# COMPUTER NETWORKS AND INTERNET PROTOCOLS

## Layer 1: Physical Layer



**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

# OSI Model Layers

| OSI layer | Function provided |
|---|---|
| Application | Network applications such as file transfer and terminal emulation |
| Presentation | Data formatting and encryption |
| Session | Establishment and maintenance of sessions |
| Transport | Provision for end-to-end reliable and unreliable delivery |
| Network | Delivery of packets of information, which includes routing |
| Data Link | Transfer of units of information, framing, and error checking |
| Physical | Transmission of binary data through a medium |



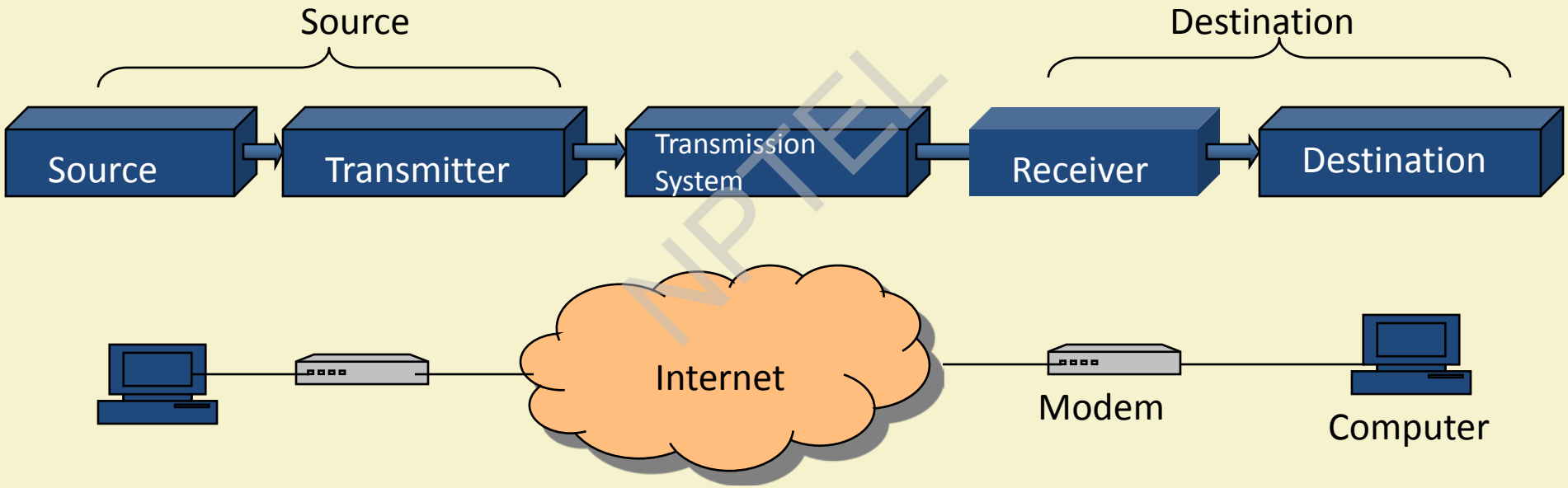
*Ref: Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com;* Worcester Polytechnic Institute (WPI), Worcester, MA, USA

# Network Communication

**Data Communications:** Transmission of signals in a reliable and effective manner. Topics covered include signal transmission, transmission media, signal encoding, interfacing, multiplexing etc.

**Networking:** Technology, architecture and protocol of the communication networks used to interconnect communicating devices (entities). Topics include LANs, WANs, network protocols, applications etc.

