Wireless Transmission:**

I. **Radio Transmission**

- ITU regulates frequency bands in the world , FCC (Federal Communication Commission) in US, Unlicensed National Information Infrastructure band is not regulated (5 GHz).
- ISM (Industrial Scientific Medical) 57-60 GHz are used by household.

a) **High Frequency**

Absorption by snow, rain

Power reduction by increased distance between TX an RX

Reflection on obstacles, energy reduction (Path loss)

b) **Low Frequency**

Can go through objects

Power reduction by increased distance between TX an RX

Low frequency radio signals travel longer distances because they can go through obstacles.

Ionosphere (charged layer about 500 Km above earth) will reflect the signal which extends reach ability.

Physical Layers of Networks

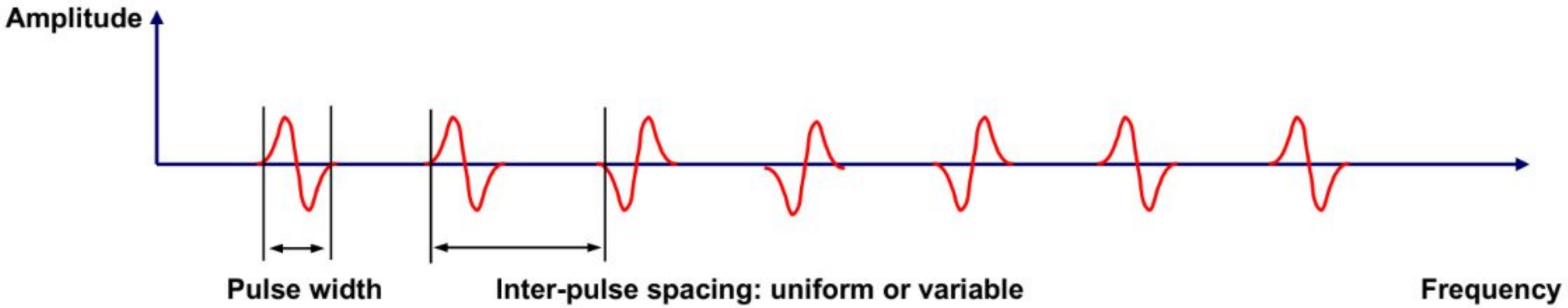
- **Physical Media types**

2) **Unguided Media**

- **Wireless Transmission:**
  - **Spectrum usage:**

c) **UWB (Ultra Wide Band)**

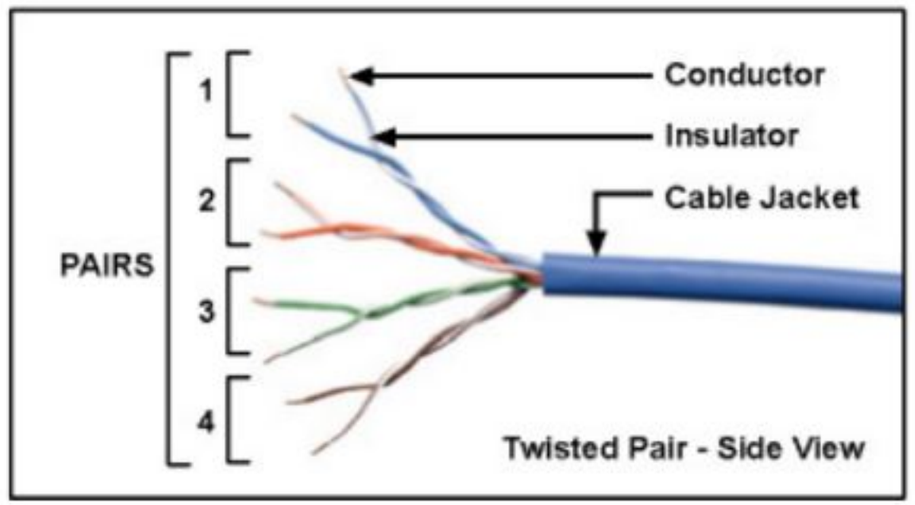
- UWB signals are modulated pulses with very short pulse duration (<1 ns) flows
- Pulse repetition frequency (PRF) from hundreds to billions of pulses/second.
- UWB is a form of extremely wide spread spectrum where RF energy is spread over gigahertz of spectrum.
- Power seen by a narrowband system is a fraction of the total.
- FCC limits ensure that UWB emission levels are exceedingly small.



Physical Layers of Networks

- **Physical Media types**
  - **Guided media: Fiber optics, metal, coax, disk**
  - **Unguided Media: RF (Radio Frequency)**

1) Guided Media



Twisted pair: consists of pairs

Cat 5: Has two pairs:

- **One pair is used by 100 Mbps Ethernet.**
- **Two pairs are used for 1 Gbps Ethernet.**

Cat 3: Has more twists, used for high speed transmission.

Cat 6: UTP (Unshielded Twisted Pair) used for 100 Gbps.

Cat 7: It is Shielded Twisted Pair used for 100 Gbps.

Transmission types:

- **Full duplex: Transmission in both directions simultaneously.**
- **Half duplex: Transmission in both directions but one at a time.**
- **Simplex: Transmission only in one direction.**

Physical Layers of Networks

- **Physical Media types**

1) **Guided Media**

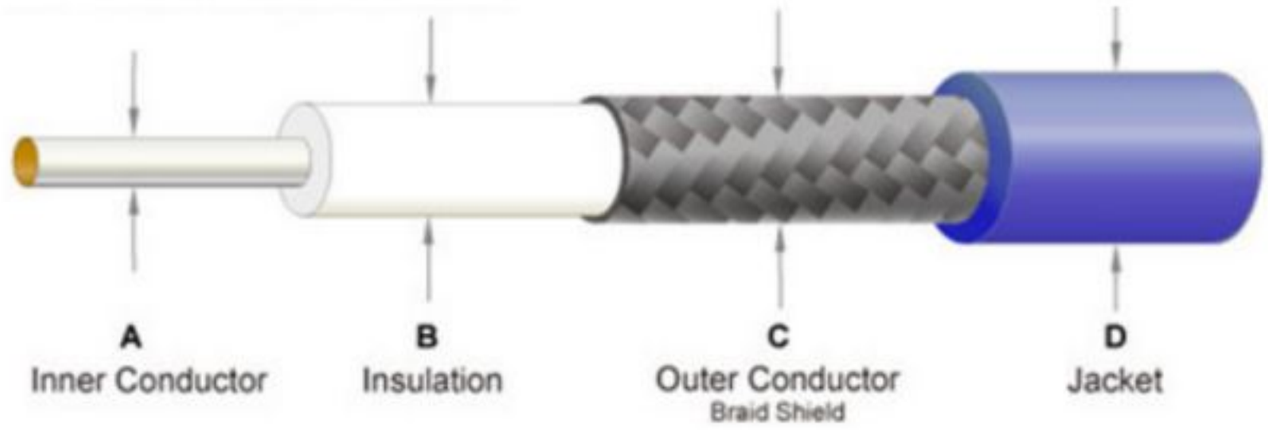
- **Coaxial Cable:**

Two types are used:

a) **50 ohm for digital transmission**

b) **75 ohm for analog transmission**

Used for Cable TV and telephony.



- **Electrical Power Line:**

a) **Outside homes for Internet broadband communications**

b) **Inside homes for LAN data connections**

Will catch home appliances signals and other signals which need to be filtered.

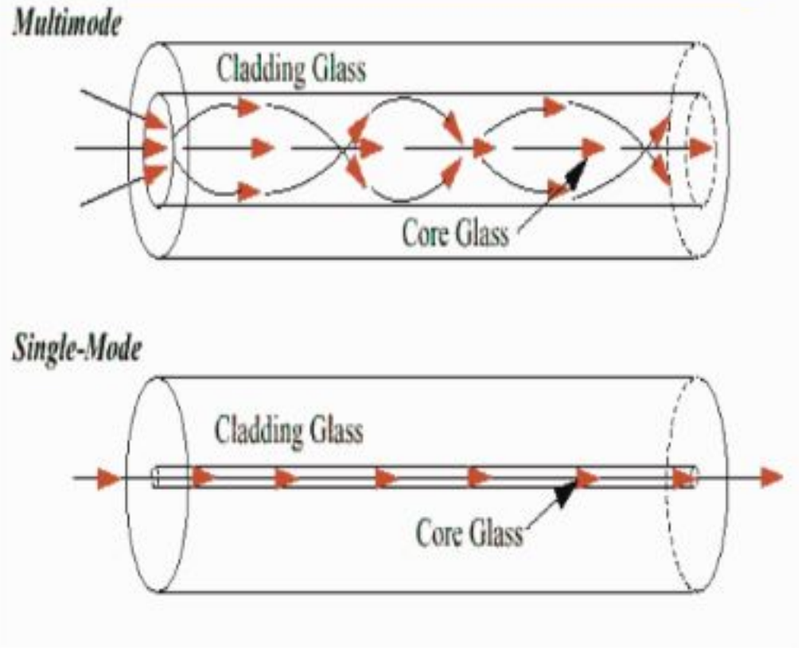
Physical Layers of Networks

- **Physical Media types**

1) Guided Media

- **Fiber Optics:**

a) Multi Mode Fiber



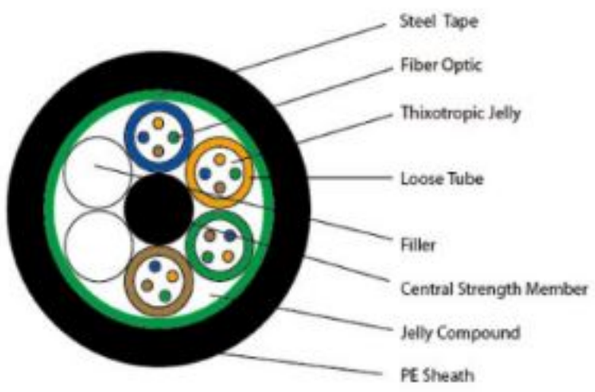
Multi Mode Fiber: The light will bounces in fiber and causes multiple rays.
They bounce in the same fiber glass.

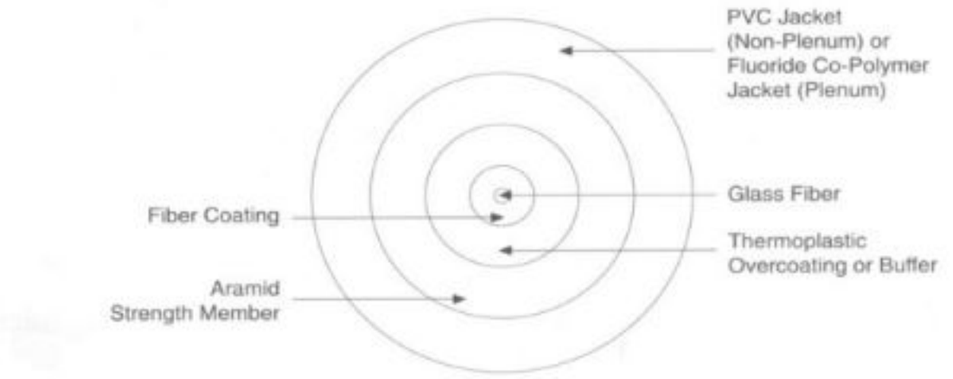
b) Single Mode Fiber:

It carries multiple wave lengths, propagates the signal in straight line.
Transports many 100 Km, the bandwidth 100 Gbps.

c) Fiber Cables:

They don't have braid, they are like fiber optics.





Tight-Buffered Cable

- Networks:

❖ RFID (Radio Frequency IDentification), sensor Networks

Is used for object tracking.

- **Tags: Are affixed to objects, contains an antenna and tag has id which is embedded in a chip.**
- **RFID reader: will sent signals to tag when the object is in coverage area of reader will send its ID to reader.**

Two type of RFID devices:

1) **Passive RFID: It will be activated by an RFID reader, by itself does not have any power supply, battery or electric powered.**
2) **Active RFID: It has power, battery or line powered.**

- **Backscatter, UHF RFID (Ultra High Frequency RFID), few meters distance: Tags reflect the received RFID reader's signals and RFID reader can process the signals (Used for Shipping objects).**
- **HF RFID (High Frequency RFID): will operate based on induction received signal of RFID reader, the tag will send its ID to RF reader (Pass port).**
- **LF RFID (Low Frequency RFID): Is used for animal movement monitoring**

Introduction to Networks

➢ Networks:

❖ RFID (Radio Frequency IDentification), sensor Networks

The response of multiple tags responses can cause collision, if collision detected CSMA is used.

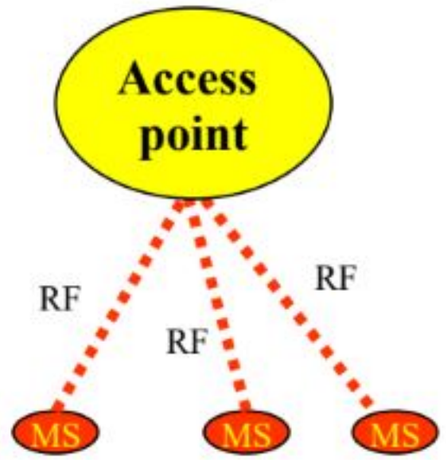
❖ Sensor Networks:

They report their surrounding environments physical conditions such as temperature, vibrations, etc.

Introduction to Networks

➢ Networks:

❖ **Wireless LAN (Local Area Networks), WiFi (Wireless Fidelity), IEEE 802.11**



Two Types:

1) **Infrastructure Networks:** Client talks to access point then access point talks to destination client, this type has access point.

2) **Ad Hoc Networks:** Clients talk to each other without access points. This type does not have access point

❑ **Multipath Fading:** Reflection of transmitted signal will have multiple copies of the same signal.

Solutions:

1) **Provide multiple independent paths to destination**

2) **Repeating the transmitted bits at different timeline**

Introduction to Networks

Networks:

Wireless LAN (Local Area Networks), WiFi (Wireless Fidelity), IEEE 802.11

- IEEE 802.11a/g rate 54 Mbps is using OFDM (Orthogonal Frequency Division Multiplexing) to transmit into sub-frequencies for parallel transmission of bits.
- IEEE 802.11n provides 450 Mbps, uses for antennas for each client.
- CSMA (Carrier Sense Media Access) is used

Security:

- WEP (Wired Equivalent Privacy) was used but it was not secure enough, the IEEE 802.11i (WiFi Protected access) was developed, WPA2 is the improved version.

Introduction to Networks

- **Networks:**
  - **Wireless Cellular Networks**

Cellular Technologies Generations:

- **First Generation Analog**
- **Second Generation Digital**

  GSM

  CDMA One(IS-95)

  US-TDMA

- **Third Generation Multimedia Packet Network Access**

  UMTS (Universal Mobile Telecommunications System) or

  WCDMA (Wideband Code Division Multiple Access)

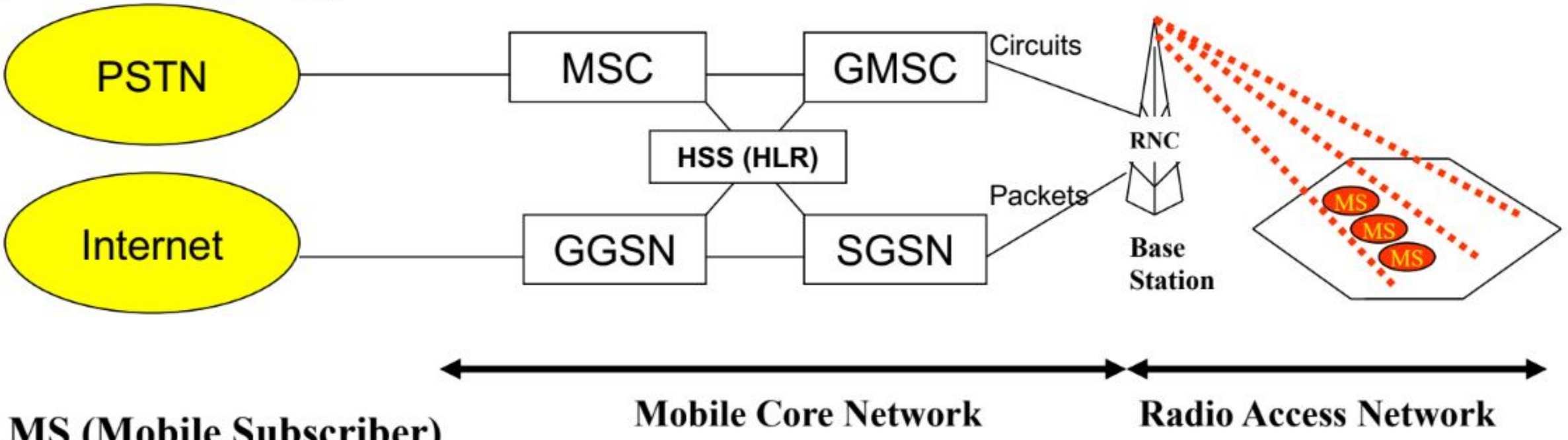
  covers TDD (Time Division Duplex), FDD (Frequency Division Duplex)

Introduction to Networks

- **Networks:**

❖ Wireless Cellular Networks

Network Topology



MS (Mobile Subscriber)

RNC (Radio Network Controller: Manages frequency spectrum.

Base Station (Node B): Contains the air interface

MSC (Mobile Switching Center): connecting user to destination

GMSC (Gateway Mobile Switching Center): Connects user to other cell ISPs

GGSN (Gateway GPRS Support Node): Packet transport to and from packet network.

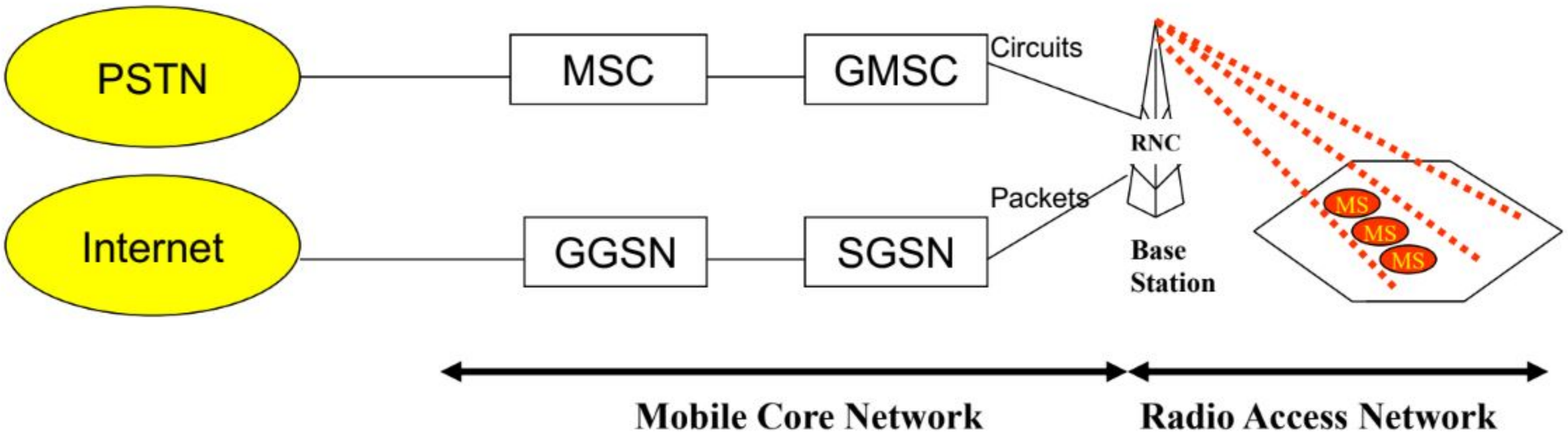
SGSN (Serving GRPS Support Node): Provides addressing to packet switching network

HSS (Home Subscriber Server) or (Home Location Resources): Tracking user's mobility

Introduction to Networks

Networks:

Wireless Cellular Networks



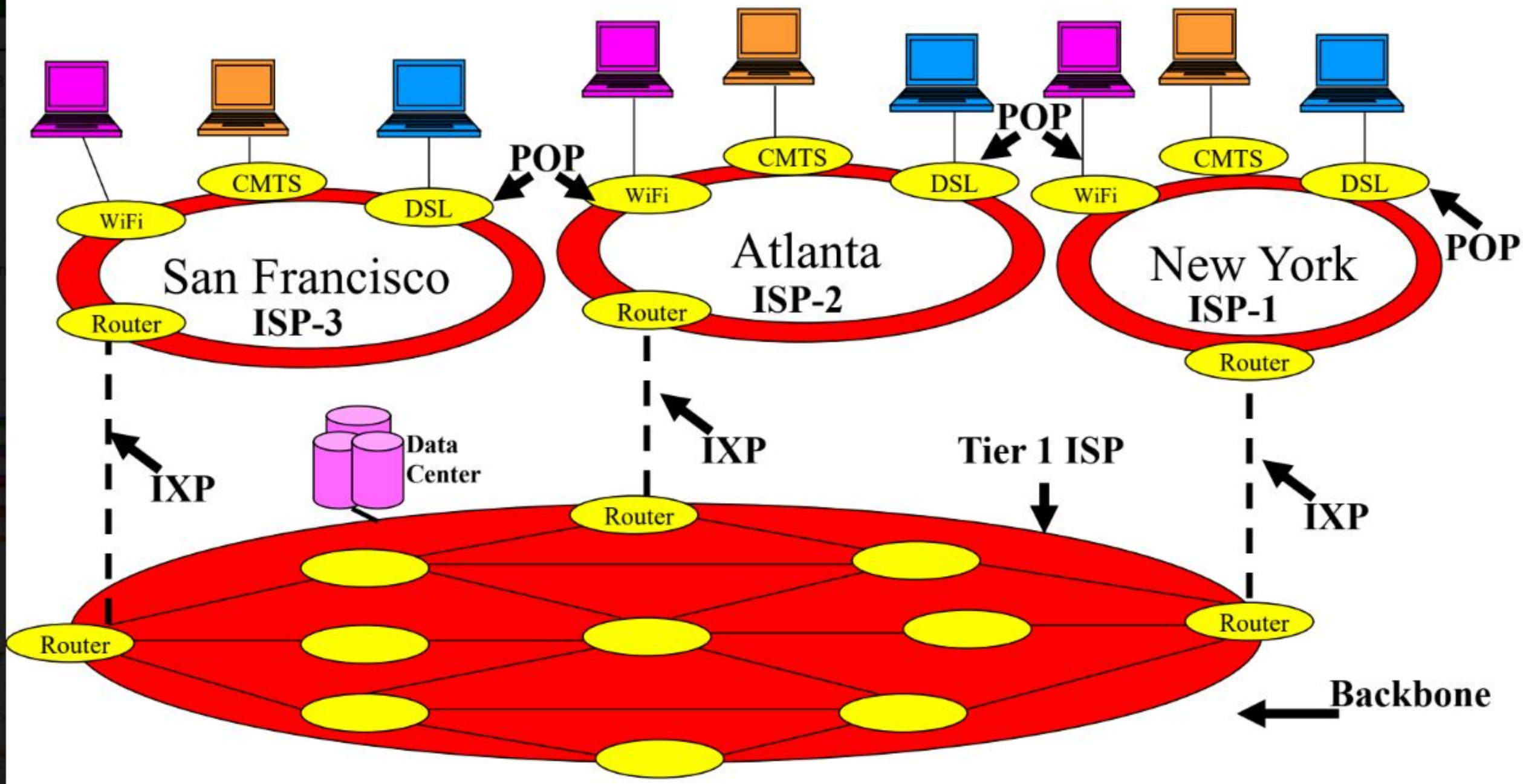
Hand off (Hand over):

- To provide QoS (Quality of Service) user will be connected from one base station to another.
- SIM (Subscriber Identity module): Provides portability of user information with different mobile device. Encrypts/Decrypts the user information with the key defined in SIM.
- 4G LTE (Long Term Evolution) provides 75-100 Mbps bandwidth

Introduction to Networks

- **Networks:**

- **Internet Architecture:**



Introduction to Networks

➢ Networks:

❖ Internet Architecture:

- **Backbone:** Provides connectivity between different segments of Internet

  The packets destined for a destination on the same ISP will be forwarded over the backbone.

- **Tier 1 ISPs:** They are building the backbone of network, all users need to connect to them. The tier 1 do not charge for transit traffic.

- **IXP (Internet eXchange Point):** connects ISP to backbone.

- **POP (Point of Presence):** The service is provided at this point to subscribers (DSL, CMTS, WiFi, or Cell phone)

- **Data Center:** Contains single servers and server farms.

- **Virtualization:** Provides a concept to access the server farm with out being physically present in data center.

Introduction to Networks

➢ Reference Models

2. The TCP/IP (Transmission Control Protocol)/(Internet Protocol)

❖ **Link Layer :**

Is a layer between the user ‘s end device and transmission link.

❖ **Internet Layer:**

This layer delivers the packet to
destination address defined in the packet header.

It uses IP (Internet Protocol) and ICMP (Internet Control Message Protocol).

❖ **Transport Layer:**

The transport layer peers at end devices communicate with each other.
There are two transport protocols:

1) TCP (Transmission Control Protocol):

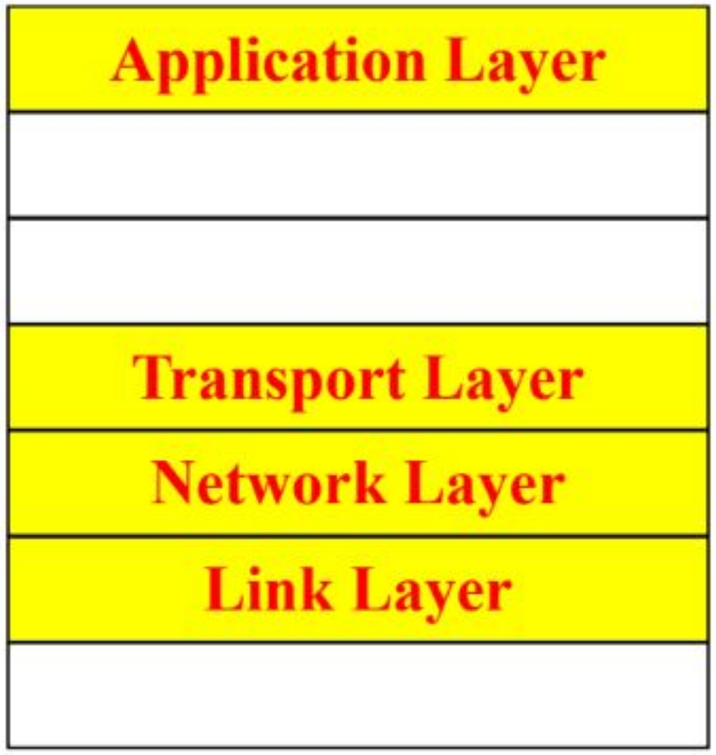
Connection oriented protocol, provides error free transport,
it segments the packets at source and reassembles at destination device.
TCP provides flow control.

2) UDP (User Datagram Protocol):

Is connectionless protocol, the application layer will provide
bandwidth control and segmentation/reassembly.

❖ **Application Layer:**

The application layer provides layer 5 and layer 6 functions.



Introduction to Networks

➢ Reference Models

2. The TCP/IP (Transmission Control Protocol)/(Internet Protocol)

For better visibility we use the five layers:

1. Layer 1- Physical Layer

Uses different Media, fiber glass, metal, or radio frequency.

2. Layer 2- Link Layer

Used for reliable transmission between end devices and access nodes

3. Layer 3- Network Layer

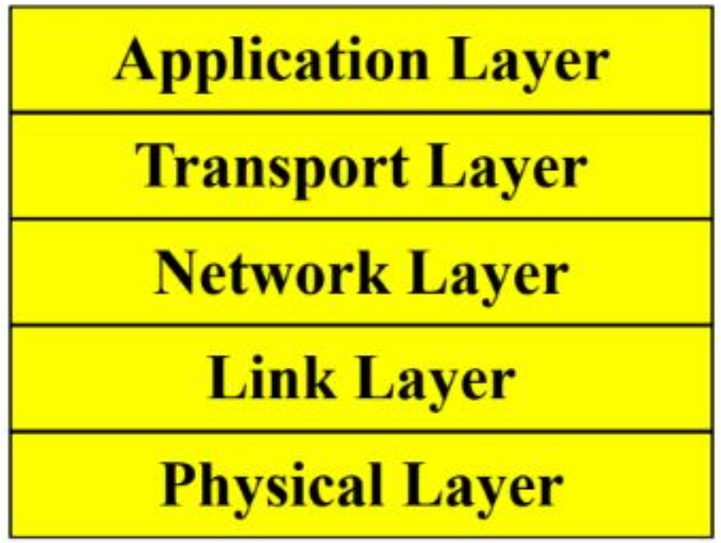
Will forward packets to destination devices.

4. Layer 4- Transport Layer

TCP or UDP is used

5. Layer 5- Application Layer

This layer uses the layers below to connect to Internet or other networks over Internet.



Introduction to Networks

- **Short coming of Modes:**

Both standards have deficiencies.

- **ISO (International Standard Organization) OSI (Open System Interconnection):**

OSI was difficult to implement, implementations had poor performance.

Some features were not addressed properly (flow control was used in many layers, and error handling).

- **TCP/IP (Transport Control Protocol/ Internet Protocol)**

This model is not generalized to describe other protocol stacks.

Introduction to Networks

➢ Reference Model

1. ISO (International Standard Organization) OSI (Open System Interconnection) Reference Model

Layer 2, Data Link Layer:

- Encapsulates the bits into Frames.
- Transports bits to the network in frames, the errors in frames are not visible to the network layer.
- It can provide backpressure control that slow processing devices are not flooded with too many frames.

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Layer 3, Network Layer:

- Routes the packets from source to destination, provides paths using static or dynamic tables.
- Will isolate the failed nodes by dynamically updating the routing paths.
- Controls congestions and load adaptation to meet QoS (Quality of Service).
- May provide packet fragmentation for large packets and address translations if the packet travels to other networks.

Data Link Layer

- **Provides flow control communications between user and network, as well errors are detected.**
- **<u>Services Offered:</u>**
  - **Acknowledged connectionless Service**
  - **Unacknowledged connectionless service**
  - **Acknowledged connection oriented service**

Application Layer	Application Layer
Presentation Layer	Presentation Layer
Session Layer	Session Layer
Transport Layer	Transport Layer
Network Layer	Network Layer
Data Link Layer	**Data Link Layer**
Physical Layer	Physical Layer

Data Link Layer

- **Data Link Layer provides flow control communications between user and network, as well errors are detected.**

- **Services Offered:**
  - Acknowledged connectionless Service, no prior logical connection. Retransmit if Ack not received.
  - Unacknowledged connectionless service, no prior logical connection (Ethernet) if any error occurs higher layer protocol will detect the errors.
  - Acknowledged connection oriented service, establishes a logical channel with network. Using timers and counters to guarantee frame transmission.

- **Frame Formats:**

Each frame has a starting and an ending flag.

- **Byte Stuffing:** To transmit the same Bytes as the start or ending flag the Escape character is used, prior to putting the Byte which is the same as start or ending flag the escape Byte is inserted, at receiver Escape characters are removed.
- **Bit Stuffing:** Transmitter includes after Escape character Escape character, the receiver removes the Escape character and passes the stuffed bit to application, after 5 bits the stuff bit added

Examples:USB (Universal Serial Buss),CAN (Control Area Network), Eth preamble 72 bits.

Introduction To Computer Networks and Internet

Computer Networks:

Network protocols:

- Request-reply: The reply request is embedded in the request message, the sender is waiting for response from destination (client, server).

Service Primitives:

- Set of operations (primitives) provided by a layer to another layer in the protocol stack.

Client-Server operations (primitives):

LISTEN : Server executes this operation, meaning accepts incoming requests, blocks server until receives CONNECT

CONNECT: Client sends to address who wants to be connected to, client will suspend process until receives response

ACCEPT: Server sends to client to acknowledge that received the CONNECT primitive and agrees to connect to client.

RECEIVE: Server is ready to receive data from this client, unblocks server for processing receiving information.

SEND: Client sends its request to server, server unblocks by arrival of this message

SEND: Server sends requested information

Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**

  Analog voice, Digital voice, Digital voice and data

- Mobile Telephone Networks:

  - **1 G (First Generation) Analog voice:**

    Used half duplex system, mobile device was installed in vehicles.

    The next version used full duplex (two frequencies, TX, RX) 23 channels.

    AMPS (Advanced Mobile Phone System):

    Used cells with lower antenna power. Reconfigurable and Ad Hoc cell setup.

    Frequency reuse, using MSC (Mobile Switching Center). Hand off 300 msec.

    FDD (Frequency Division Duplex) 832 channels uplink, 832 channels downlink.

    The channels are used are:

    - Control channel: system management
    - Paging channel: handles incoming calls to user, always user listen to this channel
    - Access channel: call setup signaling
    - Data channel: transports user information (Voice, Data).

Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Provides more security.

Standards:

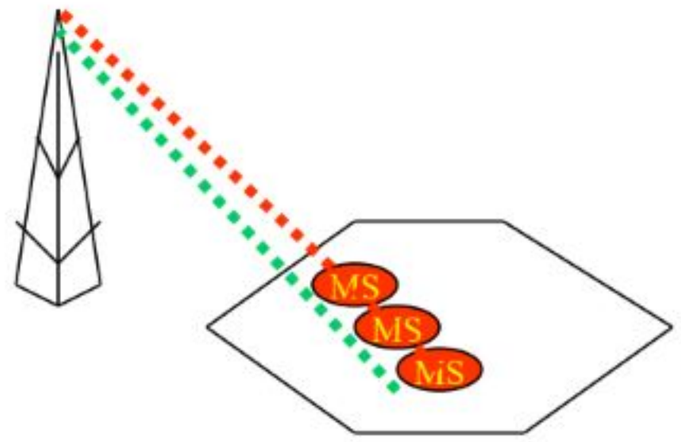
1. **DAMPS (Digital Advanced Mobile Phone System)** is digital standard using TDM.
2. **GSM (Global System for Mobile communications)** uses TDD(Time Division Duplex) and FDD(Frequency Division Duplex). Used first in Europe then US, now world wide. Uses FDD and TDD.

Is full duplex uses one of the time slots for

transmit and one for receive on the up and frequency downlink.

Eight time slots for uplink and eight time slots for downlink

Frequency range 900, 1800, and 1900 MHz, 200 KHz frequency spacing.

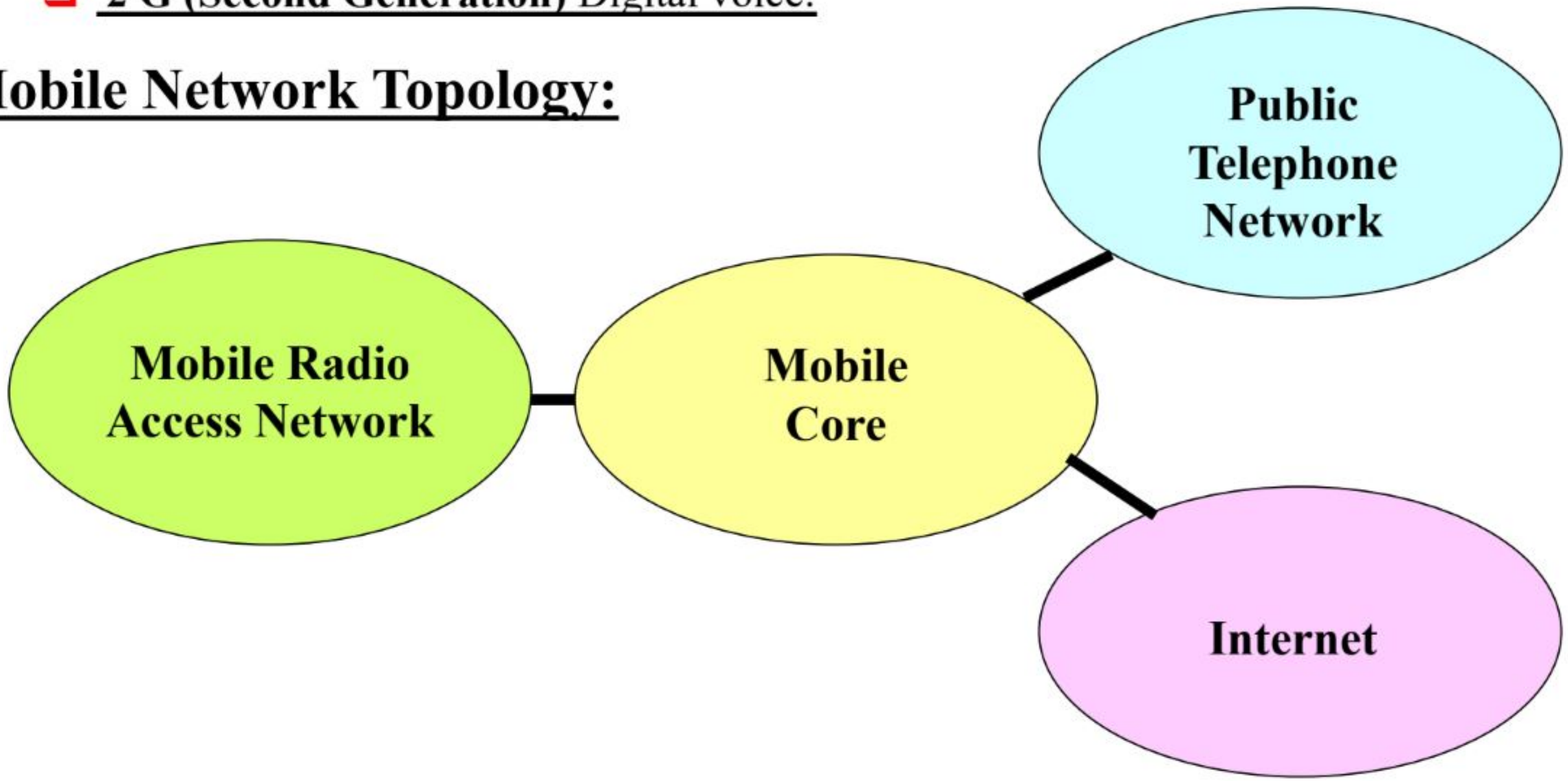


Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**

- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

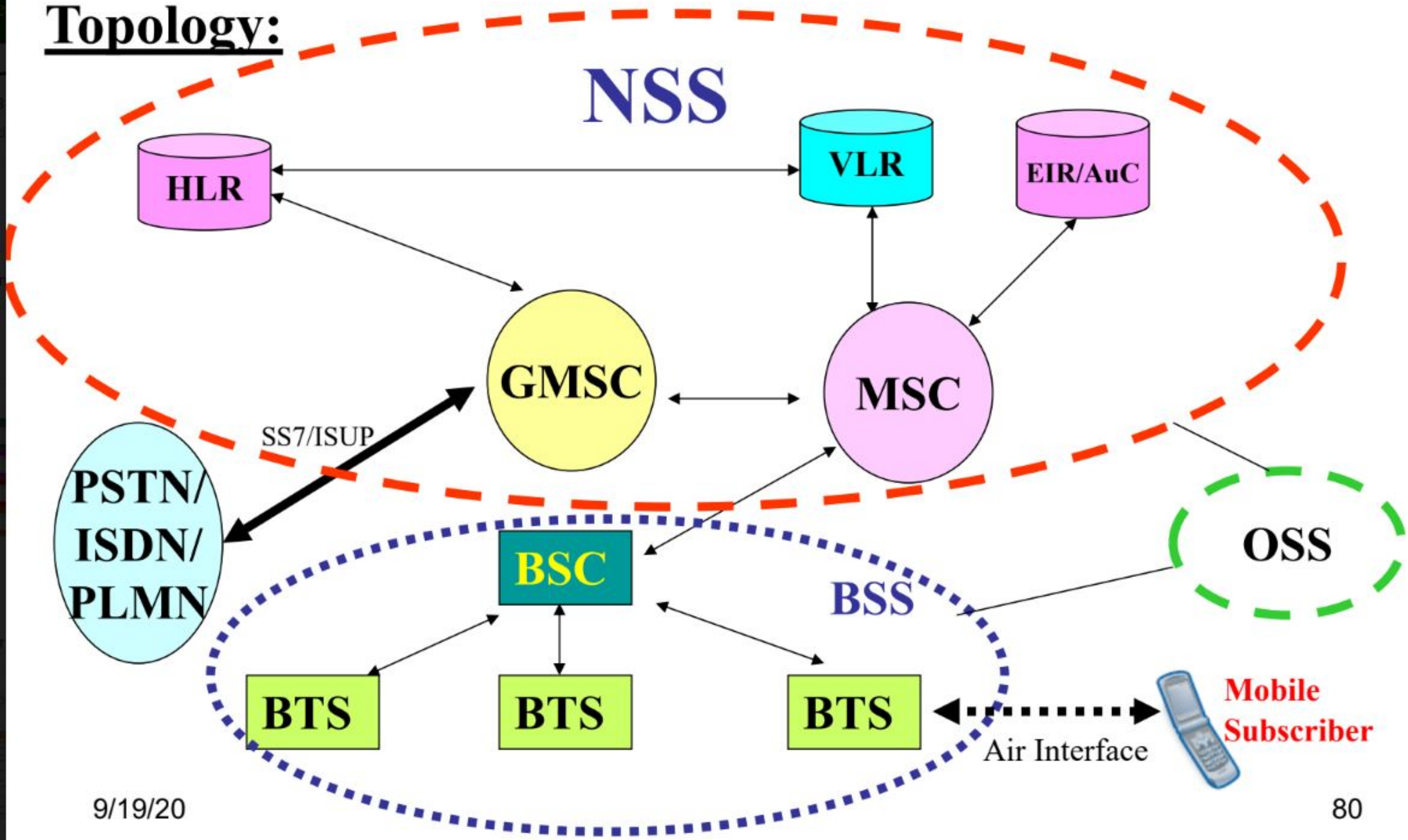
Mobile Network Topology:



Physical Layers of Networks

- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Topology:



❖Mobile Telephone Networks:

❑ 2 G (Second Generation) Digital voice

Introduction and overview

GSM Subsystems:

- **MS(Mobile Station):** User access device(Handheld or portable station)
- **SIM(Subscriber Identity Module):**Defines identity of user and MS. Determines directory number and the subscriber billing.
- **BTS(Base Transceiver Station):** Radio link between MS and network.
- **BSC(Base Station Controler):**BTSs in one area are connected to BSC by Abis-interface.
- **MSC(Mobile Switching Center):**Many BSCs are connected to MSC through A-interface. Routes incoming and outgoing calls and assigns user channels on the A-interface.
- **HLR(Home Location Register):** A database which contains user's last location information.
- **VLR(Visitor Location Register):**Contains moving part of user database, reliefes HLR.
- **EIR(Equipment Identity Register):** To bar Stolen equipment to access mobile network.
- **GMSC(Gateway Mobile Switching Center):**Interface to other networks(PSTN)and HLR communication capability.
- **OSS(Operation Subsystem Operation and Maintenance).**

Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Frame Structure:

Each time slot contains the information in this format,

Head	Data	Flag	Training	Flag	Data	Tailing	Guard
3 bits	57 bits	1 bit	26 bits	1 bit	57 bits	3 bits	8.25 bits

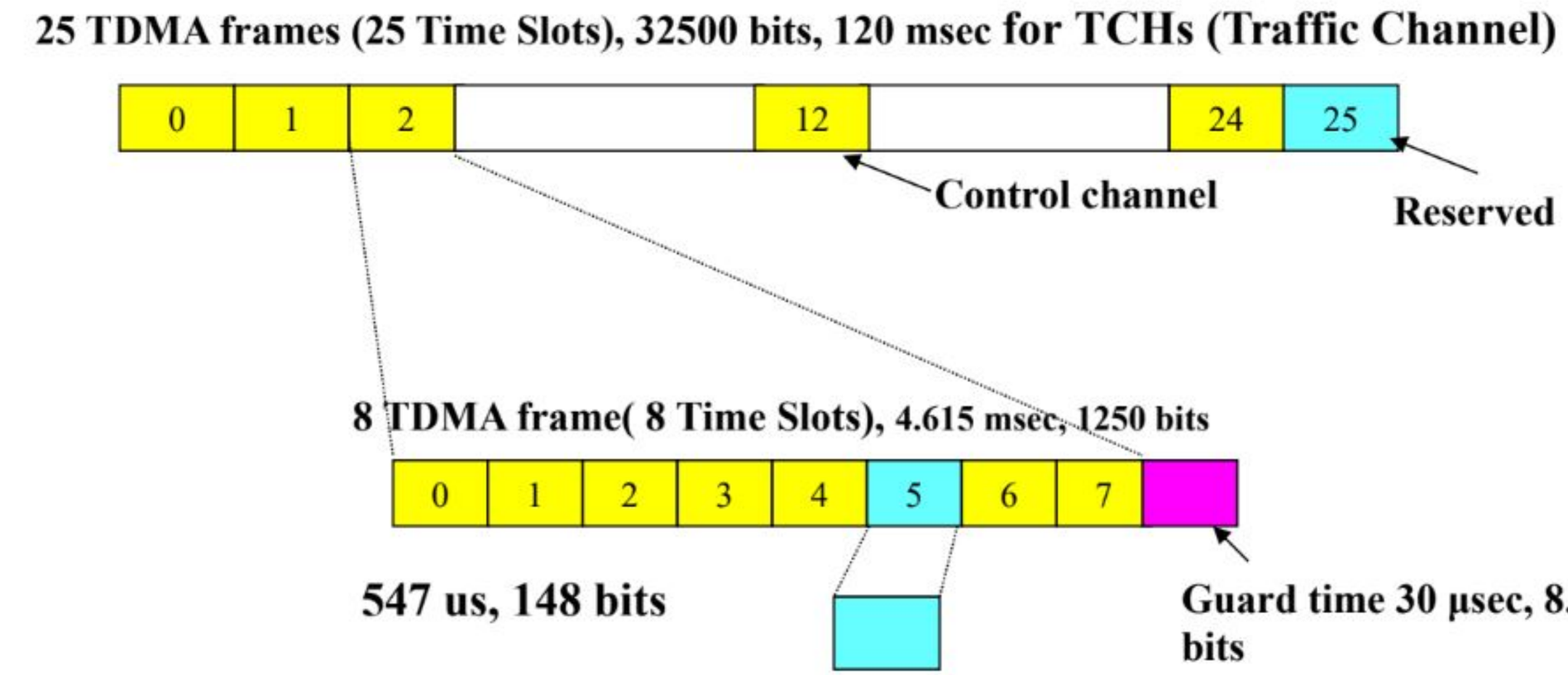
The frame will be sent in each eight time slots.

Total of 24.7 Kbps per user, for voice 13 Kbps is used.

Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Frame Structure



Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Frame Structure

- **Dedicated Control channel:** Call setup (announcing time slot available), registration location update (VLR)
- **Common Control channel:** request dedicated time slot, access grant channel announces the allocated channel
- **Paging channel:** Announcing incoming call.

Handoff (Handover):

MS measures the signal and reports to BSC, the handoff can be performed (Assisted Handoff)

Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **3 G (Third Generation)** Digital voice, Digital Data:

Providing more services, SMS, surfing Internet sites contain multimedia, TV, streaming video, chat, and mobile e-commerce.

Standards:

UMTS (Universal Mobile Telecommunication System) WCDMA (Wideband CDMA) 5 MHz.

CDMA (Code Division Multiple Access):

Long pseudo random numbers provide low probability of cross correlation with each other.

The chips can carry different rates between MSs (Mobile Subscribers) and BTS (Base Transceiver Station)

Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **3 G (Third Generation)** Digital voice, Digital Data:

CDMA (Code Division Multiple Access):

One frequency is used for all users, the users are separated with chips from other users.

Sectorized antenna can be used with one frequency.

When other users in cell coverage area are silent the bandwidth can be used by other users.

Soft hand off is supported, hand off is without complication to other BTS, because the same frequency is used.

4G LTE (Long Term Evolution):

Full IP based connectivity, available every where at any time, and service portability.

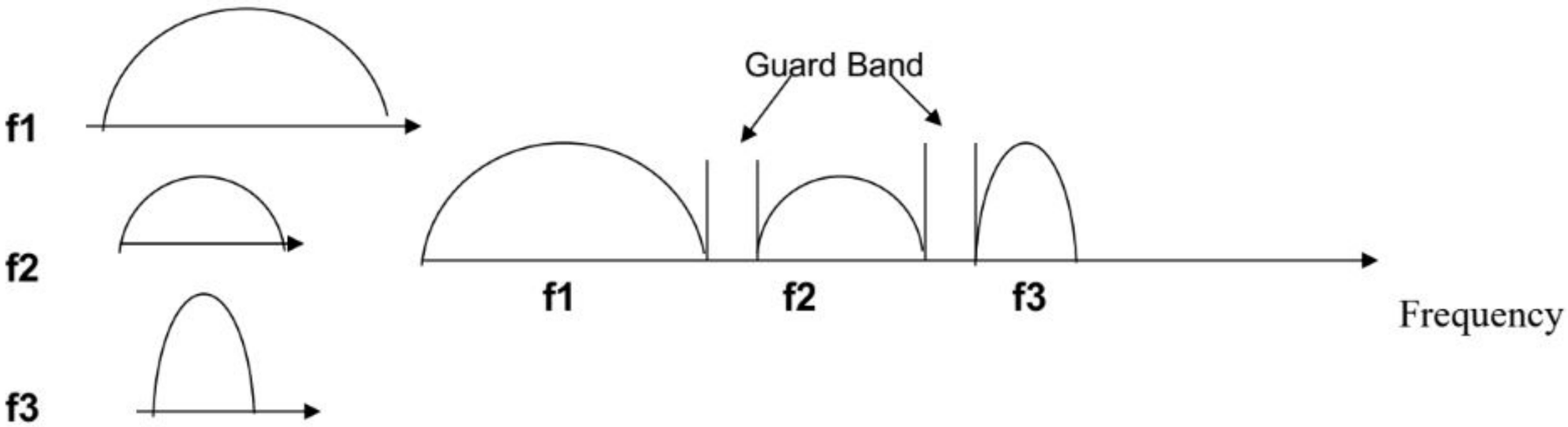
Physical Layers of Networks

Modulation

FDM (Frequency Division Multiplexing):

Individual users use different frequency to transmit.

All frequency channels are **multiplexed** together and transmitted.



OFDM (Orthogonal Frequency Multiplexing):

Provides solution with out guard band, the spectrum is subdivided in sub-channels.

Using QAM (Quadrature Amplitude Modulation)

Introduction to Networks

➢ Network Standards:

❖ International Organizations

❑ **NIST (National Institute of Standards and Technology)**

Produces standards in U.S.

❑ **IEEE (Institute of Electrical and Electronics Engineering)**

Very active, many publications, standards, the largest in the world.

Works on standards for electrical and computing.

❑ **Internet Standard Organization**

- **IAB (Internet Architecture Board) was overseeing and guiding ARPANET.**
- **IAB researchers moved to IRTF (Internet Research Task Force) and expanded, IRTF focuses on future.**
- **IETF (Internet Engineering Task Force) is under IAB, the IETF owns all RFCs (Request for Comments), IETF has routing, security, etc. groups.**
- **RFC should explain the idea that had been tested on two independent sites for four months, after approval IAB will become Internet Standard.**
- **Internet Society consists of members interested in Internet development and is under IAB.**

❑ **W3C (World Wide Web Consortium)**

Develops standards for www.

Introduction to Networks

➢ **Network Standards:**

They define requirements for interoperability of products.

❖ International Organizations

❑ ISO (International Standard Organization):

Members are National committees:

- **DIN (Germany)**
- **ANSI (U.S.)**
- **BSI (England)**
- **AFNOR (France)**

✓ **ISO Covers all standards on different subjects.**

✓ **ITU-T (International Telecommunication Union-Telephony) and ISO work close to prevent overlaps.**

✓ **ISO has 200 TCs (technical committees), they have WGs (Working groups)**

✓ **The Working group JTC1 handles information technology (computer, networks)**

✓ **National standard committee provides proposal to working group, a committee will work on draft that will be available for review for 6 months, if committee approves then will be voted. If accepted will become ISO standard. May take years until approved, because of many revisions.**

Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**

- Switching types:

1. **Packet Switching**

Information is transmitted in packets, stores and forwards packets, sensitive to congestion, is not wasting bandwidth.

2. **Circuit Switching**

Dedicates resources, using time slots, waste of bandwidth when user does not use the Bandwidth.

Physical Layers of Networks

PSTN (Public Switched Telephone Network)

Data Transmission in PSTN:

Using DSL (Digital Subscriber Line):

Transmits bits over the same telephony structure with higher speed than modems V.90 and V.92.

Maximum transmission rate is 56000 bps, modem standards used were V.90 and V.92.

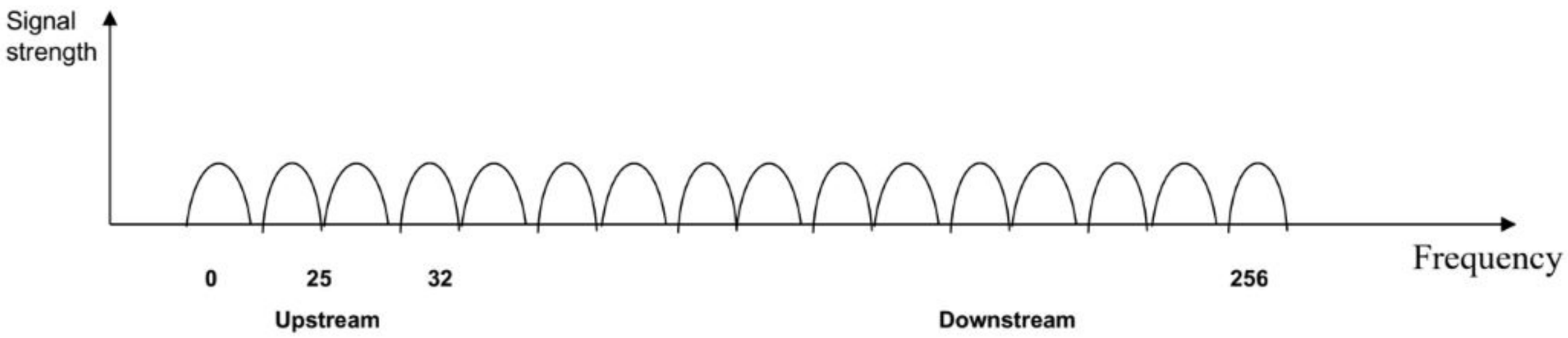
The OFDM technology is used with 256 sub-channels.

Channel 0 is used for speech telephony, channels 1-5 are not used.

Using 1.1 MHz spectrum.

The 250 channels are used for user's information transmission (voice, video, or data).

Using QAM (Quadrature Amplitude Modulation).



Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
- **Data Transmission in PSTN:**
- **Using DSL (Digital Subscriber Line):**

Two paths: Voice traffic uses 0-4000 Hz, Data traffic uses the rest of spectrum.

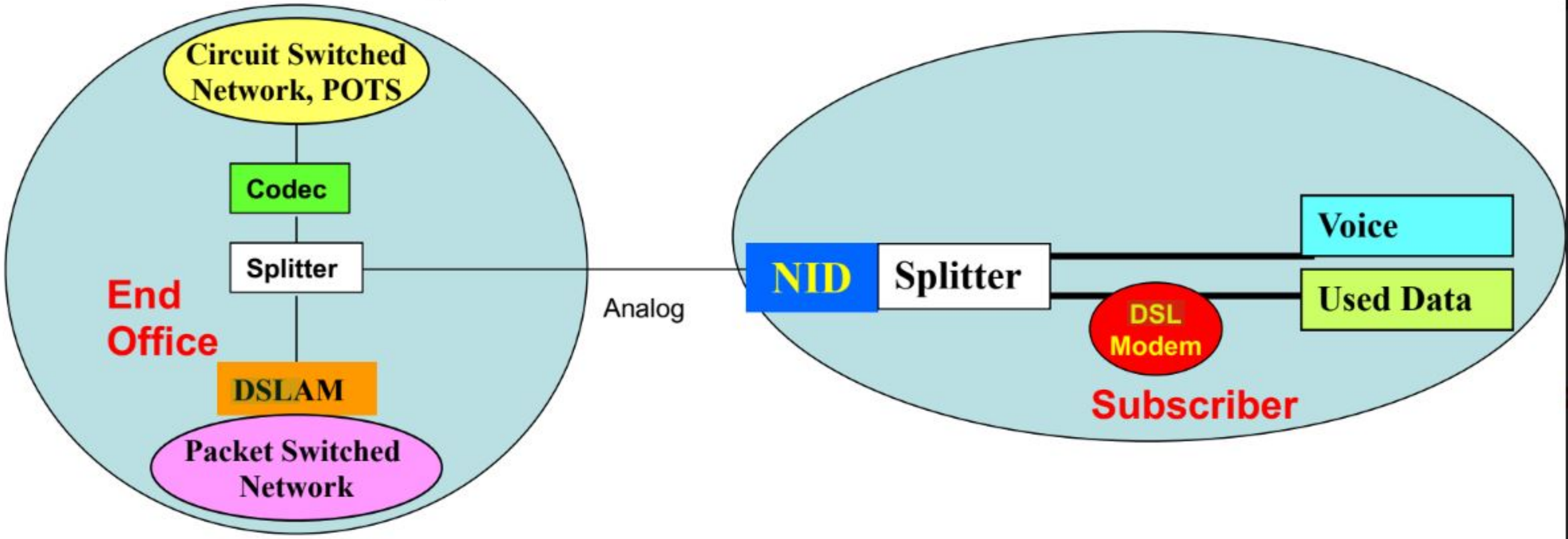
NID (Network Interface Device) is used for demarcation of subscriber and End Office.

Splitter, is a filter to separate the voice and data traffic.

DSLAM (Digital Subscriber Multiplexer) connects many users to the packet switched network

Codec converts analog to digital.

G.Lite will eliminate the splitter on subscriber side.

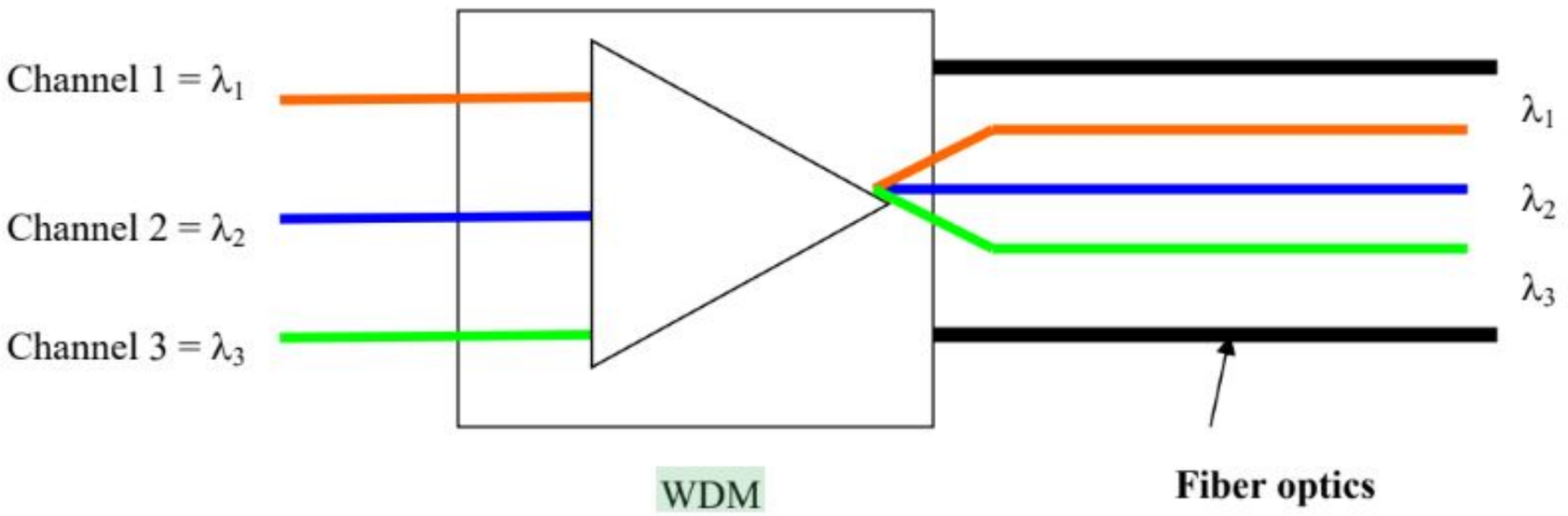


Physical Layers of Networks

➢ **PSTN (Public Switched Telephone Network)**

❖ WDM (Wave Division Multiplexing)

- From a specific frequency range incoming optical signals are maps to a specific wavelength (Lambda λ).
- WDM is a method to aggregate input signals in one transport medium (fiber glass).
- WDM carries each signal independently of other signals.
- At the end of fiber the signals are de-multiplexed and sent to the proper destination device.
- Every 1000 Km optical signals are amplified.
- Technical University of Denmark (DTU), has managed to transmit 43 terabits per second over a single optical fiber with just one laser transmitter



Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
- **TDM (Time Division Multiplexing)**

SONET (Synchronous Optical Network)/SDH (Synchronous Digital Hierarchy):

SONET/SDH is a high-speed TDM physical layer transport technology.

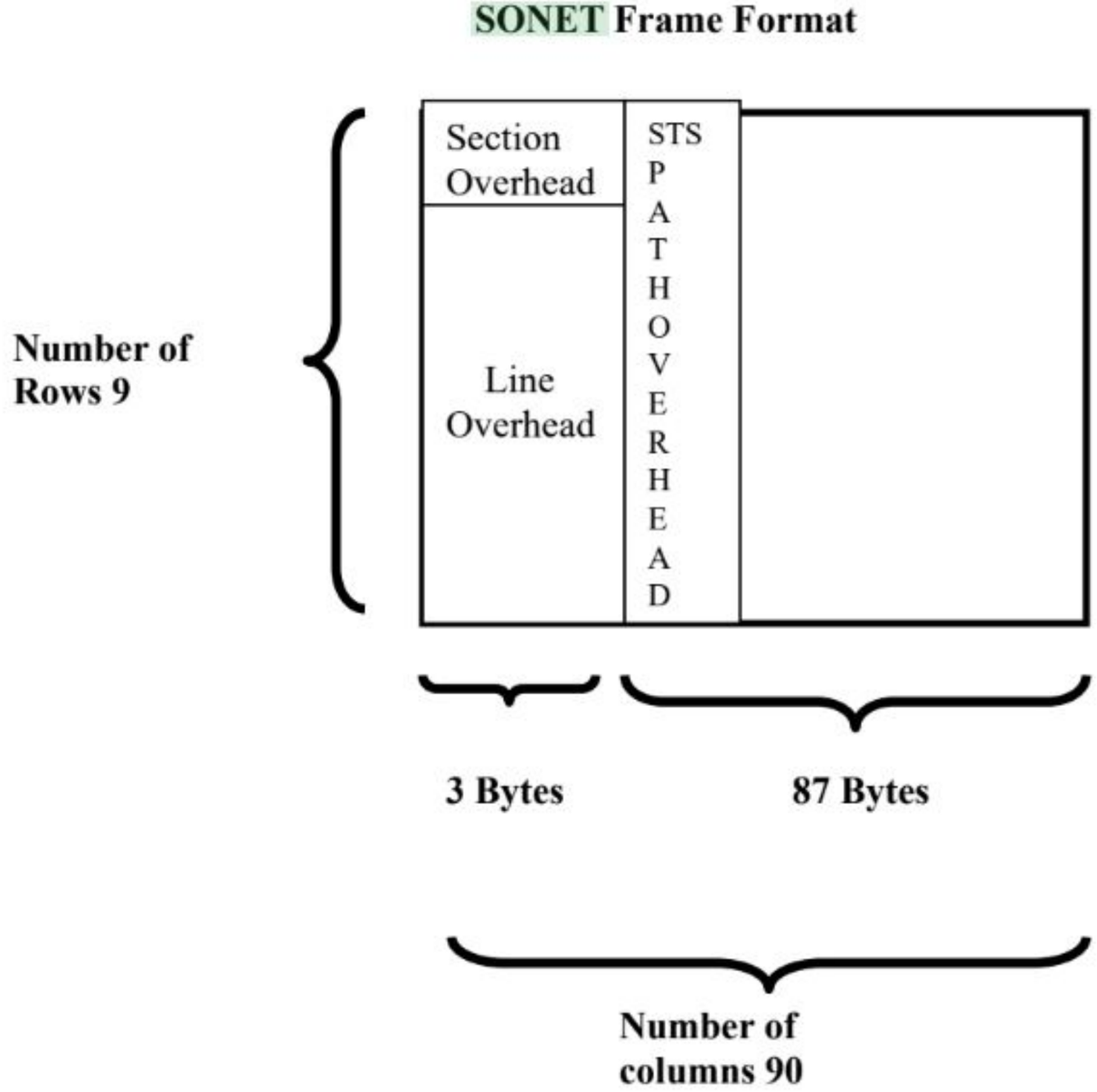
- Every second 8000 frames are transmitted.
- SONET/SDH frame is 810 Bytes = 9 Rows X 90 columns.
- 8000 times per second 8X810 = 6480 bits are transmitted.
- The SONET/SDH frame is divided into transport and payload Bytes
- Transport overhead consist of section and line overhead Bytes
- The basic transmission rate of SONET is 51.840 Mbps, referred to as ***STS (Synchronous Transport Signal Level 1)***
- Transmission rates of Multiples of 51.840 Mbps
- SONET uses containers.
- SPE (Synchronous Payload envelop) contains user information for data transmission
- SPE will float insides SONET container a pointer will provide its position in the container.

Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
- **TDM (Time Division Multiplexing)**

SONET (Synchronous Optical Network)/SDH (Synchronous Digital Hierarchy):

SONET Frame Format:



Physical Layers of Networks

- **PSTN (Public Switched Telephone Network)**
- **TDM (Time Division Multiplexing)**

SONET (Synchronous Optical Network)/SDH (Synchronous Digital Hierarchy):

- **SONET Hierarchy**

SONET	Line Rate (Mbps)	Optical	SDH (ITU)	Number of 64 Kbit Channels
STS-1	51.840	OC-1	---	672
STS-2	103.680	OC-2	---	1344
STS-3	155.520	OC-3	STM-1	2016
STS-12	622.08	OC-12	STM-4	8064
STS-24	1244.16	OC-24	STM-8	16128
STS-48	2488.32	OC-48	STM-16	32256
STS-n	nX51.840	OC-n	(n / 3)	((nX51.840X1000) / 64) **-138n**

Data Link Layer

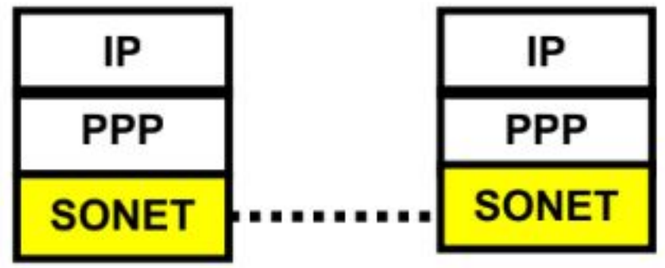
- **Data Link Layer Protocols**

Examples:

All the following technologies use PPP (Point to Point Protocol)

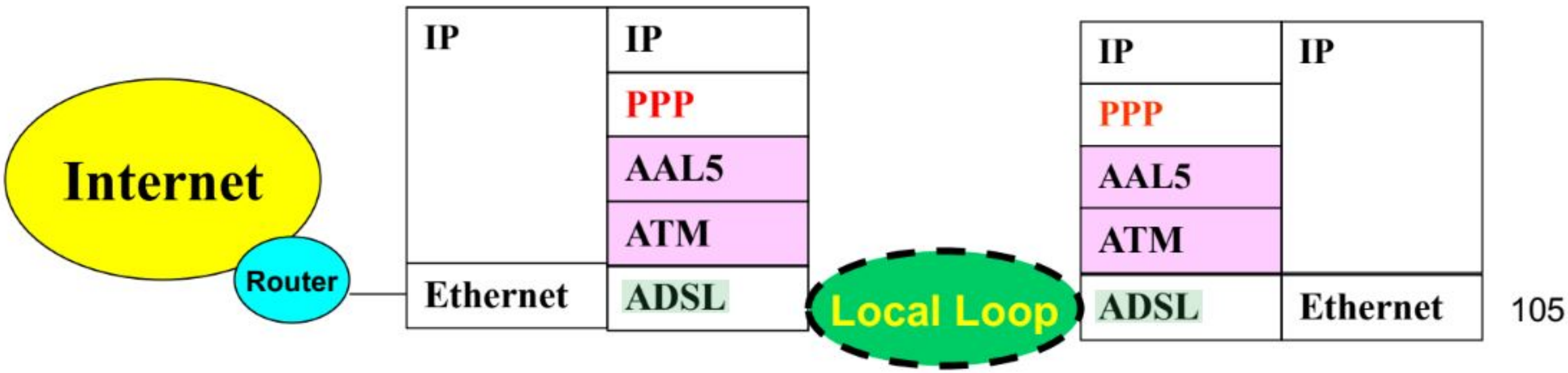
1. SONET (Synchronous Optical Network)/SDH (Synchronous Digital Hierarchy):

Used for Point-to-Point connections of router to different part of ISP network.



2. ADSL (Asynchronous Digital Subscriber Line)

- Connects users from access to local loop of POT network Point-to-Point will carry traffic to Internet.
- ADSL is a data link layer protocol which uses existing telephone infrastructures.
- On the same POT infrastructure the data packets are transmitted over local loop to central office and then IP packets are filtered (DSLAM Digital Subscriber Line Multiplexer) and will be sent to IP network, the voice traffic is diverted to the circuit switched network (telephony network).



Physical Layers of Networks

- PSTN (Public Switched Telephone Network)
- Mobile Telephone Networks:
  - **2 G (Second Generation)** Digital voice:

Frame Structure

- **Dedicated Control channel:** Call setup (announcing time slot available), registration location update (VLR)
- **Common Control channel:** request dedicated time slot, access grant channel announces the allocated channel
- **Paging channel:** Announcing incoming call.

Handoff (Handover):

MS measures the signal and reports to BSC, the handoff can be performed (Assisted Handoff)

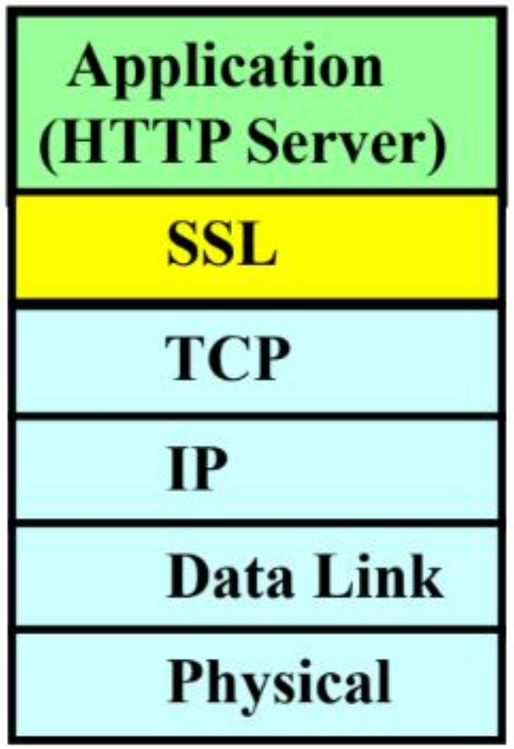
Security

- **SSL (Secure Socket Layer)**

It is protocol independent implementation (RFC 2246)

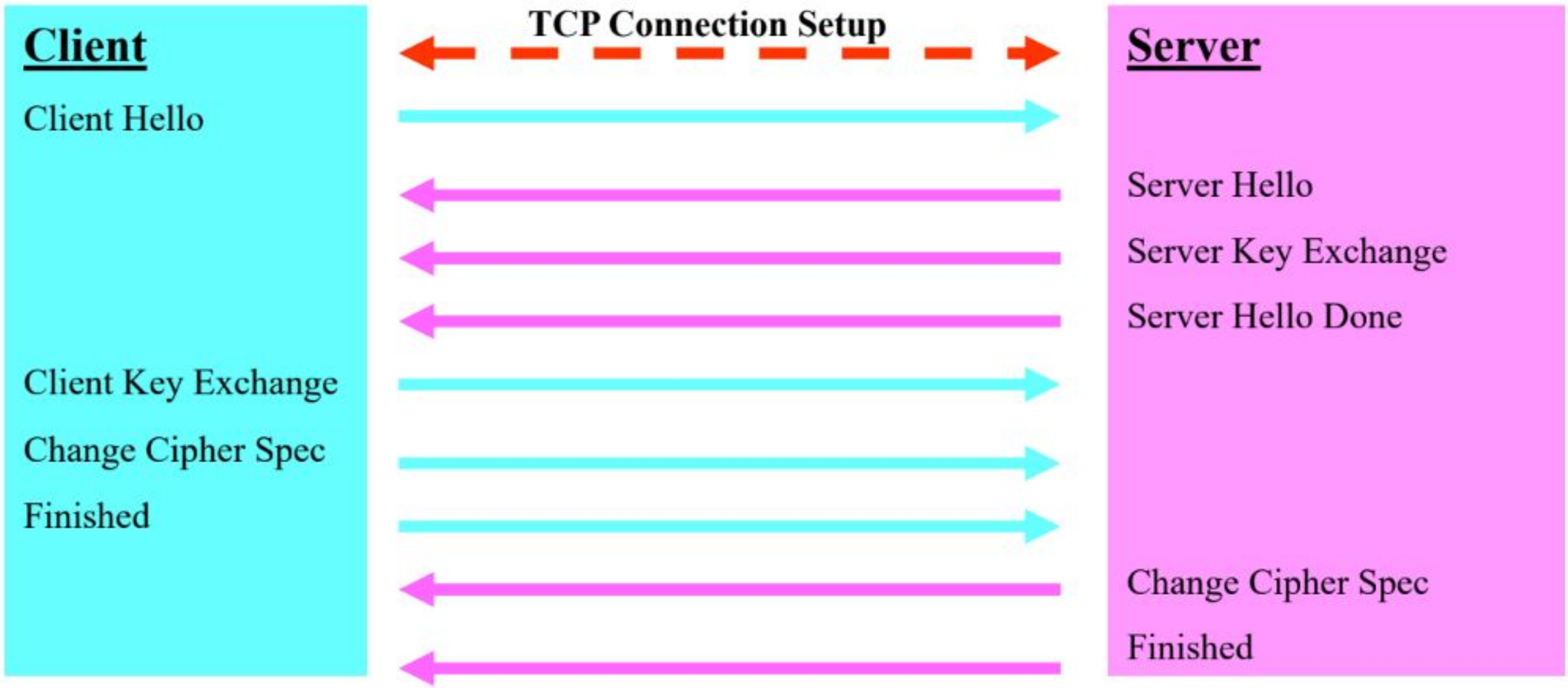
SSL is by itself a layer.

Any Public key/private key, and symmetric key can work with SSL



SSL Protocol stack

SSL Protocol Messages:



- **SSL Protocol Messages:**

- **Client Hello:** First message after TCP connection is established is sent to server to begin the negotiation.

Message contains:

- Supported SSL version,
- 256 bit Random Number for server to feed Random-number generator,
- session-ID,
- list of supported ciphers,
- supported compression

- **SSL Protocol Messages (continue):**

- **Server Hello:** Response to Client's Hello

Message contains:

- SSL version server agrees,
- 256 bit Random Number for client to feed Random-number generator,
- session-ID,
- Cipher's type,
- supported compression (if zero, no compression is supported)

Security

- **SSL Protocol Messages (continue):**
- **Server Key Exchange:** Server sends its public key to client, format is based on cipher type.
- **Server Hello Done:** Server says the client he is done sending certificate.
- **Client Key Exchange:** Contains client's public key.
- **Change Cipher Spec:** Indicates that all messages after this are encrypted.
- **Finished:** After "Change Cipher Spec" is sent by server or client this message follows. Both need to send this message for completion.
- **Certificate:** Server sends this message to ask client to verify server's identity

Security

- **SSL Protocol Messages (continue):**
  - **Hello Request:** After server and client have negotiated, server may send this message to renegotiate, if client refuse will return **alert** message. This message is issued, when server realizes duration of session was too long for the same key or key is compromised.
  - **Certificate Request:** Server will verify the client certification.
  - **Certificate Verify:** Response to the certified request.
  - **Alert:** Server or client issue this message to indicate warning or error.
  - **Application Data:** Indicates the message payload is destined for application and should not be interpreted from SSL.

Bridges:

- To connect LANs together, using algorithms to prevent loops and forward the frames to the correct destination.
- Each port of switch can be connected to one Ethernet LAN, the CSMA/CD is used because of collision in that domain, each bridge port has its own collision domain.

Flooding:

- The bridge uses hash table for forwarding.
- The bridge in initial stage does not have any information where to forward the frames.
- When bridge receives a frame will forward to all ports (flooding) except to the port the frame was received from.
- The bridge will learn the destination and will build its hash table.
- Flooding is used if there is no entry in their hash table for that frame's destination address.

Learning:

- The bridge will see from which port the frames arrive and will know which user is connected to which port on the bridge, this information will be added to hash table.
- Each entry in the hash table will have a time stamp.
- Hash tables will be cleaned up every few minutes (configurable) if a frame was not seen with the address for that entry.

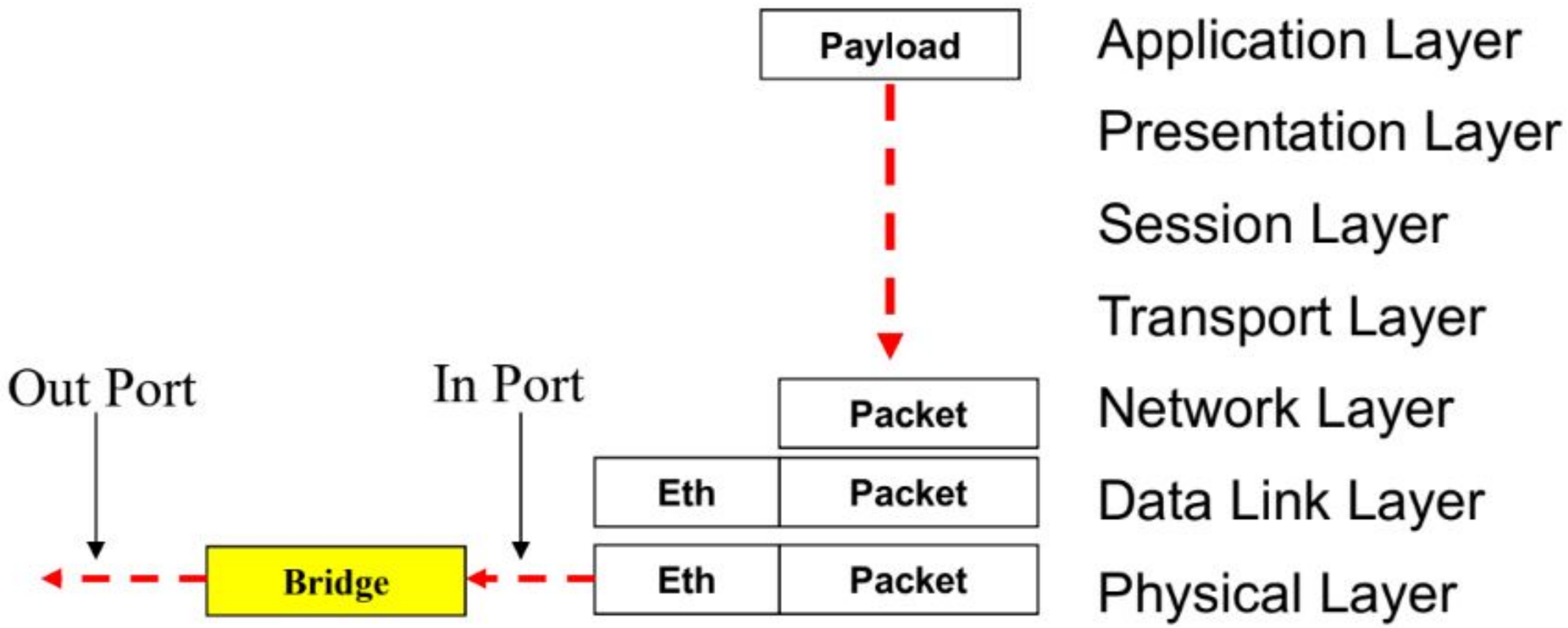
➢ Bridges:

❑ Learning rules:

Routing algorithm concept:

1. Discard the frame if the port for destination address is the same as the source port.
2. Forward the frame if the port for destination address is not the same as the source port
3. Flood, if the destination number is not known

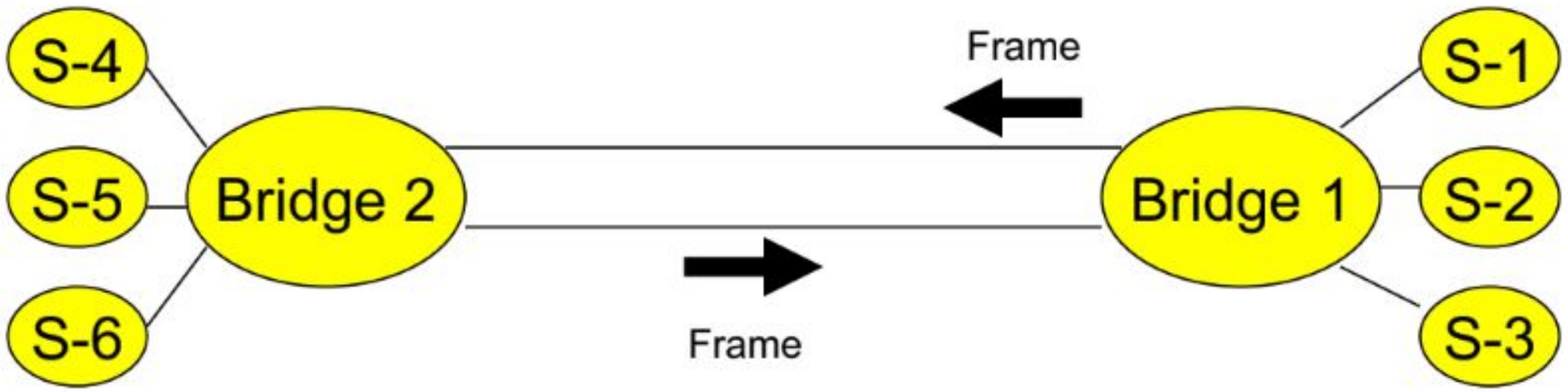
- Cut through will process the destination MAC address and forward the frame based on the entry in hash table.
- Bridge will Relay Ethernet frame, may modify header.



Bridges:

Spanning Tree (IEEE 802.1D):

If we use multiple links from one bridge to another we create a loop for unknown frame, because the bridge will flood the frame to all its ports.

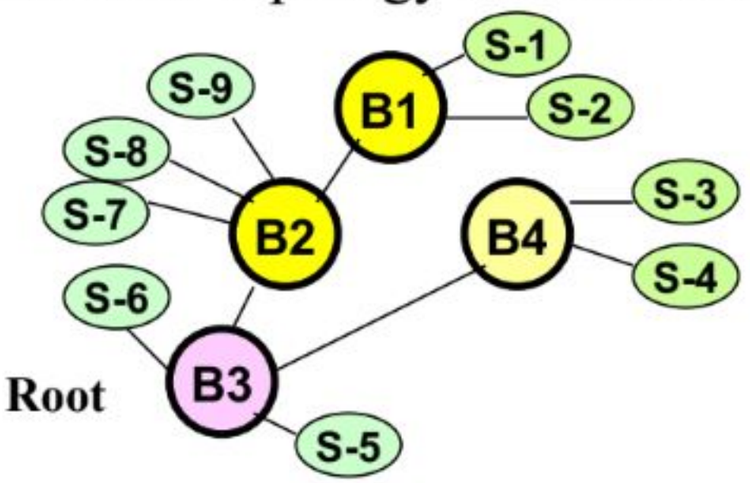


➢ Bridges:

❑ Spanning Tree (IEEE 802.1D):

Spanning Tree Algorithm concept:

1. Each station connects only to a single bridge.
2. One path exist from each station to another station
3. Bridges broadcast periodically a configuration frame from all its ports to neighbor, each bridge process the received broadcast message from its neighbor.
4. The received broadcast messages are not forwarded, they are processed.
5. In the configuration frame the bridges send their unique MAC addresses.
6. The lowest MAC address will be the root.
7. A shortest path from each bridge to root will be created.
8. The bridges will not use the port which are not included in spanning tree paths.
9. The algorithm is active all time to find out the new topology modifications (adding, removing)



Repeaters:

They are devices which filter and amplify the physical signals for transmission.

They are used to extend the reach ability of physical signal.

Hubs:

Are used for connectivity between multiple devices (inputs)

They are not amplifying the signals and do not lookup at the MAC addresses.

The devices access the hub should have the same speed.

The frames transmitted from stations may have collision.

Bridges:

- They operate at layer 2 and connect LANs.
- Each port has its own collusion segment.
- If the port operates full duplex, there is no collusion.
- The frames are buffered for Look up process of destination address to send the frame to proper output port.
- Multiple frames can be sent to multiple ports at the same time.
- Different speeds and networks can be connected to ports.
- The bridge may drop frames when input speed is higher than processing speed of bridge.

Wireless Local Area Networks IEEE 802.11

2. Media Access Control

- Using CSMA/CA (Collision Media Access Control with Collision Avoidance)
- Because the radio received signals are weak and the station at the same time can not transmit and verify the received signal, for this reason the CSMA/CD (Collision Media Access Control with Collision Detection) from Ethernet can not be used.
- Specific time (back off time) the station will wait to verify no signal is transmitted at that time, then transmits, should receive ACK from receiver, if does not receive ACK an error accrued.
- Back off time will be increased until the frame can be sent.

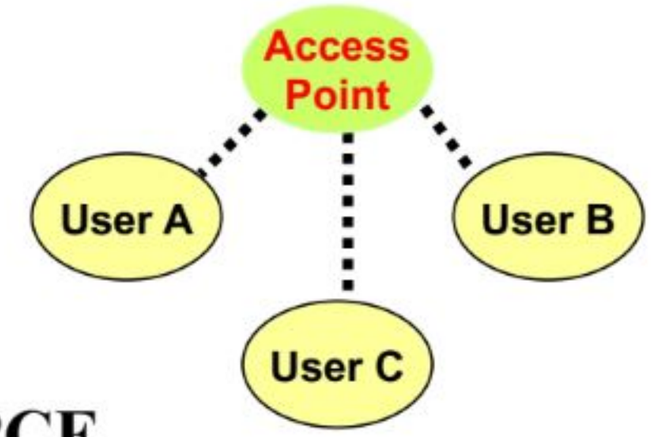
➢ Wireless Local Area Networks IEEE 802.11

2. Media Access Control

Two type of infrastructures:

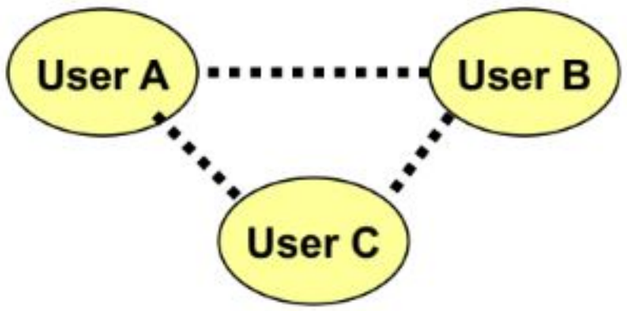
a) PCF (Point Coordination Function)

A node is the coordinator of communication between other nodes.



b) DCF (Distributed Coordination Function)

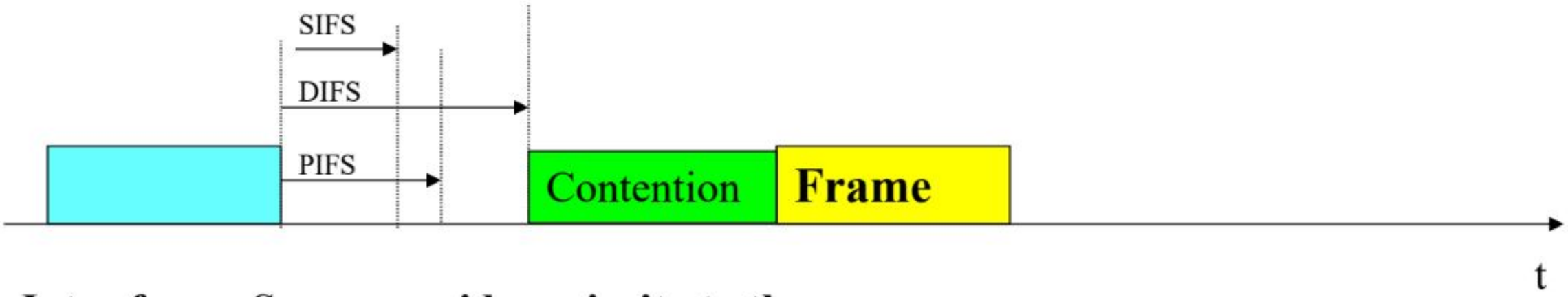
Each node operates independently is used not PCF.



Wireless Local Area Networks IEEE 802.11

2. Media Access Control

❑ Timing sequence



Inter-frame Space provides priority to the users.

PIFS (Point Coordination Function Inter-Frame Space): Transmitting device can transmit after PIFS and preempts contention-base transmission (Data).

DIFS (Distributed Coordination Function Inter-Fame Space): It is minimum idle time of medium for contention based service. (If zero, immediate access for devices to medium).

SIFS (Short Inter-fame Space), High priority can start after SIFS(RTS/CTS).

➢ Wireless Local Area Networks IEEE 802.11

2. Media Access Control

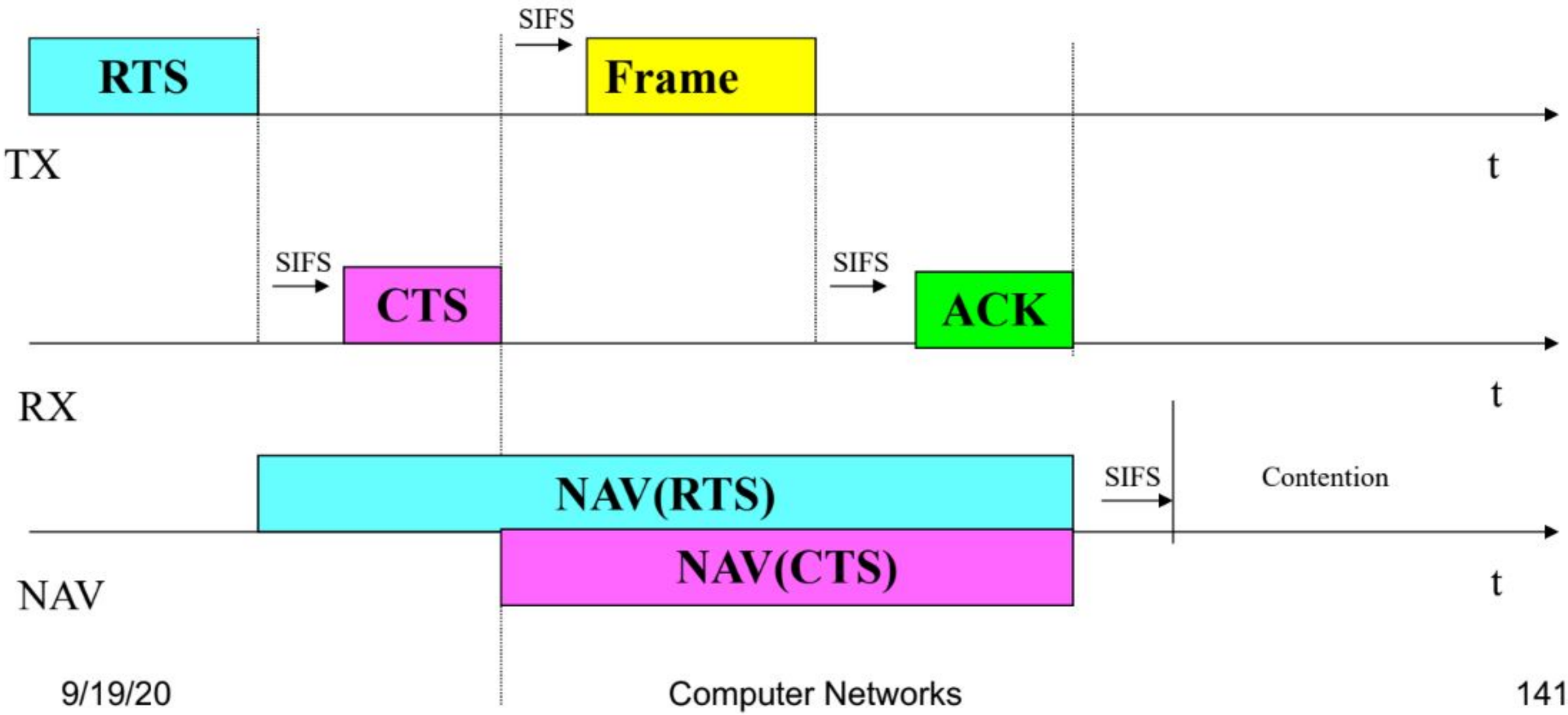
❑ Timing sequence

To have clear communication we use:

1- Media sensing for RF signal

2- Using NAV (Network Allocation Vector)

RTS (Request To Send)/ CTS (Clear To Send)



Bluetooth

- Connects communication devices in short distances (about 10 meters).
- Piconet structure used to connect master with 7 slave devices, the connectivity between master and slave is pairing.
- The master initiates the connection to one or more slaves.
- The piconets could be connected with each other over the bridge devices.
- TDM (Time Division Multiplexing) method is used between Mater and slaves.
- Scatternet is connectivity between multiple piconets over bridge devices.
- Parked nodes are devices in battery power saving mode, can respond to a master (max. 255 nodes).

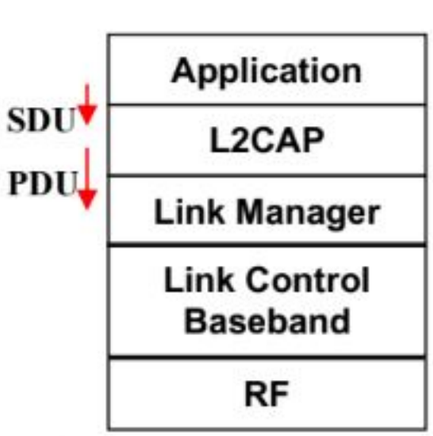
Bluetooth

Applications (Profiles):

- They are connectivity between keyboard, camera, audio, and headsets with PC.

L2CAP (Link Control Adaptation Protocol) Resource Manager

- Provides resource management when submitting L2CAP Protocol Data Units (PDUs) to the controller for transport, packet size 64 KBytes.
- The L2CAP Service Data Units (SDUs) are segmented into manageable PDUs and then fragmented into start and continuation packers of a size suitable for the controller buffers.
- Multiplexing/De-Multiplexing, protocol type differentiation
- It manages controller buffers to ensure availability for channels with Quality of Service (QoS) commitments.
- Error handling, retransmission.



Link Manager

- The creation, management and deletion of the L2CAP channels for the transport of service protocols and application data streams are controlled by the channel manager.
- L2CAP is used to communicate with a channel manager on a remote device to create the L2CAP channels and connect the endpoints with the required QoS.

Bluetooth

Baseband Resource Manager

- The access to the radio modem is controlled by the base-band resource manager.
- The base-band resource manager schedules time on the physical channels to all of the entities that have negotiated an access contract.
- The base-band resource manager also negotiates access parameters QoS that is required.

Link Controller

- The link controller encodes and decodes Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link.
- TDM is used, the even slots are used for master, the odd numbers for slaves.
- The link controller also does the link control protocol signaling for flow control.
- Security at pairing time, the transmitted key will be confirmed by receiver.

RF Block

- The RF block transmits and receives packets on the physical channel.
- The control path between the base-band and the RF block allows the base-band block to control the timing and frequency of the RF block.
- Using adaptive frequency hoppy, excludes the RF channels used by other wireless technologies.
- Transmission speed max. 3 Mbps.

Bluetooth

Physical Link Channel Types:

SCO (Synchronous Connection-Oriented):

Slots are at very beginning by master allocated for each slaves, carries voice.

Three SCOs could be connected to the same slave.

A slave can support up to 3 SCO links from same master or 2 from different masters.

ALC (Asynchronous Connectionless):

The slots are not reserved the master can exchange in any slot the information with the slave

NOTE: Restrictions on devices can form a physical link in a piconet:

There is always a physical link between the master and each slave, but there can be no physical links between two slaves.

Medium Access Control

Bluetooth

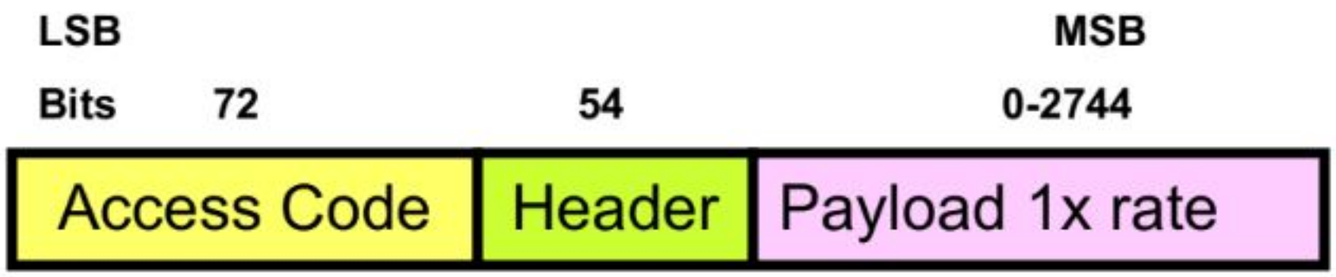
General Frame Format

The packet header fields are generated at basic rate and payload header at higher rate.

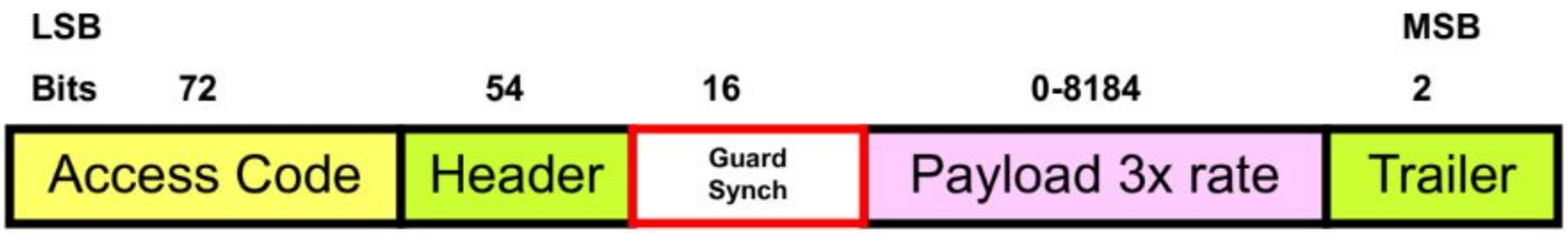
Frame Formats:

1) **Basic Rate Frame:**

Payload 2744 bits, uses 5 slots for transmit. For single slot payload is 80, 120, or 240 bits.



2) **Enhanced Rate: Carries more than 3 times payload bits.**



Access code: Is 72 bits fixed size, is used for synchronization, master identification.
All packets sent in the same piconet are preceded by the same channel access code.
Paging access code is used to send message to other units.
Inquiry is used to discover what other Bluetooth units are active in the coverage area.

Bluetooth

General Frame Format

Packet Types:

Two physical links are defined, SCO (Synchronous Connection Oriented) and ACL (Asynchronous Connectionless).

For each of these types 12 different packet types are defined.

Four control packets are common to all link types ,4 bits type code is used

Packet Header:

Is 54 bits, contains LC (link Control) information and consists of six fields:

- **AM ADDR: 3-bit for active member address, max. eight devices**
- **TYPE: 4-bit type code, SCO (Synchronous Connection Oriented) and ACL (Asynchronous Connectionless).**
- **FLOW: 1 bit flow control, set by slave when its buffer is full.**
- **ARQN: 1-bit ACK, used by slave for ACK piggy backing with data frame.**
- **SEQN: 1-bit sequence number bit, used to ask for retransmission of frame**
- **HEC: 8-bits Header Error Check**

The total number of header is 18 bits.
Three times the 18 bits are repeated, 18x3=54.
All three samples are verified by slave the majority bit set will be processed.

- **Routing:**
- **Routing Algorithms**
- **Ad Hoc Networks Routing**

AODV (Ad Hoc on-demand Distance Vector):

Destination will use in the reply message a sequence number that will be incremented by each response. If is a new route the value starts with zero.

The sequence number is used by source to refresh its table.

The responses with the higher values are saved in the routing tables on the response path.

TTL is set by source incrementally (1,2,3,..) if no response comes back the TTL will be incremented.

Soft state (Hello) messages are used monitor the path to neighbor, if no response arrives then the connection is no more active.

Since topology changes dynamically if the packet can not reach through an existing path destination, then the path is removed from table and new path will be calculated.

Network Layer

- **Routing:**

- **Congestion Control:**

The congestion will reduce the good put.

The congestion control will prevent congestion collapse.

Flow control provides a control mechanism between source and destination.

Solutions:

- **Reduce the input** to the network or add more resources (Bandwidth).
- **Discard packets (Load Shedding):**

  RED (Random Early Detection): dropping packets randomly from each circuit when the buffer reaches a defined threshold in the router.

- **Hop-by-Hop Backpressure:**

When destination experiencing low buffer it will inform hops carrying traffic to slow down transmission rate to destination.

- **Routing:**
- **Congestion Control:**

Solutions:

- **Admission Control:**

  Checking bandwidth availability, monitoring arrived traffic into network traffic based on average bit rate and the traffic burst (leaky Bucket, Token bucket), by passing the heavy loaded areas in network.

- **Provisioning**
- **Traffic aware network** (time of the day traffic), provide more paths
- **Traffic Throttling:**

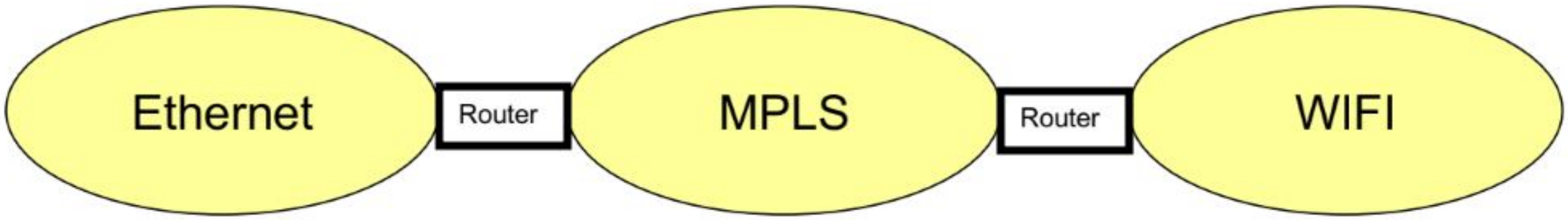
  The queue threshold in the buffer can predict a congestion. Router will generate messages to notify the source, choke packets are generated to inform the source.

  ECN (Explicit Congestion Notification) will notify destination to inform source to slow down.

Internetworking

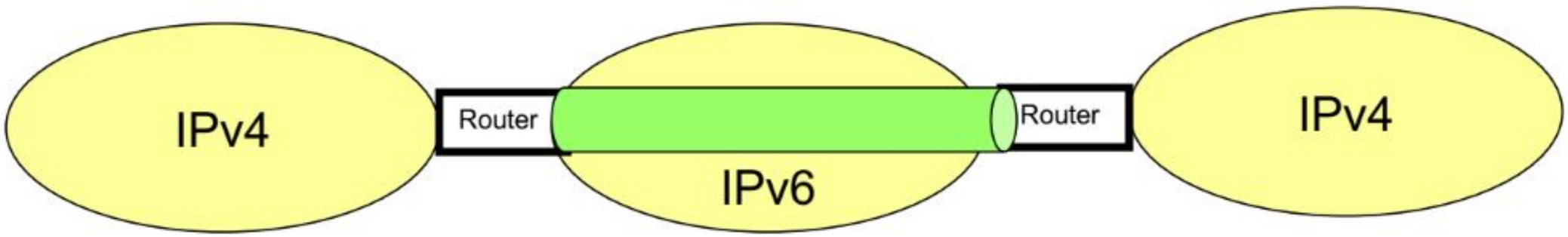
- **Internetworking provides connectivity between different protocols and network types.**

Multiprotocol routers support multiple protocols.



Tunneling:

Source and destination are on the same network type.



➢ Internetworking

❖ Fragmentation:

The packets are fragmented based on MTU (Maximum Transmission Unit).

❑ Transparent method:

At the edge ingress router of network segmentation and fragmentation will be performed , the intermediate nodes will receive fragments, will reassemble those and send to next intermediate router, this router will fragment the packets and send to next router, at egress then reassembly process will be performed at egress router.

❑ Non Transparent Method:

At the edge ingress router of network segmentation and fragmentation will be performed and reassembly process will be performed at destination host, no fragmentation is performed at intermediary routers,.

❑ Path MTU Discovery:

The host sends a packet with "Don't Fragment" flag set to network, the routers have smaller packet sizes will response with packet size which can support, the host will perform fragmentation and sends the new packet to destination host.
If the route changes the MTU may change, the source will receive an error to correct the MTU.

ICMP (Internet Control Message Protocol):

Provides connectivity related information.

ICMP Messages:

- **Redirect:** Will inform the source to update the routing table and use correct path.
- **Echo and Echo Reply (Ping):** Will verify designation is reachable, expects response from destination.
- **Time Stamp request and reply:** Will time stamp the message by departure and measure the time between transmit and receive.
- **Destination unreachable:** The destination can not be reached or if DF (Don't Fragment) flag in IP header is set and the packet size has larger size than MTU.
- **Time Exceed:** Will notify TTL was expired and the packet had been dropped to prevent the loop.
- **Parameter Problem:** Invalid value in the IP header is detected.

OSPF(Open Short Path First):

- It is an interior routing protocol which is used by Autonomous Systems.
- Is using “Link State” algorithm.
- Supports load balancing, splitting load over multiple paths.
- The Hierarchical concept is supported.
- Supports Unicast and Multicast.
- It creates the map of network (graph) with connections between nodes (arcs) with their weights.
- From network to routers the weight is zero, as well the hosts on a network have one path to hosts with weights zero (route to host but not through them).
- Every node calculates the shortest path to all nodes in the network.
- The network is segmented in “areas”, routers inside one area only are “internal routers”.
- Area zero is defined as backbone area which contains backbone routers.
- All areas are connected to backbone area (area zero).
- Area border routers will summarize destinations host’s routes based only on cost and propagates to other areas for selection of better cost and enter that (shortest path selection) in their routing table.
- When an area has only one router is named as stub area.

➢ OSPF(Open Short Path First):

When the source and destination are in different areas the path should go through area zero (backbone).

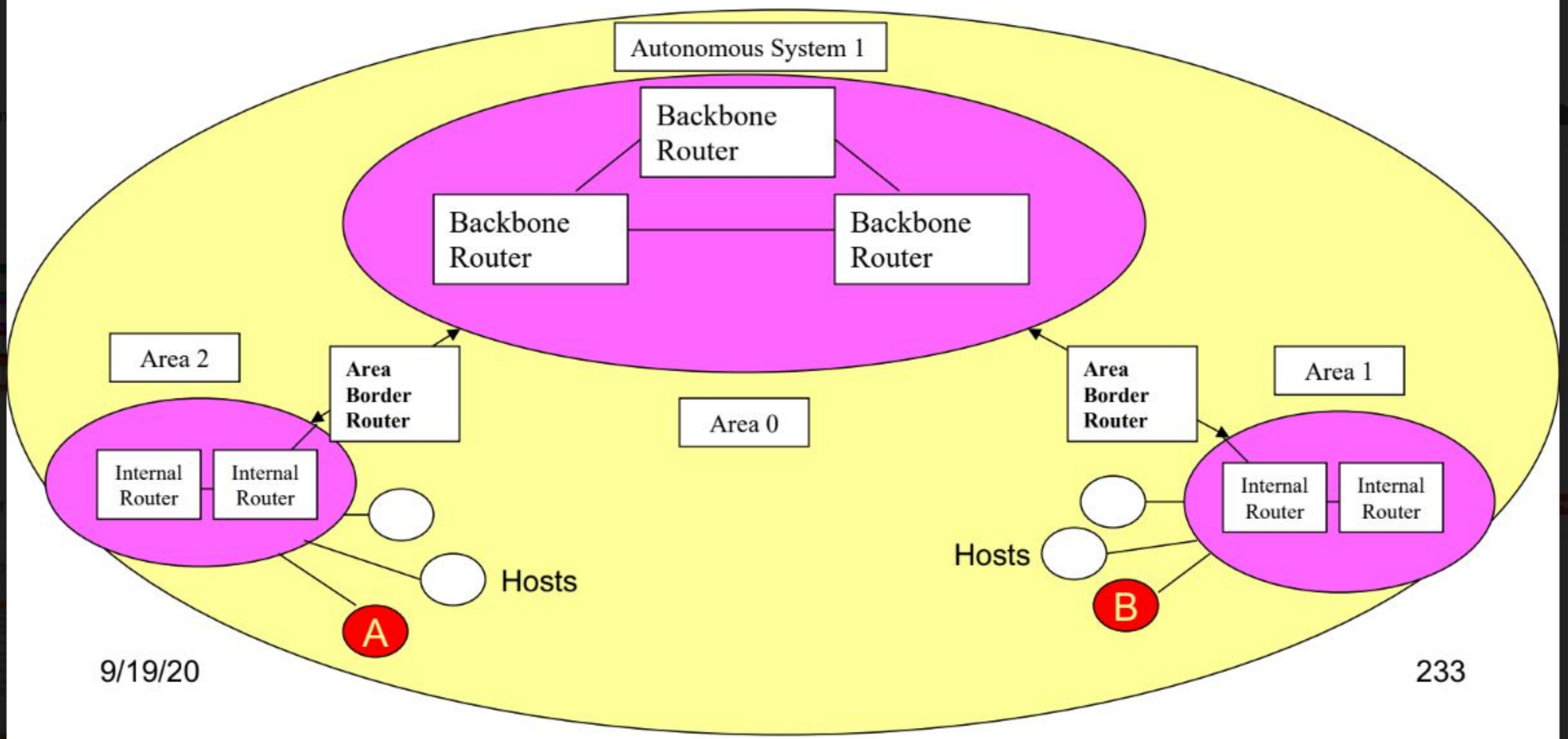
HELLO messages are sent at the initialization to neighbor nodes and multicast to all routers in a group.

"Designated Router" is adjacent to all other routers and exchanges routing information with them.

Messages are: Hello, Link State Update, Link State ACK, Link State Request, Database Description.

A hot standby designated router is used as backup for crash.

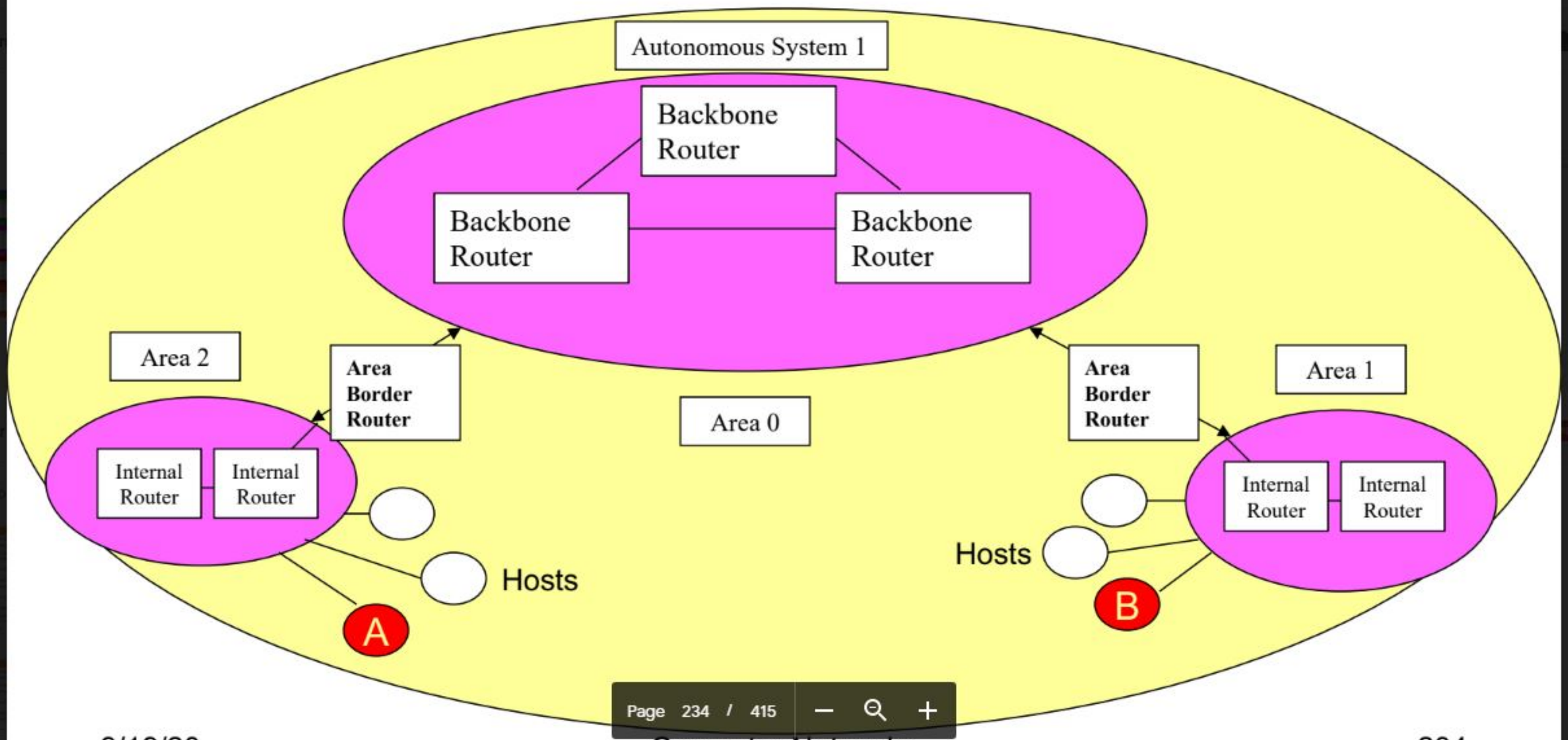
"Link state update" with unique sequence numbers are sent periodically from routers to adjacent router.



➢ OSPF(Open Short Path First):

In response to link state message the "Database Description" message is sent with sequence numbers with states entries held in database to verify which entry in database is the most recent, the nodes will update their tables.

Adjacent nodes or routers can issue link state request.



➢ MPLS (Multi Protocol Label Switching):

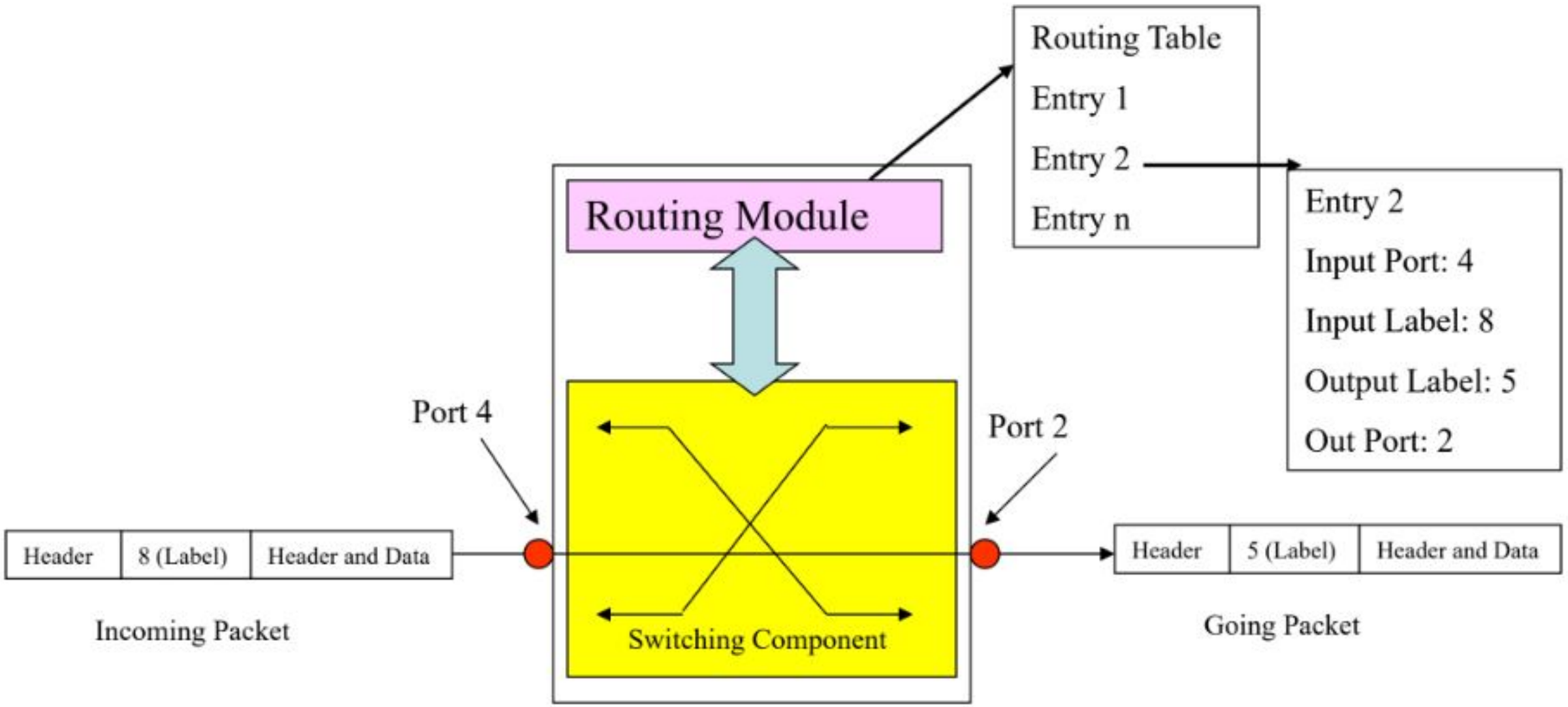
Repetitive and high priority data flows use virtual circuit switching paradigm instead of classical routing paradigm (Packet-by-packet).

Enables:

- **Traffic Engineering**
- **Label is used as pointer to the explicit routing policy**
- **Service Differentiation**
- **Scalability**

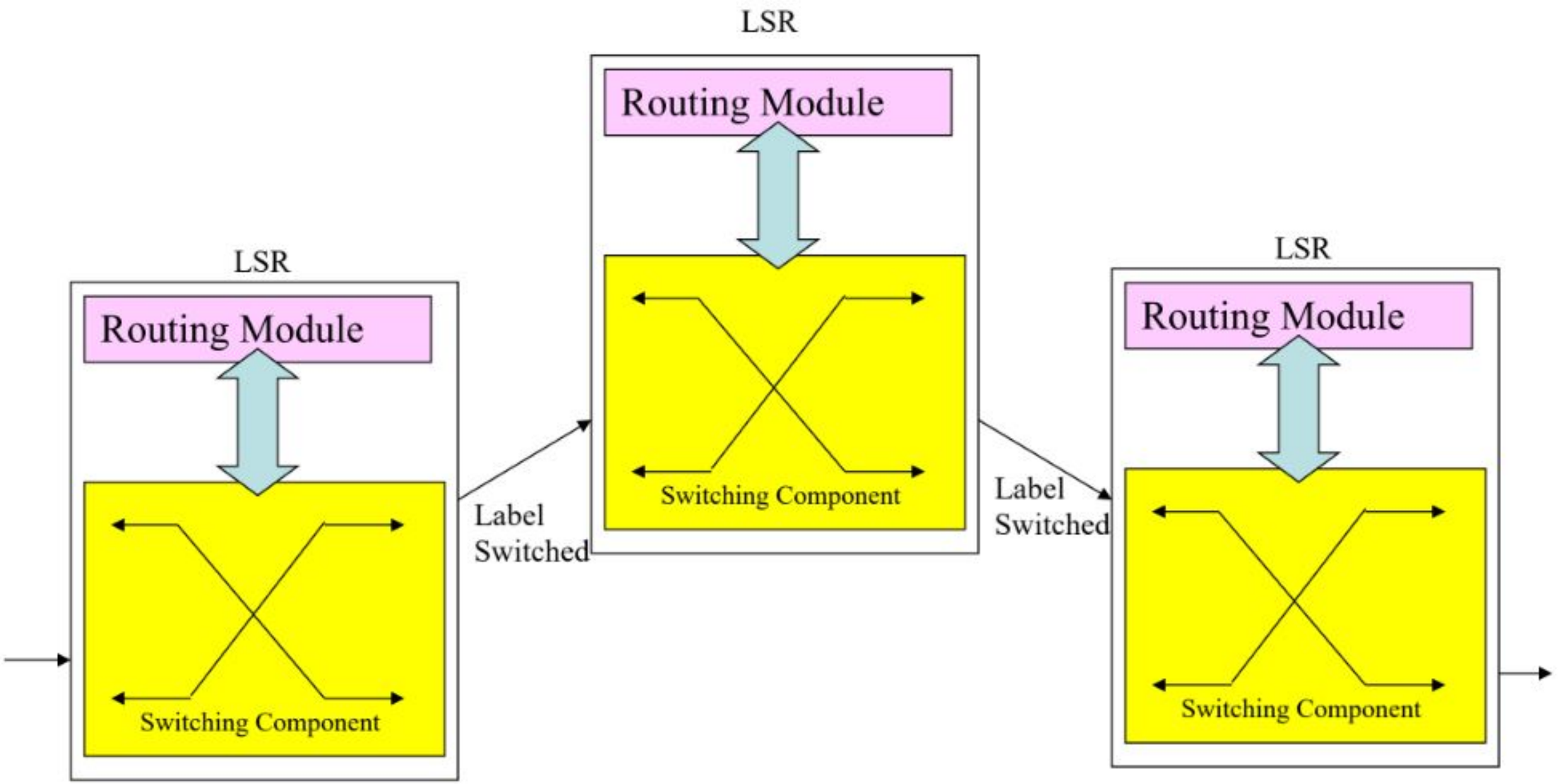
➢ MPLS (Multi Protocol Label Switching):

Label Switching Operation:



➢ MPLS (Multi Protocol Label Switching):

Label Switching Operation:

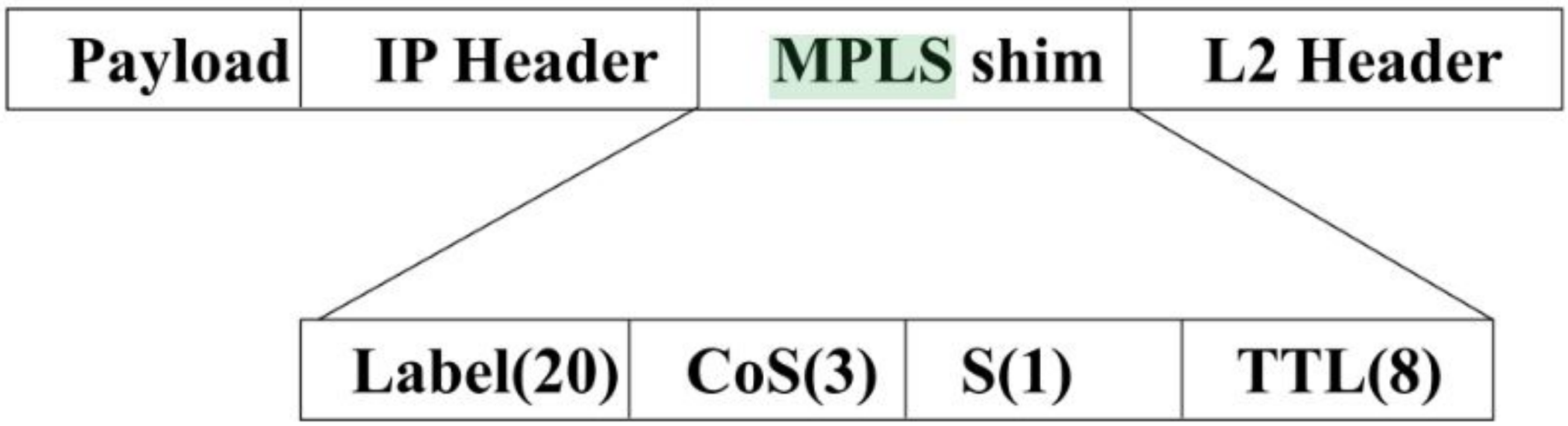


➢ MPLS (Multi Protocol Label Switching):

Label Switching Operation:

Packet Entry:

- Labels are shimmed into the packet between Network and data link layers.
- If FEC is not present, then packet is routed



➢ MPLS (Multi Protocol Label Switching):

Label Switching Operation:

Packet Exit :

- ❑ At the egress the labels are removed
- ❑ Packets are conventionally routed

Network Hopping:

- ❑ Intermediate Routes check for next Label
- ❑ If not found the packet is routed
- ❑ Else it is swapped with new label and forwarded

MPLS Operation:

Label Management:

1-Time-to-live:Loop prevention

2- Class of Service: Provides packet processing priorities

3- LDP provides a reliable distribution of Labels for Forwarding

- Distribution by local node or ingress node, propagates to egress
- Distribution by egress node to ingress

➢ Transport Protocols:

Two transport protocols in IP network,

1. Connectionless Protocol UDP (User Datagram Protocol)
2. Connection Oriented Protocol TCP (Transmission Control Protocol).

1. Connectionless Protocol, UDP (User Datagram Protocol) RFC 768

- ❖ It provides multiplexing, de-multiplexing, error detection, does not provide congestion control and retransmission.
- ❖ **UDP Header, 8 Bytes**

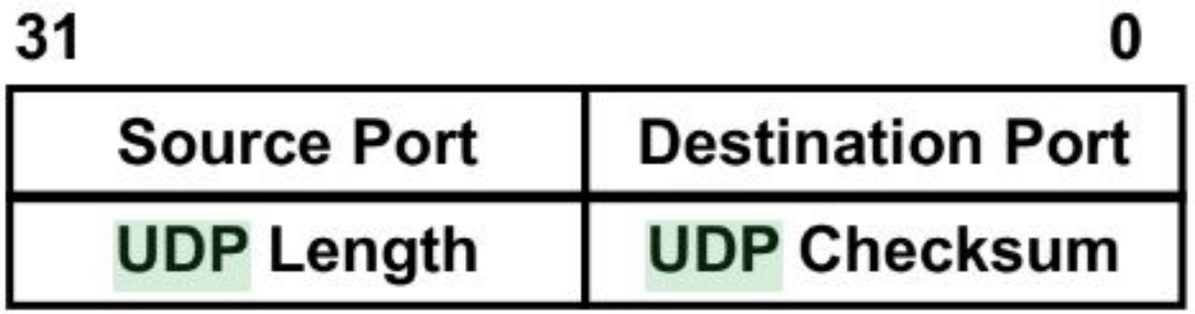
Port: The packet is forwarded to the destination port number identified in header.

UDP length: Maximum 65,515 Bytes

Checksum: will include UDP header + payload + pseudo header.

The packet is padded with zeros to have a 16 bit words, then adds all Bytes and compute one's complement of the sum.

If checksum is not calculated then is set to zero, for voice traffic is zero



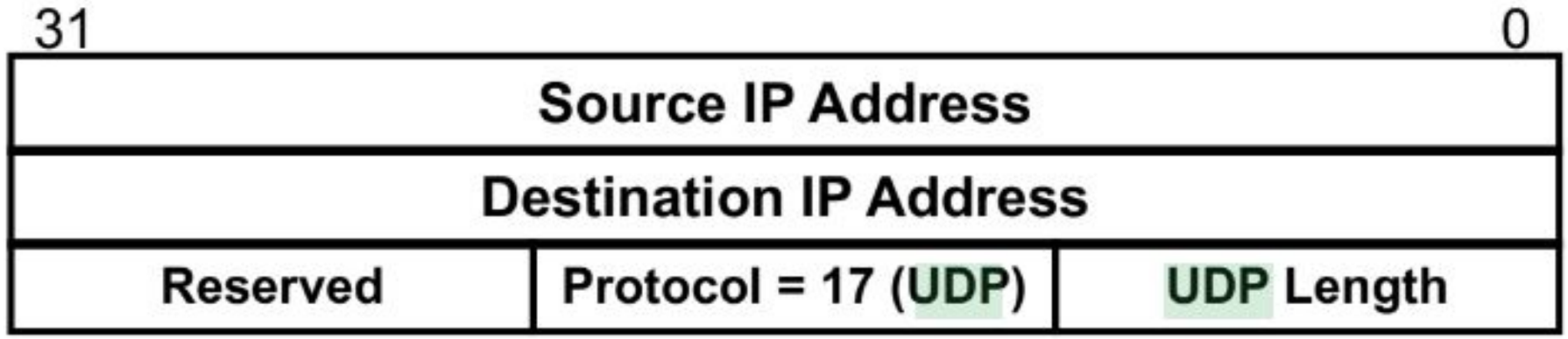
- **Transport Protocols:**

1. **Connectionless Protocol, UDP (User Datagram Protocol) RFC 768**

❖ **The IP Pseudo Header contains:**

Source IP Address, Destination IP Address, Protocol identifier for UDP =17, and UDP length which consists of UDP header 8 Bytes + payload.

NOTE: TCP uses the same pseudo header for checksum calculation.



❖ **UDP applications**

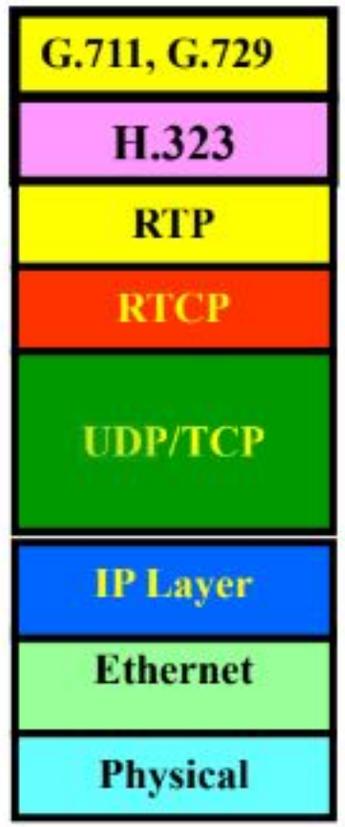
The applications are remote procedure call to servers, short messages with timing bounded responses, example DNS.

Transport Layer

- **Transport Protocols:**

1. **Connectionless Protocol, UDP (User Datagram Protocol) RFC 768**

❖ RTP (Real Time Protocol)



For real time communication between client and servers, used for voice and video transmission using UDP transport layer.

No Guarantee of delivery since using UDP.

RTP packet contains sequence numbers.

Can carry different encoding types.

Using single counter to timestamp in sequence multiple streams to be played out in synch (background sound, subtitle, multiple languages)

Transport Protocols:

1. **Connectionless Protocol, UDP (User Datagram Protocol) RFC 768**

❖ RTP (Real Time Protocol)

RTP Header:

Version: currently 2

P: Padding the packet with n*4 to become, last field will have the count of Bytes

X: Extension bit =1 (enable) , Extension bit =0 (disable)

CC: Contributing sources (0-15)

M: Mark bit, will mark the start of frame

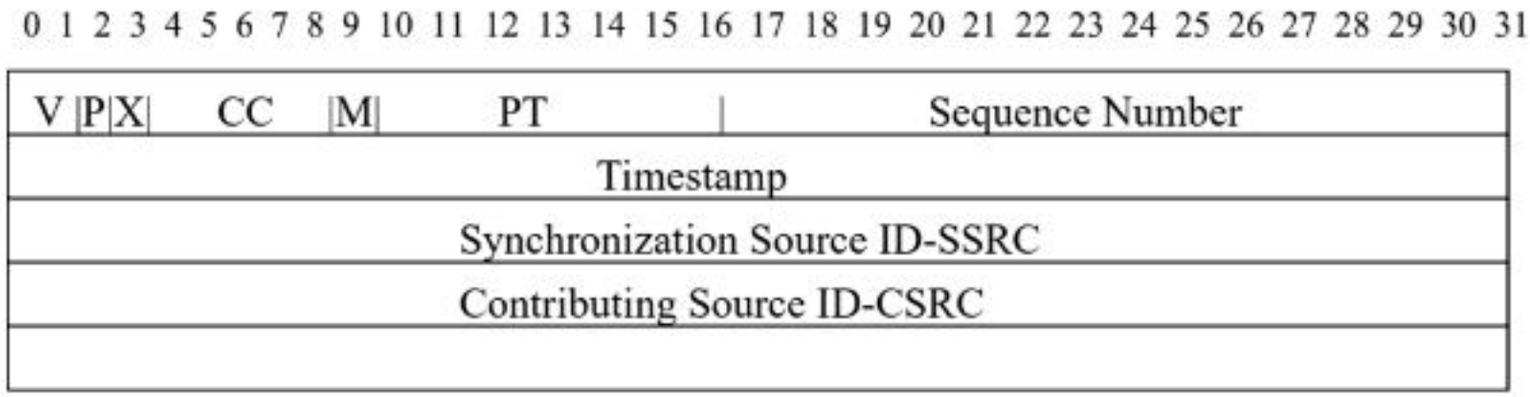
Sequence number: the sequence of frames.

Payload type: Type of encoding, on the fly encoding may change

Timestamp: The time packet was generated

Synchronization Source Identifier: Which stream owns the packet.

Contributing Source Identifier: Used for mixers, if used that will be the source



Transport Protocols:

1. **Connectionless Protocol, UDP (User Datagram Protocol) RFC 768**

- **RTCP (Real-Time Transport Control Protocol)**

It defines procedures for hosts using RTP to exchange information to control the session.

Features:

- Monitors packet loss and inter-arrival jitter
- Traffic source identification
- RTCP packets are transmitted every 5 seconds
- It uses RTP port number + 1 (Means different stream to carry the information)

➢ Transport Protocols:

1. Connectionless Protocol, UDP (User Datagram Protocol) RFC 768

❖ RTP (Real Time Protocol)

Playout buffer:

- **Will reduce the jitter which is caused by different inter-arrival times.**
- **The packet will be put in buffer, if their arrival time is in acceptable range else will be discarded.**
- **Playback point is the time a receiver waits to play out the packet, if the jitter is high the receiver needs to set the playback point higher.**
- **The other method is to set application the Marker "M" in RTP packet in the gasp in a conversation, then receiver plays out the buffer.**

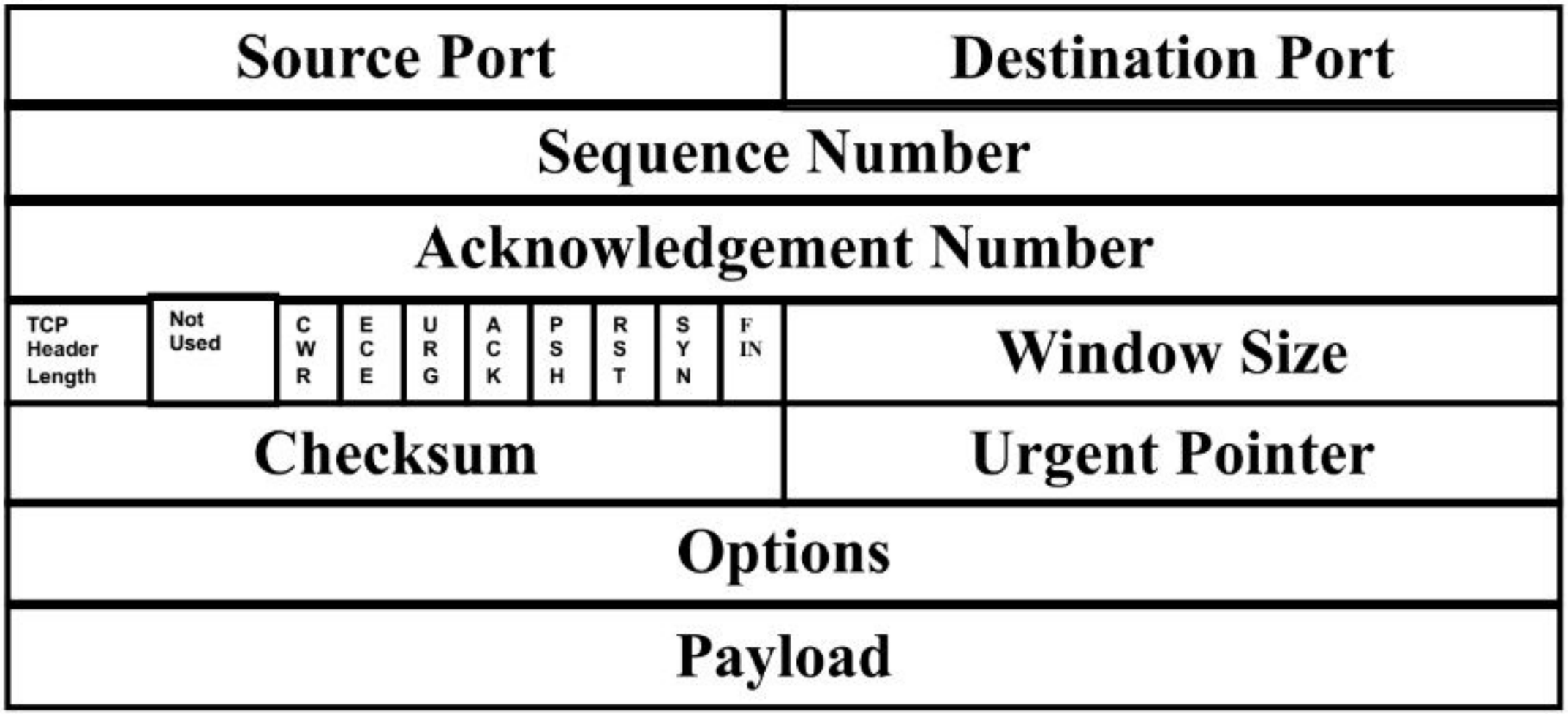
➢ Transport Protocols:

2. Connection Oriented Protocol, TCP (Transport Control Protocol)

RFC 793, RFC 1122, RFC 1323, RFC 2018, RFC 2581, RFC 2873

- TCP provides reliable transport over Internet.
- There are designated ports for specific services.
- TCP connection is bi-directional.
- TCP buffers data after packaging large amount and then transports.

TCP Header, 20 Bytes:



- **Transport Protocols:**

2. **Connection Oriented Protocol, TCP (Transport Control Protocol)**

Header, TCP Flags:

- **PUSH Flag:** Application requests for immediate transmission of specific data.
- **Urgent Flag:** Stops buffering data, sends all buffered date with some application's control data, receiver will interrupt all activities and handle the urgent data, it is application signaling.
- **ECE (Explicit Congestion Notification Echo) Flag:** is set to say to sender slow down
- **CWR (Congestion Window Reduced) Flag:** sender will tell to receiver that has slowed down the rate.
- **ACK Flag:** Is set for ACK packets.

NOTE: Window size 0 in ACK means busy, don't send more

- **RST (Reset) Flag:** Reset connection, reject invalid sequence No., refuse connection.
- **SYN Flag:** Set up connection.
- **FIN Flag:** Disconnect, no more data for transmit.

- **Transport Protocols:**

2. **Connection Oriented Protocol, TCP (Transport Control Protocol)**

- **TCP Header:**

Sequence Numbers: Used for segmentation and ACK of packet. The next expected Byte number is included in ACK.

Payload: The range is defined by MTU and maximum can not be above 65,515 - [20(IP header)] – [20 (TCP header)] = 65,495 Bytes.

Source Port, Destination Port: Identify the connection end points

Header Length: Contains variable options field, zero or more n*32 bits.

Window Size: Will be sent in ACK contains Bytes can be processed by receiver.

Checksum: Is built on header + data

Options: Option contain TLV (Type, Length, Value), provides additional options. Using Window scale option both side negotiate the maximum packet size.

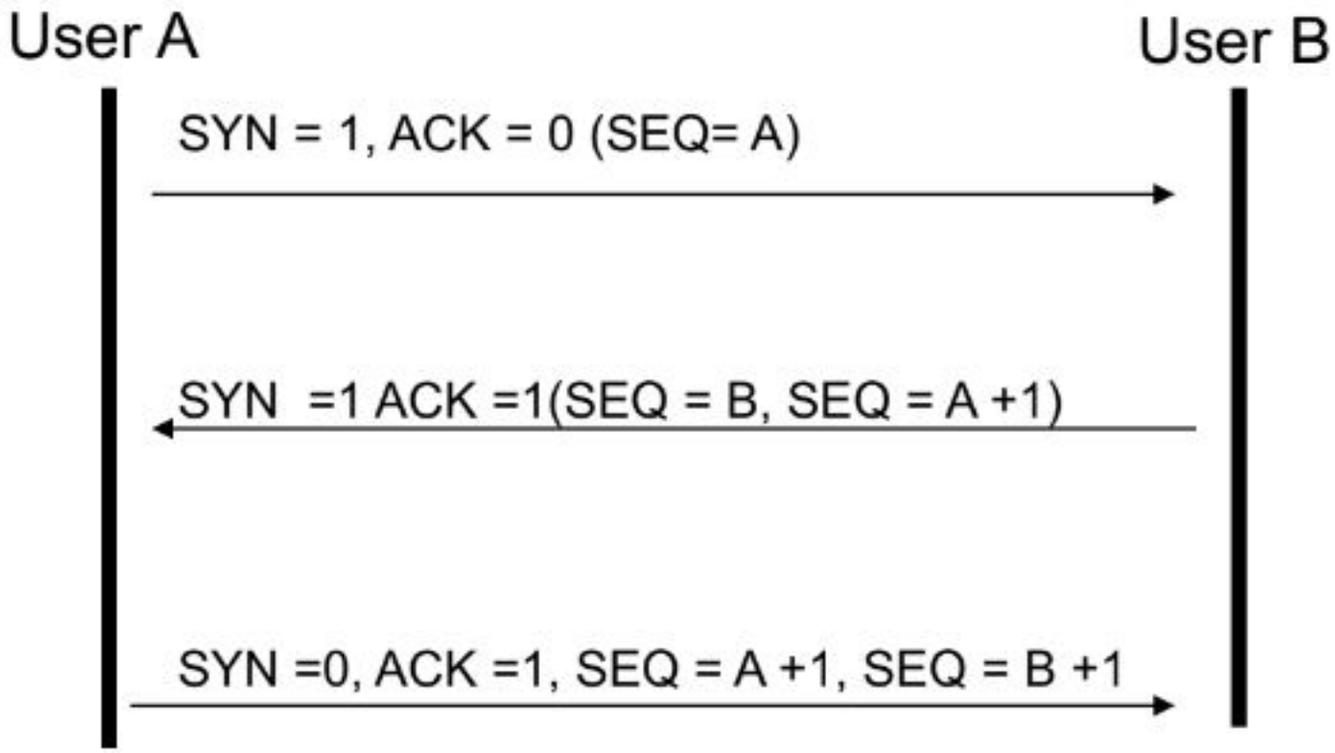
- **Timestamp option** to verify round trip delay, and packet loss
- **SACK (Selective Acknowledgement) option** will verify duplicate packets.

Transport Layer ***Review

- **Transport Protocols:**

2. **Connection Oriented Protocol, TCP (Transport Control Protocol)**

TCP 3 Way handshake Connection Setup:



SYN Flood: Stops server to operate.

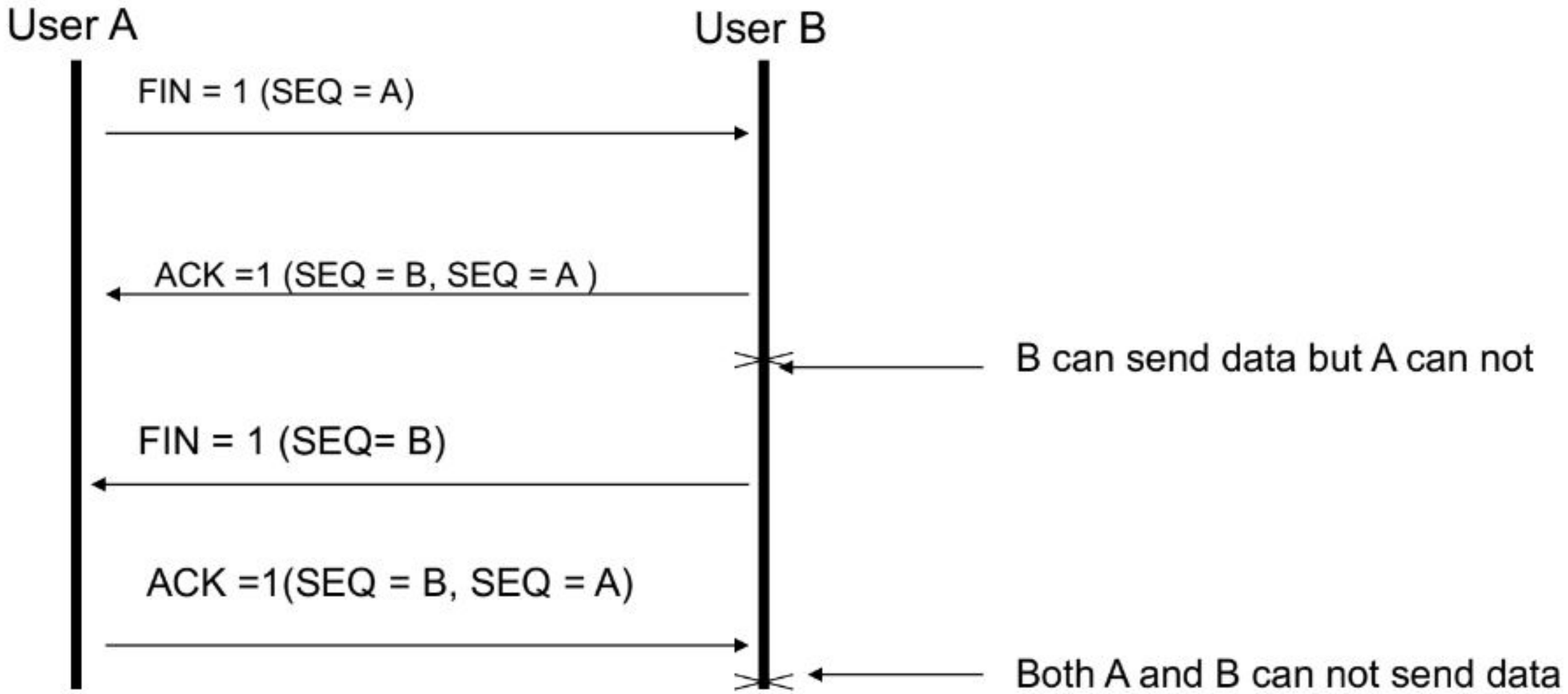
A malicious host sends many SYN packet and does not complete 3 way handshake.

The SYN cookies prevent that by using crypto sequence number generated by using IP address and port or other known data to use for crypto algorithm, the response will be decrypted and verified.

- **Transport Protocols:**

2. **Connection Oriented Protocol, TCP (Transport Control Protocol)**

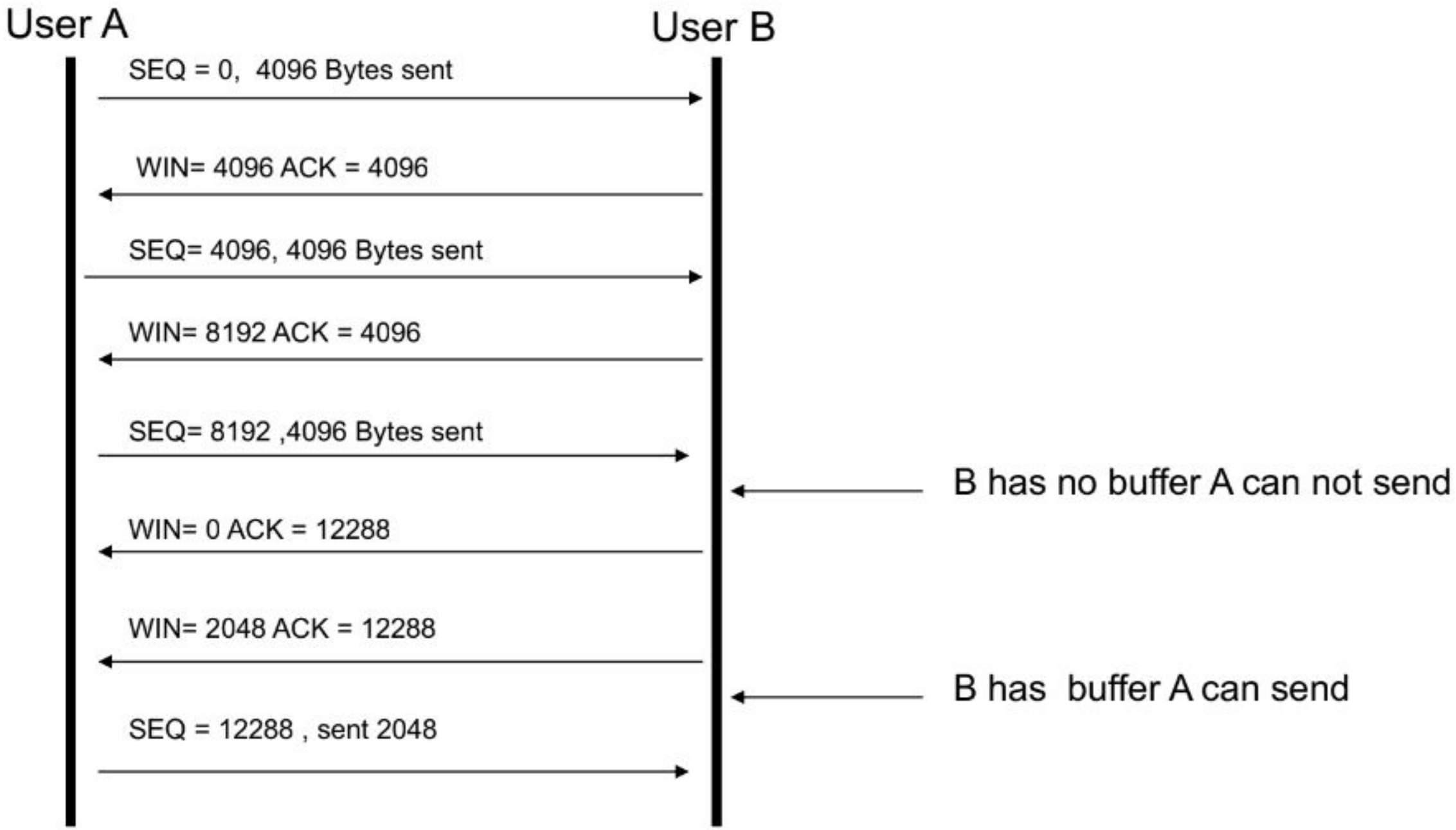
TCP Connection Release:



- **Transport Protocols:**

2. **Connection Oriented Protocol, TCP (Transport Control Protocol)**

TCP Window Rotation



❖ Connection Oriented Protocol, TCP (Transport Control Protocol)

Silly Window Syndrome:

Transmitter sends large packet but receiver Application reads one Byte and sends Request for one Byte to source, when this process repeats will cause the bandwidth is wasted for Byte by Byte transmission.

Solutions:

1. **Receiver Side:**

The receiver should not send small window update, should send when the number of packets reaches a defined limit which was defined at initialization time or half of that.

The receiver should put a limit on the number of Bytes sends to application, not a small number.

2. **Transmit Side:**

The transmitter should not send small packets.

➢ Connection Oriented Protocol, TCP (Transport Control Protocol)

❖ TCP Timers:

a) Retransmission Timer:

This timer is set when no acknowledgement arrives from peer before the timer expires else the packet will be retransmitted.

b) Persistence Timer:

Prevents deadlock, when receiver sends ACK with zero (no buffer available)

If the new update packet is lost then persistence timer will expire and sender will send a probe to ask for the window size.

c) Keepalive Timer:

This time will become active when the link becomes idle.

This message will help to keep the connection alive.

Connection Oriented Protocol, TCP (Transport Control Protocol)

TCP Congestion Control:

The Network Layer will inform Transport Layer.

TCP handles a congestion window, which contains number of Bytes the sender has in the network.

AIMD (Additive Increase Multiplicative Decrease) is used to control the congestion window, additive will increase the bit rate then by congestion decrease multiplicative.

Slow start:

- **Initializing the congestion window, use linear increase and AIMD.**
- **For each ACK received the congestion window will be incremented by one.**
- **Effectively doubling the window size each round trip time (exponential), sending first 1 packet, then 2 packets , 4 packets, …**
- **The transmission rate will be increased until packet loss is detected**
- **Transmitter will reduce the offered number of packet.**
- **When slow start threshold is reached, then TCP uses slow-start the linear growth algorithm, the window is increased by 1 segment for each Round Trip Time.**
- **When the time out happens and transmitter does not receive ACK, the slow start begins again (Congestion occurred).**

- **Connection Oriented Protocol, TCP (Transport Control Protocol)**

- **TCP Congestion Control:**

Duplicate Acknowledgement:

- A packet is lost when the next packets arrive at destination the ACK for them will be generated and carry the same number of expected packet which is lost.

(Generates three duplicate acknowledgements with the same acknowledge number)

- Receiver will receive duplicate ACKs will realize a packet is lost and has not arrived at destination.

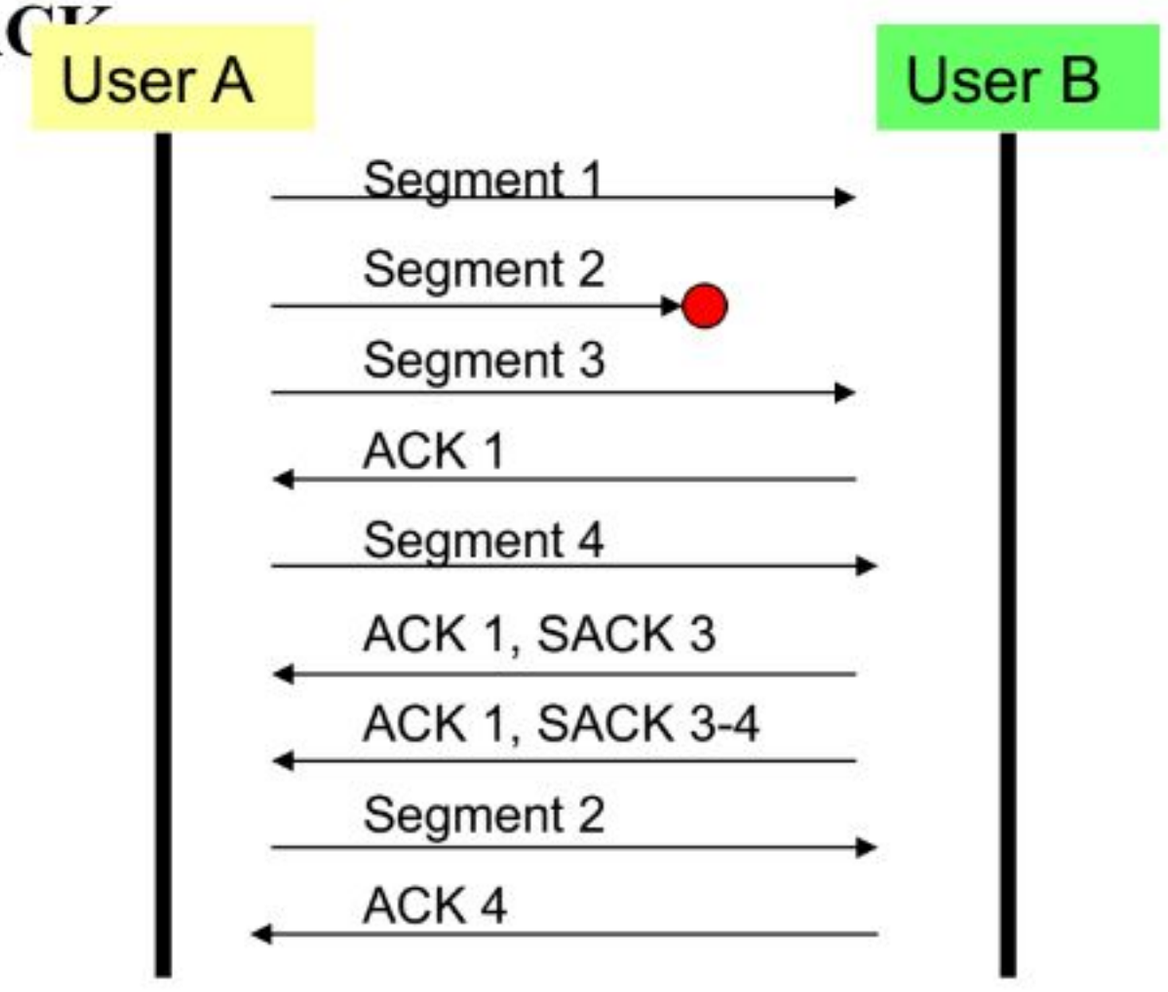
Fast retransmission:

- This method reduces the time a sender waits before retransmitting a lost packet.
- Starts with congestion window set to one with a threshold value half of the current congestion window.
- Congestion window will increase until reaches the threshold then will be linear increase, until packet loss happens, the procedure starts again.

- **Connection Oriented Protocol, TCP (Transport Control Protocol)**
- **TCP Congestion Control:**

SACK (Selective ACK) RFC 2883:

- **Will be negotiated at connection setup.**
- **It will send accumulative ACKs for received segment No. and implicitly the missing segment number in SAC**



➢ Connection Oriented Protocol, TCP (Transport Control Protocol)

❖ TCP Congestion Control:

❑ ECN (Explicit Congestion Notification)

- Is an extension to the IP header which allows advance notification of congestion.
- When a network node receives a packet marked as ECN capable and anticipates congestion, it will set an ECN-flag notifying the sender (Traffic originator) of congestion.
- The sender then should decrease its transmission bandwidth.
- ECN is only used when the two hosts agree.
- TCP adds two flags in its header to indicate, the sender to reduce the amount of information it sends.
- TCP peers receiving marked packets lower their transmission rate to ease congestion and prevent segment losses.

Connection Oriented Protocol, TCP (Transport Control Protocol)

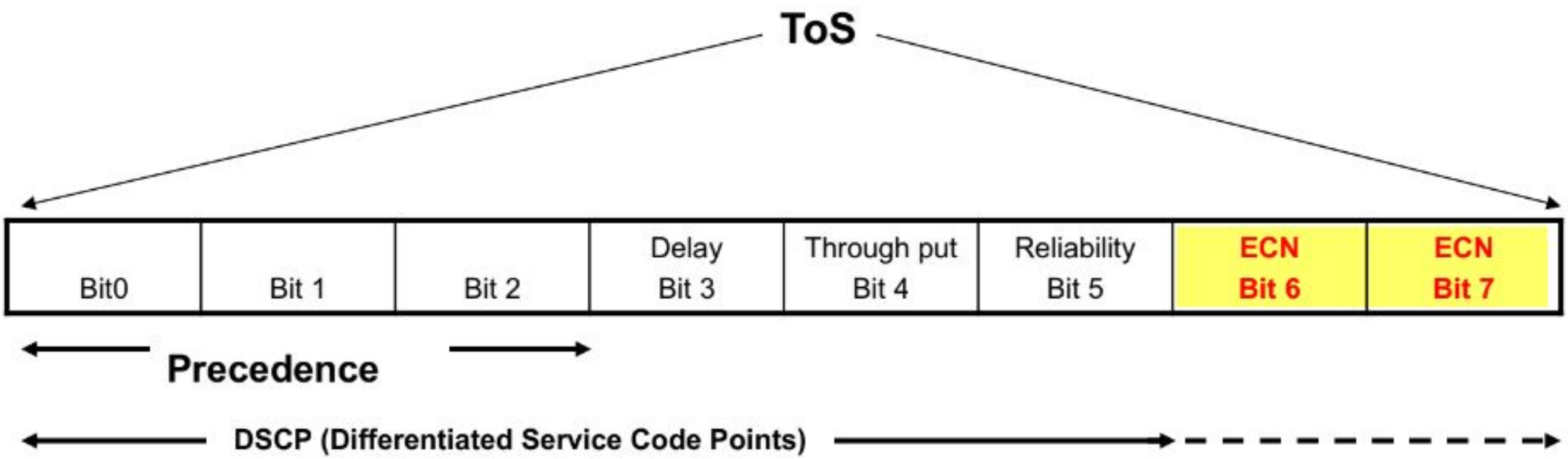
TCP Congestion Control:

ECN (Explicit Congestion Notification)

The two unused bits of ToS field are defined in RFC 3168 as the ECN field, which have the following values:

- **00** The sending host does not support ECN.
- **01 or 10** The sending host supports ECN.
- **11** Congestion has been experienced by a router.

An ECN-capable host sends its packets with the ECN field set to 01 or 10.



Transport Layer

➢ Connection Oriented Protocol, TCP (Transport Control Protocol)

❖ TCP Congestion Control:

❑ ECN Support in TCP

When an IP packet's ECN field is set to 11 by a router, the receiver is informed of the congestion in the transmission path, but not the sender (originater of traffic).

ECN uses the TCP header to indicate to the sender that the network is experiencing congestion and to indicate to the receiver that the sender has received the congestion indication from the receiver and has lowered its transmission rate.

❖ ECE, The ECN-Echo (ECE)

This flag is used to indicate that a TCP peer is ECN-capable during the TCP 3-way handshake and to indicate that a TCP segment was received on the connection with the ECN field in the IP header set to 11.

❖ Congestion Window Reduced (CWR)

This flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set.

NOT USED	NOT USED	NOT USED	NOT USED	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN

Applications

Electronic Mail

- Less snail mail sent after email deployment, provides spam filtering.
- File transfer with recipient email's address, broadcast or multicast address is used.

Topology Elements

User Agent: Provides command interface, composes, sends, receives, and filters messages.

Multimedia and International text support using MIME (Multipurpose Internet Mail Extension).

Screen size adaptation for messages to fit the screen.

Message Transfer Agent: Ships mail from user to user by using mail server, sends commands to mail server.

Message Transfer: SMTP (Simple Mail Transfer Protocol), RFC 821, 5321, transfers mail, reports status, does CC, BCC, high priority, forward to alternative recipient, and encryption.

Mail Box: It is maintained by mail server, saves received mail.

Applications

Electronic Mail

Spam:

Will be filtered buy ISPs, they see how the traffic is distributed from originating point to ISP, and they have the list of spammers originators.

botnets: It is a spam targeting a specific region for offers (Money in bank account, diploma, drugs).

Email Features:

- **Prioritize received emails:** put in different folders
- **Searching emails**
- **Auto response:** Is installed on mail server not in user agent (not always online). Paging user and sending subject field to pager. Vacation notification.
- **Signature block generation, adding response address, or propose, the list of recipients, all are provided by user agent.**
- **Email address format:** User_name@domain_name.
- **X.400 ISO:** Is used for addressing in some other countries.

C (Country) =DE/ST (State)=Bavaria/L (Locality)=Rim/PA (Add.)=234 Peter Str./CN (Common Name)= John Mayer

- Mailing List: A generated list located at originating user's side can be used by user agent, sends separate email to users.
- A generated list located at message transfer agent, users send to list then transfer agent sends to other users.

Applications

- **Electronic Mail**

Email Message Format RFC 5322

To: Recipient (s) DNS address, primary receiver (s).

Cc: Secondary receivers

Bcc: (Blind carbon copy): Sends email to a group of recipients but the Bcc recipients are not visible by primary and secondary in received email.

From: The person who initiates the email to administrator

Sender: Sends out the mail to a group.

Received: The transfer agent identity, receiver time by transfer each agent is added, used to return the response.

Return Path: Collected by receiver transfer agent which contains the list of transfer agents except the originated one.

Message-Id: Unique number for this message for identification.

Applications

➢ Electronic Mail

❖ Email MIME (Multipurpose Internet Mail Extension)

- ❑ Provides different languages for text (Russian, German, Chinese, etc.), audio, video, binary
- ❑ Is used for other applications (Web Browsing)
- ❑ RFC 822 for text is the base, if required the features of RFC 5322 are added

MIME headers:

MIME-Version: Message with out this header will be processed as an ASCII text.

Content-Description: A text will provide information about attachment (Dog, Cat, etc.)

Content-Id: Identifies the content, has same value as Message-Id.

Content-Transfer-Encoding: Encoding method used to permit 8 bit binary and self executed codes to be transferred by SMTP (Expects ASCII base64 Text encoding, each line is not longer than 1000 characters, we need encoding to convert to a transferable format).

Content-Type: Provides information about the presentation of content,

Content-Type: Type/Subtype example → Content-Type: video/mp4

Applications

➢ Electronic Mail

❖ Email MIME (Multipurpose Internet Mail Extension)

Example: Content-Type: Type/Subtype example → Content-Type: video/mp4

❑ Content types and subtypes defined in the standard:

Type	Usage	Subtypes
Text	*For text contents*	*Plain, css, html, xml*
Audio	*Voice, Music*	*mpeg, basic, mp4*
Video	*Moving pictures*	*mpeg, quicktime , mp4*
Image	*Pictures*	*jpeg, tiff, gif*
Model	*3D*	*vrml*
Application	*Generated data by app.*	*pdf, zip, javascript*
Message	*Encapsulated message*	*rfc 822, http*
Multipart	*Multiple types embedded*	*parallel, mixed, digest, mixed*

Applications

- **Electronic Mail**

- **Email MIME (Multipurpose Internet Mail Extension)**

Example: Content-Type: Type/Subtype example → Content-Type: video/mp4

Content subtypes defined in the standard:

Type Application: Generated data by application , user agent may take care of processing, else will be passed to application to handle the content.
User agent will not process leaves to user the processing by saving the content and open from a list of applications.

Message: Will isolate the content and put in a container, some big contents can be segmented and send individually.

Multipart:

- Subtype mixed: Multiple different types (video, audio, text) are embedded in email.
- subtype Alternative: The content is included in email in different media types (Plain text, HTML, voice)
- Subtype parallel: Two content types are delivered parallel (voice, video)
- Subtype Digest: Two contents are packet together in one composite packet

Applications

- **Electronic Mail**

- **Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321**

  - **The protocol does not have authentication**
  - **Any client can send the email**
  - **Clear text ASCII format is used, MIME base64 encoding provides extension for other formats.**
  - **No encryption provided.**
  - **Bandwidth is not optimized for transmission**
  - **Extension to SMTP (ESMTP) has been used to handle the above issues**

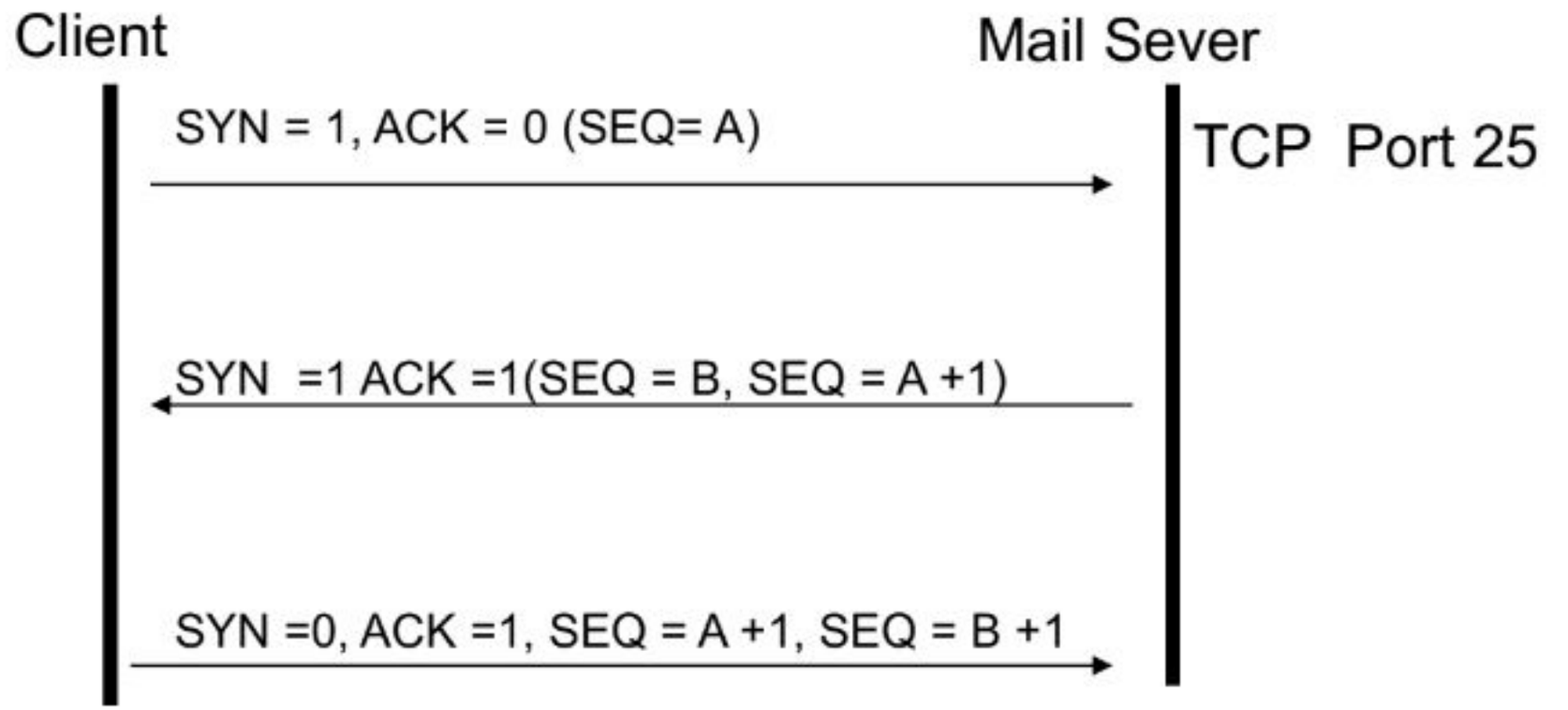
Applications

- **Electronic Mail**

- **Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321**

1- Client sets up TCP connection to port 25 of destination mail server

TCP Three Way Handshake:



Applications

Electronic Mail

Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321

Messages exchanged:

S: 110 intel.com SMTP service ready

C:HELO scu.edu **<<<client uses EHLO for extension for HELO (HELLO), server send supported extensions**

S:150 intel.com says hello to scu.edu

C:MAIL FROM: <peter@scu.edu>

S:150 sender ok

C:RCPT TO: <john@intel.com>

C:DATA

S:254 Send mail; end with "." on a line by itself

C:From: peter@scu.edu

C:To: John@intel.com

Applications

➢ Electronic Mail

❖ Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321

Messages exchanged: (Continued)

C:To: John@intel.com
C:MIME-Version: 1.0
C:Message-Id:<09995678.DDDD90908@scu.edu
C:Content-Type: multipat/alernative; boundary=rstklmno
C:Subject: Meeting tomorrow at 2 PM
C:--rstklmno
C:Content-Type:text/html
C:<p> Sound of Music
C:Good Movie to go with you.
C:
C:
C: --rstklmno
Content-Type:message/external-body;
C: access-type="image/jpeg";
C: site="library.scu.edu";
C: directory="pub";
C: name="matrix.snd"
C:content-type:text/plain
C:content-transfer-encoding:mpeg
C: --rstklmno
C:. <<<< End Mark
S:150 message accepted
C:Quit
S:121 Intel.com closing connection

Applications

Electronic Mail

- **Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321**

SMTP Extensions:

Keyword	Function
AUTH	Authentication
BINARYMIME	Server process binary
CHUNKING	Server can process large message in chunks
SIZE	Check message sized before transmission
STARTTLS	Use TLS
UTF8SMTP	International addresses

Connectivity to mail server:

Mail is sent by client through user agent to transfer agent to connect to mail server, the server will identify the user when AUTH extension used by user.

Applications

Electronic Mail

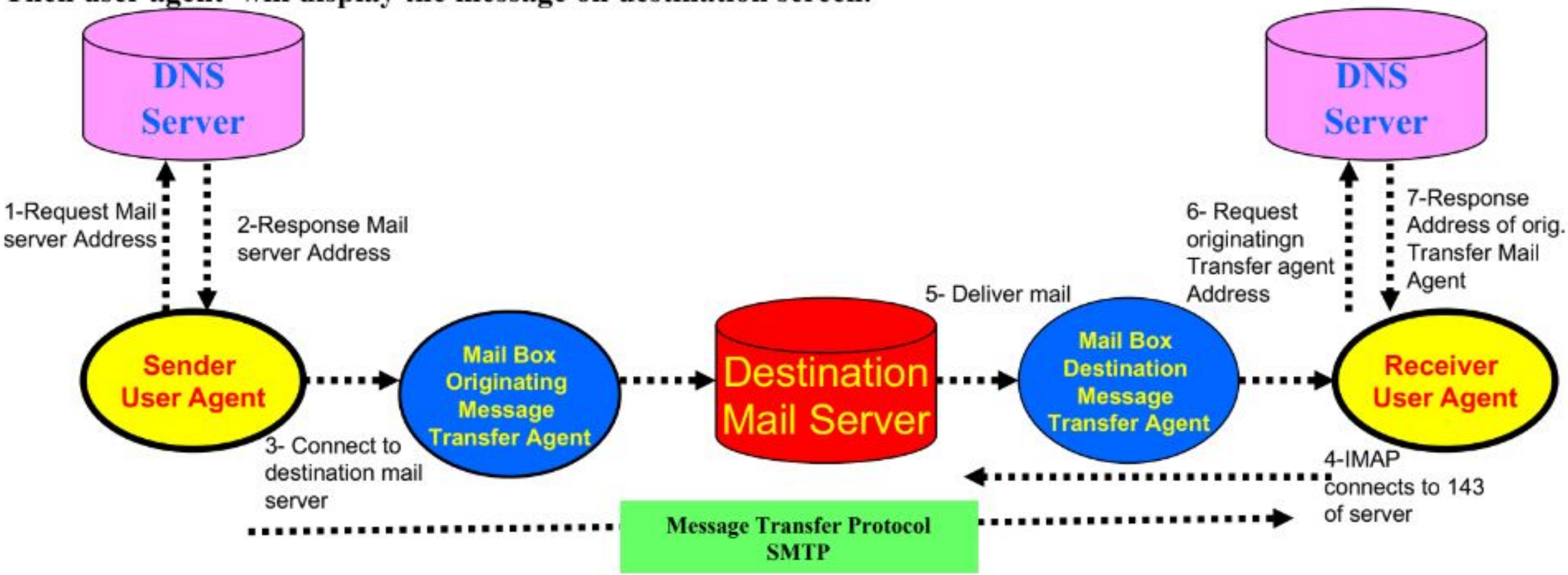
Email Message Transfer protocol SMTP (Simple Mail Transfer Protocol) RFC 5321

To connect to the right server the client will send DNS message with MX to get records of destination email server (The receiving).

Receiver user agent will request for origination transfer mail agent address from DNS, if is known the email will be accepted.

IMAP (Internet Message Access Protocol) server listens at port 143, the user agent at destination connects to this Port.

Then user agent will display the message on destination screen.



Applications

➢ Electronic Mail

❖ IMAP (Internet Message Access Protocol) RFC 3501

Used by mail server and user agent.

IMAP Commands:

Command	Function
STARTTLS	Start TLS
LOGIN	Log on to server
AUTHENTICATE	The method of authentication
SELECT	Select a folder
EXAMINE	Select read only folder
CREATE	Create a folder
DELETE	Delete a folder
RENAME	Rename a folder
STATUS	Get status of a folder
LIST	List available folders
APPEND	Add a message to folder
FETCH	Get a message from a folder
SEARCH	Search a message in folder
STORE	Change message flag
COPY	make a copy of message in a folder
EXPUNGE	Delete the messages with deletion flag
LOGOUT	Log out disconnect the connection

Applications

- **Electronic Mail**

- **Webmail**

- User agent provides services using web (Gmail, Microsoft, Yahoo) .
- Mail server uses for SMTP TCP port 25, user agent is UI (User Interface) that uses browser to access the email for reading or sending.
- After login procedure user can access the email on the email webpage.
- Server will find client mail box after login the content of mailboxes are accessible.
- User can read emails, delete, or move to other folders.
- For delivery web server uses SMTP.
- For interactive responsive interface the web page uses JavaScript, they run on client for response to local events such as mouse operations, send message to server in background.

Applications

➢ WWW (World Wide Web)

❖ URL operation Client:

Protocols http, https, ftp, file (local file), RTSP, SIP, about (plugins) are used.

The websites are written in HTML (Hyper Text Markup Language), browser interprets HTML.

Page navigations

→ **Forward**

← **Backward**

Browser uses MIME (Multipurpose Internet Mail Extension) to display the delivered content from server if browser does not know how to interpret the content.

Plugins: **They are executed and reside in local browser and provide codes such as pdf, Flash, Media Play, etc..**

The browsers have interfaces to communicate with plugins.

Note: Installing new plugin may overwrite the most recent plugin function.

Helpers: **They are programs running in separate process. It process the downloaded content file.**

They are browser's independent, vendors can create their own helpers with extensions vnd (vendor specific format).

Applications

➢ WWW (World Wide Web)

❖ URL operation Server:

- ❑ After client connects to TCP port 80, resolve name of the web page, check restriction for access, the server will retrieve the file from server or cache, verify MIME type, deliver the content, log file update, run timer to disconnect TCP connection.
- ❑ The last content will be cached on the server to provide fast access to the content for clients.
- ❑ One process can handle multiple threads.
- ❑ Client request is processed in process module to verify if cache is available, if not then will access for the content on the disk.

Cookies (RFC 2109):

- ❑ Identifies user and tracks user's activities, payments, shopping cart items, and personalized functions on a portal. They are saved at client's browser in directory format.
- ❑ IP address is not sufficient (IP add. Changes when using DHCP, using NAT all users same IP add.)
- ❑ The cookies are generated by server and will be sent to browser (client).
- ❑ They have originating Domain Name, path to server file tree, the character "/" means the whole tree, content has format name = value (any value assigned by server), Secure browser should use a secure protocol SSL/TLS, Expire time of cookies in date and time.
- ❑ When expire field is not present it is nonpersistent cookie, meaning browser discards the cookie, if expire field is present it is persistent cookie then browser keeps that for duration of expiration,

Applications

WWW (World Wide Web)

Cookies (RFC 2109):

- Advertisers can track the cookies to find out the user's navigation behavior (Google Analytics, DoubleClick).
- Spyware are cookies track user across multiple websites.
- Third party cookies are not from the main visited page, they are from different sites.

Static web pages:

Pages from server are transferred to client.

HTML (Hyper Text Markup Language):

- Provides formatting information for presentation of website.
- It separates content and presentation.
- The browser will understand the standard commands and will apply to content or reformat if required.

Using tags inside brackets <>

<head> begin of head

</head> end of head

<body> begin of body

</body> end of body

<a> begin of hyperlink

 end of hyperlink

Applications

- **WWW (World Wide Web)**

AJAX (Asynchronous JavaScript and XML):

Provides user interface and access to information on server asynchronously.

Consists of HTML, DOM (Document Object Model), XML, JavaScript.

- **DOM (Document Object Model):**

  It is a tree structure of HTML components.

  Is used to modify the HTML page only nodes need to be changed in tree will be replaced, the browser will display the result.

- **XML (eXentsible Markup Language):**

  Provides structured content. Web content could be structured better for search.

- **XSLT (eXtensible Stylesheet Language Transformation):**

  Will be used to transform XML into HTML.

- **XHTML (extensible HyperText Markup Language):**

  It is creating web pages strictly based on XML.

- **SOAP (Simple Object Access Protocol):**

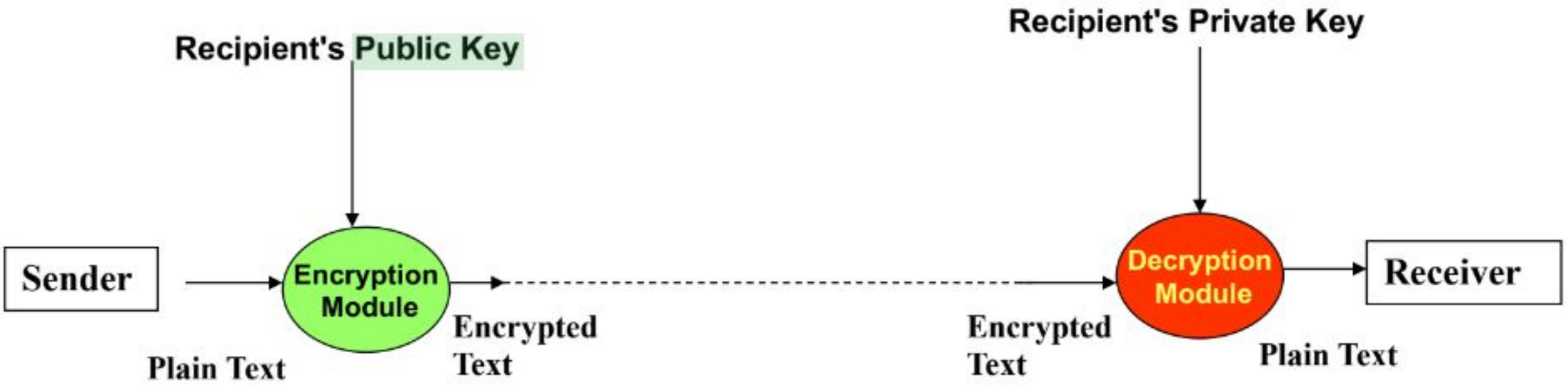
Is used for information exchange in the implementation of web services. It uses XML Information for communication between client and server. Its purpose is to provide neutrality and independence for exchange of information.

Security

- **Public Key**

- Different keys are used to encrypt and decrypt it is different than symmetric key
- Receiver uses a unique decryption key, known as private key.
- Receiver should publish its public key for encryption
- Requires third party to certify public key belongs to certain entity (person, company)

- Public and private keys are related algorithmically.



Security

- **Public Key**

Algorithms for Public key

- **RSA (Rivest, Shamir, Adelman MIT 1978):**

  Key Generation:

  Each peer needs to generate public and private key.

  Public key generation

  - Select two large prime numbers p and q
  - Calculate n = p X q (n not less than 526 bits)
  - Calculate number "e" the range 1<e<(p-1)(q-1)
  - No common factor between e and (p-1)(q-1)
  - The "e" and "n" will be made public
  - Advantage of RAS is the attacker can not have enough time to break the large key "n" for duration of communication.
  - **Public key (n , e)**

Security

- **Public Key**
  - **RSA (Rivest, Shamir, Adelman MIT 1978):**

    Key Generation:

    Private key generation

    The number "d" is private key and is the inverse of e modulo (p-1)(q-1)

    Private key is (n , d)

    Encryption:

    The plain text is multiplied with itself "e" times then reduced to modulo "n" the result is the cipher text.

    Decryption:

    The plain text is raised to power of "d" the result modulo n is plain text.

Security

➢ MD (Message Digest)

- Provides authentication does not encrypt the whole message.
- Using hash algorithm with variable input text length the output is fixed bit length text.
- It computes fast, very good encrypts, very strong packet integrity.

Example for public key usage:

- Originator calculates message digest of plain text
- Plain text and signed message digest are sent
- If en route the message is changed then receiver can verify that.

Security

- **Management of Public Keys**

- We use certificate for secure distribution of public keys.
- A centralized online server that give the public trusted keys of other parties will become the source of bottleneck or failure.
- (Certified Authority) is the organization that certifies public keys.
- Certificates binds the public key to a person or organization.
- An Authority issues these certificates to users who asked for.
- The receiver of certificate can send it to certification site or a process, the site or process will send after encryption with public key and a random number to user, if the user can decrypt and send back, this shows the certificate is valid.
- For every session a new random number can be used.
- Note: Certificate can contain object, attribute (citizenship, age)

Security

- **Management of Public Keys**

- **X.509**

It is the standard for certificates, is not required to communicate with

CA (Certificate Authority), it uses encoding ASN.1 (Abstract Syntax Notation 1)

Format:

/C=Country/O=Organization/OU= Organization Unit/CN= Common Name

Security

➢ Management of Public Keys

❖ X.509

X.509 Certificate's format

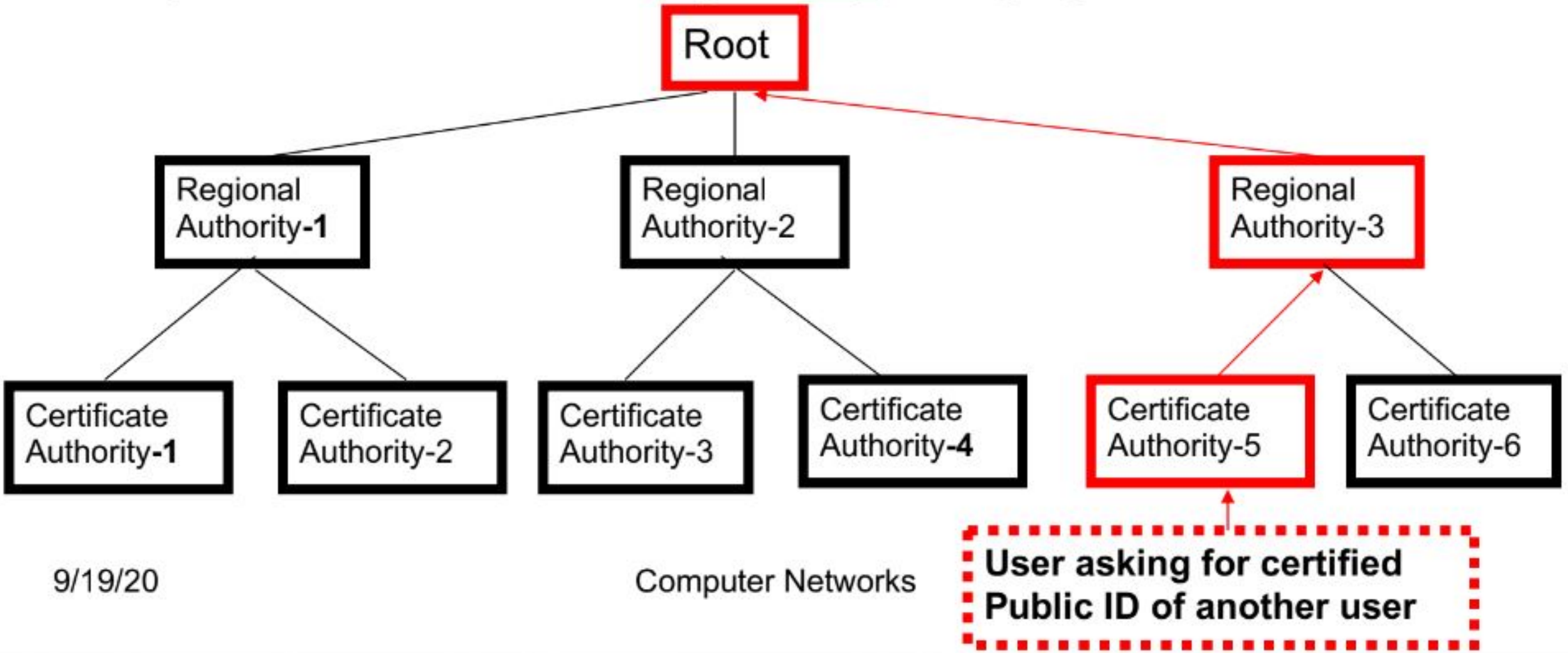
Standard information in an X.509 certificate includes:

- **Version** – which X.509 version applies to the certificate
- **Serial number** – the identity creating the certificate must assign it a serial number that distinguishes it from other certificates
- **Algorithm information** – the algorithm used by the issuer to sign the certificate
- **Issuer distinguished name** – the name of the entity issuing the certificate (usually a certificate authority)
- **Validity period of the certificate** – start/end date and time
- **Subject distinguished name** – the name of the identity the certificate is issued to
- **Subject public key information** – the public key associated with the identity
- **Extensions**-optional

- **Management of Public Keys**
  - **Public Key Infrastructure**

We need Public Key of a user to communicate with that user, need to get certificate which contains that.

- **Certificate Authority** certificate should be approved by **Regional Authority** and the **Root** should approve **Regional Authority** certificate.
- User we want to connect to will provide the **Certificate Authority** and **Regional Authority** certificates, we use the **Root's** public key to verify top level certificate.



Management of Public Keys

Public Key Infrastructure

- Chain of trust or certification path are the requests sent to Root.
- There are many Roots which can provide the high level authority to users, the browsers will provide public keys of 100 Roots called trusted anchors.
- There is no need for a central worldwide Root.

Directories:

Where are certificates stored?

1. **DNS can provide the certificates at the time provides the IP-Addresses.**
2. **X.509 directory server can provide certificates using X.500 naming.**

Management of Public Keys

Public Key Infrastructure

Revocation:

- The certificates can be revoked (not paid payments, the validation time expired)
- **Certification revocation list** contains revoked certificates.
- Reinstated if payment has been paid, a new can be issued if time was expired.
- Could be placed on directories, else in some other nodes will be stored.
- A master list will be maintained and infrequently will be sent to proper nodes.

Security

Symmetric Key

Definition: The same key is used for encryption and decryption.

Block Cipher: convert the n bits of plaintext into n bits of ciphered text in HW or Software.

The conversion could be in form of substitution or transposition

Substitution:

- **S-Box (**Substitution Box): Converts **n** input bits to m output bits (m=n or n !=m)
- **P-Box (**Permutation Box)

Transposition:

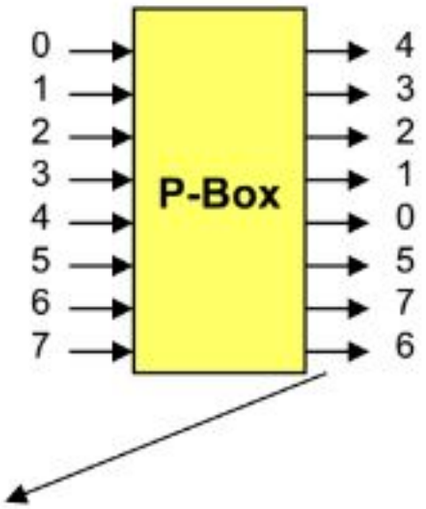
Using bit shuffling over S-Box inputs.

Security

Symmetric Key

Phase I

Permutation of input bits

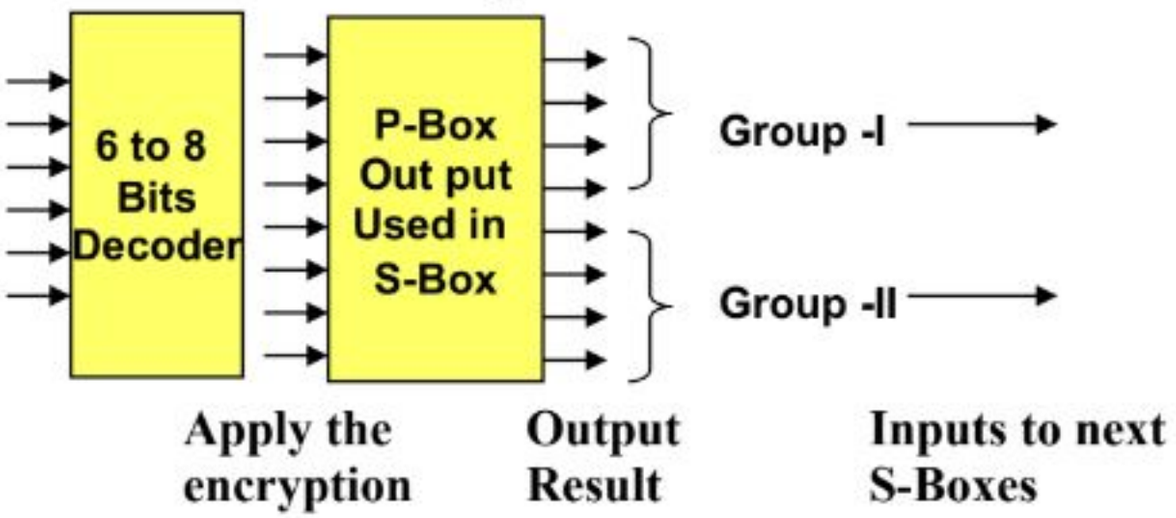


Phase II

The 6 bits decoder will select one of 8 bits and modify.

Most implementations are

64 or 256 inputs



Security

- **Symmetric Key**

- **DES (Data Encryption Standard)**

Developed by IBM.

Algorithm:

IP (Initial Phase) Permutation

The 64 bit block is divided in two 32 bits blocks and processed alternately (Feistel Function).

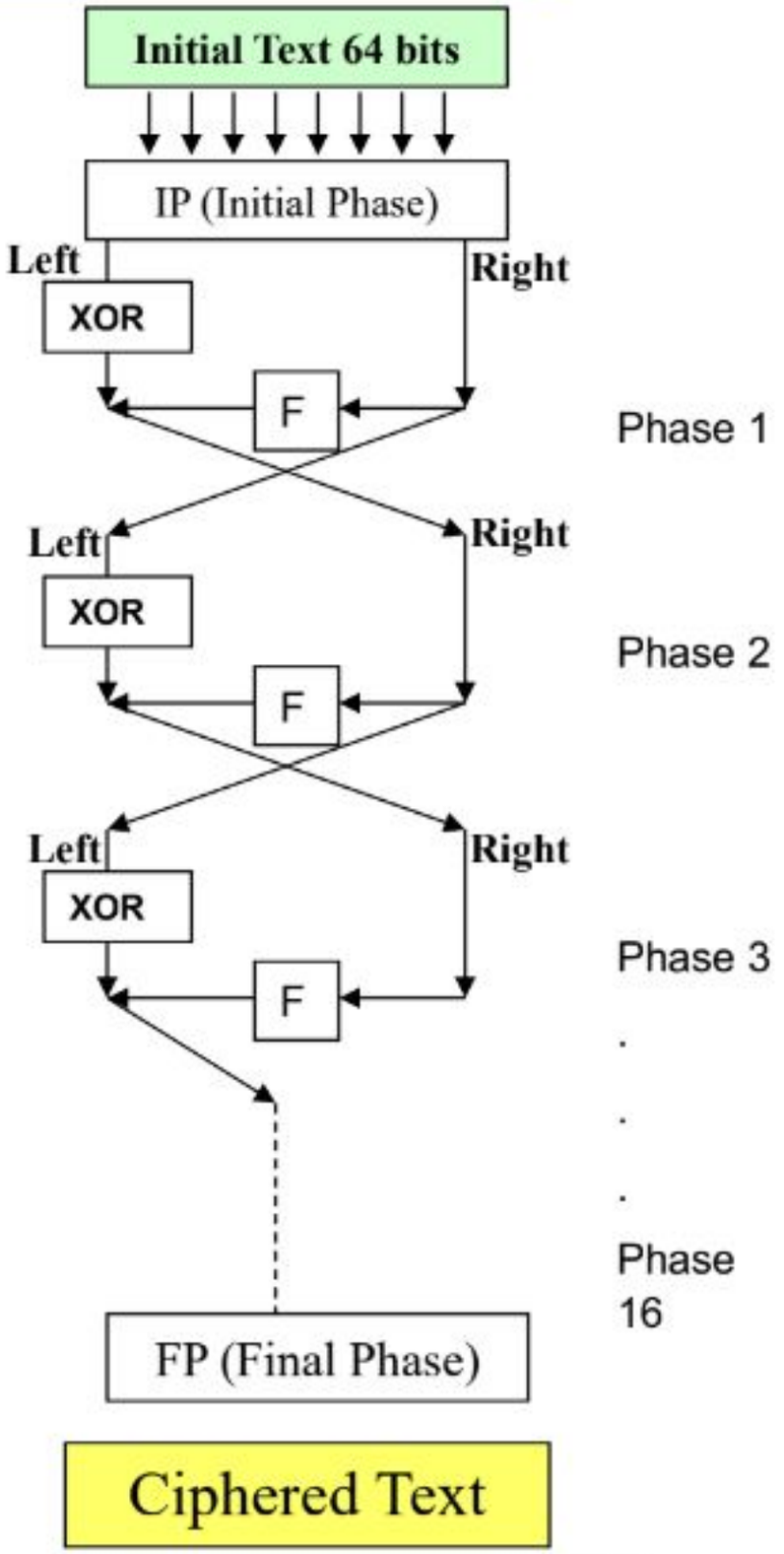
Function "F" scrambles half a block together with some of the Key.

The out put of "F" is then merged with other half of the block.

Before the next round the 32 bits halves are swapped

⊕

FP (Final Phase) Permutation



Security

- **Symmetric Key**
- **Cipher Mode**

Mono-alphabetic substitution, when same plaintext in same encrypted text out. Easy to break the key.

- **Electronic Code Book mode:**

Plaintext → Cipher text (old code books: Words → Digits)

AES and triple DES

Plain text divided in 8 Bytes blocks and encrypted in order with one key.

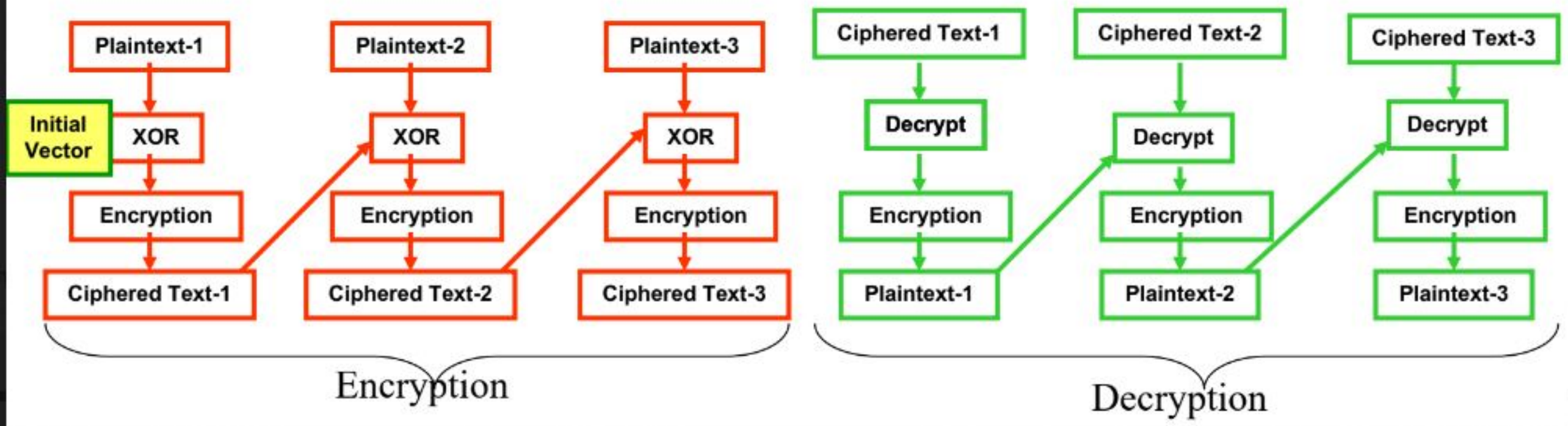
If requires leftover Byte will be padded to 64 bits.

- **Cipher Block Chaining Mode:**

Cipher Block Chaining prevents the replacement of blocks in ciphered text.

For example in 0-15 blocks ciphering with out cipher block chain we can replace blocks without detection.

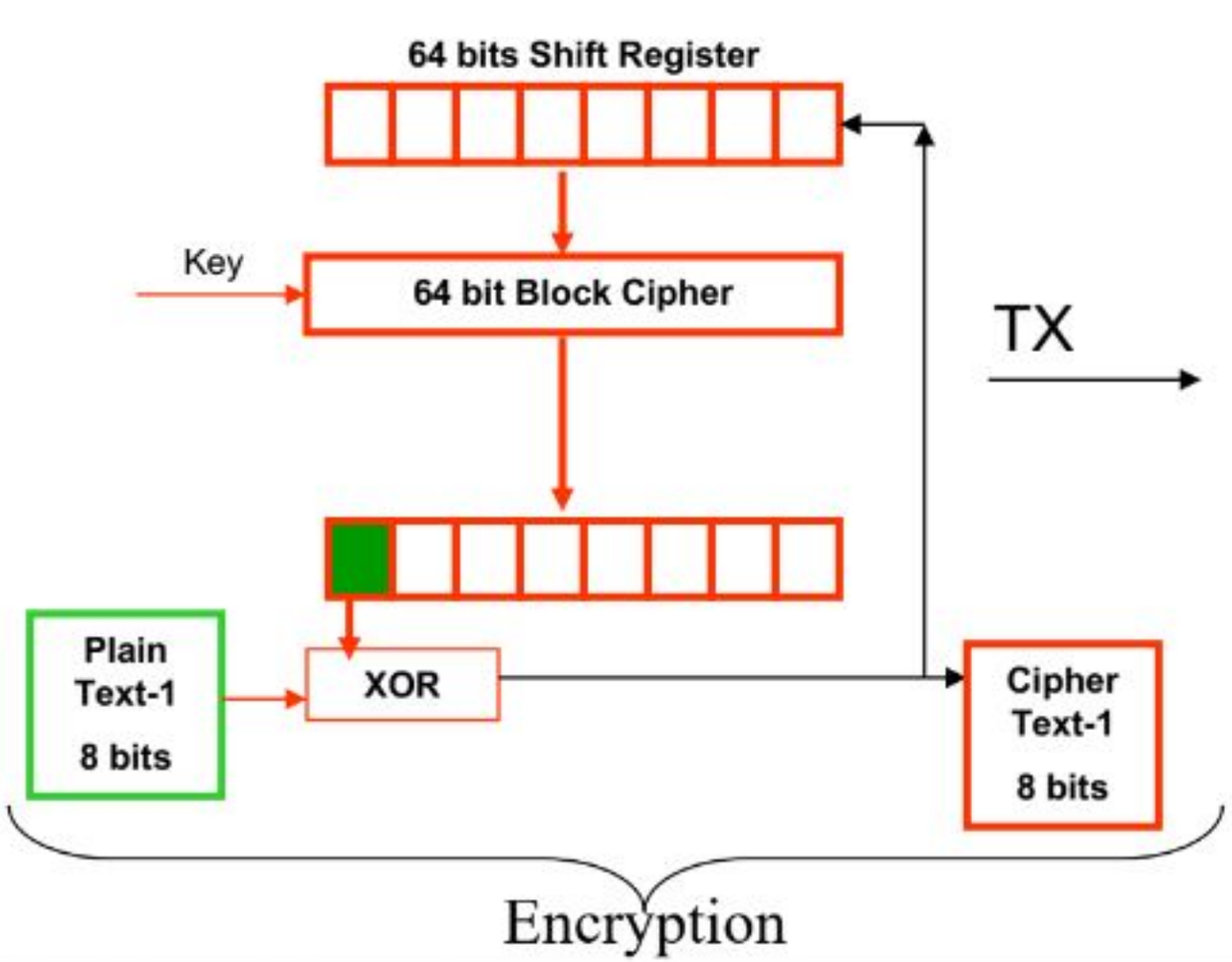
Each plain text will be XOR with previous cipher block prior to encryption. The first block is XORed with Initial Vector (Randomly generated). cipher- Text-1 and IV (clear text) are sent.

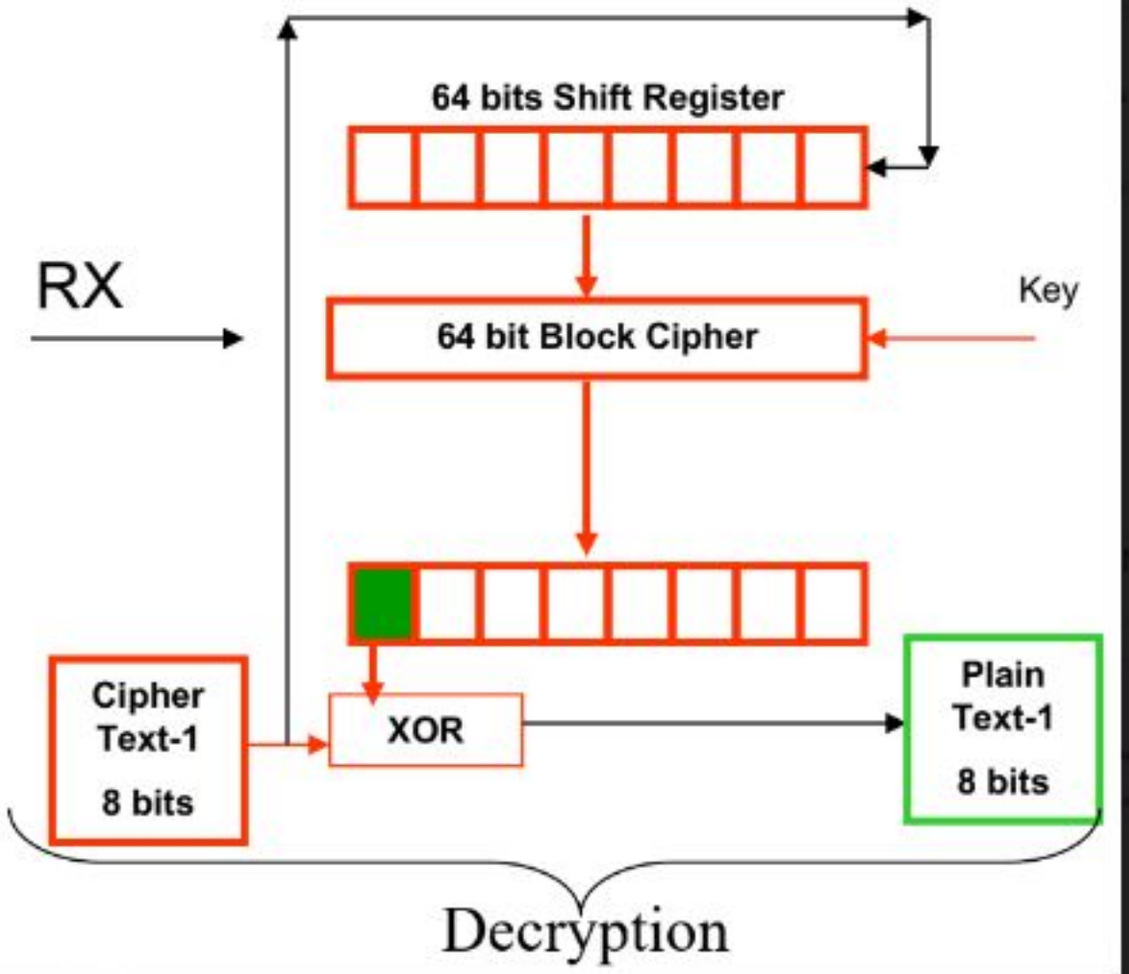


- **Symmetric Key**
- **Cipher Feedback Mode**

The data is ciphered in the smaller units than block size.
This method could be used to cipher one bit or one Byte before transmission.

- The 64 bits shift register is loaded with IV (initial Vector, for each transmitted message has different value, no need to keep secret), encryption algorithm is run once to generate 64 bits output.
- The most left bits of the register are XORed with Byte to be transmitted, the result is transmitted as well this value will be forwarded to 64 bits shift register.
- The most left 8 bits are shifted and then the process starts again.





Security

- **Symmetric Key**

- **Stream Cipher Mode**

- It is used to encrypt text using cipher key, algorithm to apply on each bit.
- Encrypts the entire plaintext, the encryption of any plaintext bit in the block depends on the other plain text bits of same block.
- They are fast for applications with limited resources (Cell phones)
- The block is 128 bits or 64 bits long.

Adding a bit from key stream to a plaintext, there are two types:

1. **Synchronous stream cipher:** Key stream depends only on key (Mostly used)
2. **Asynchronous stream cipher:** Key stream depends as well on the cipher text.

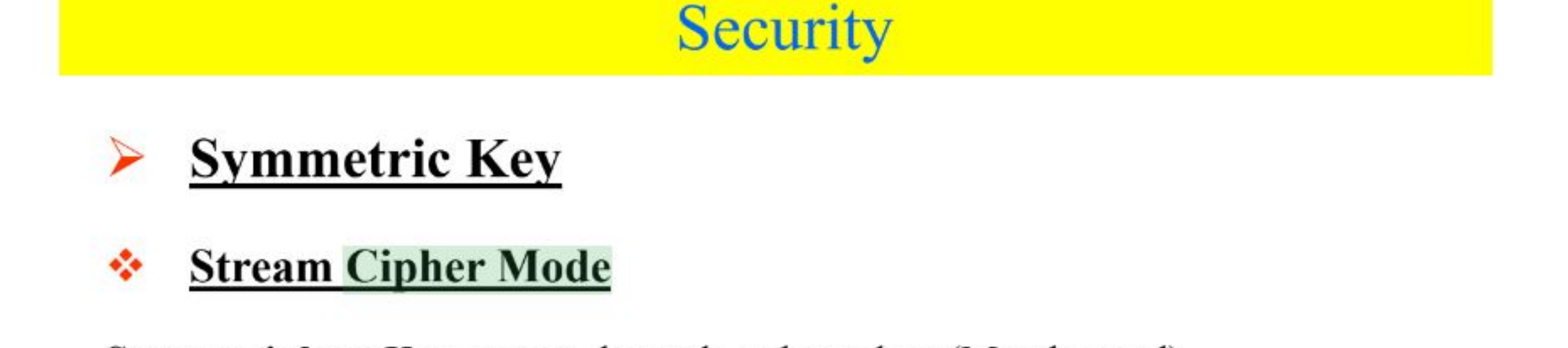
Security

- **Symmetric Key**

- **Stream Cipher Mode**

Stream cipher: Key stream depends only on key (Mostly used)

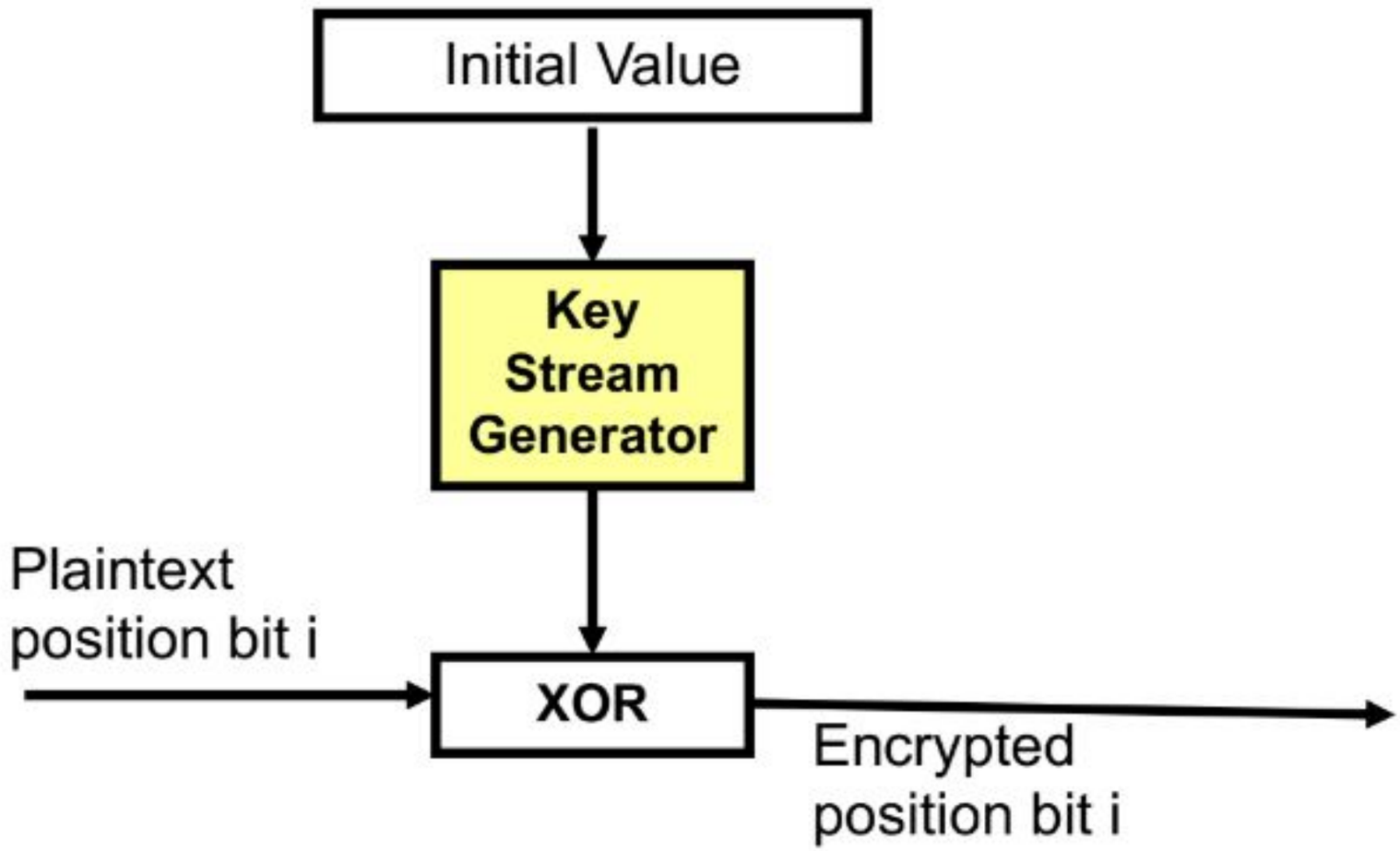
To encrypt, the bit "i" is added to the key in position "i" (Modulo 2)



Security

- **Symmetric Key**
- **Stream Cipher Mode**

1. **Synchronous stream ciphers:**



Security

- **Symmetric Key**
- **Stream Cipher Mode**

2. **Asynchronous ciphers:**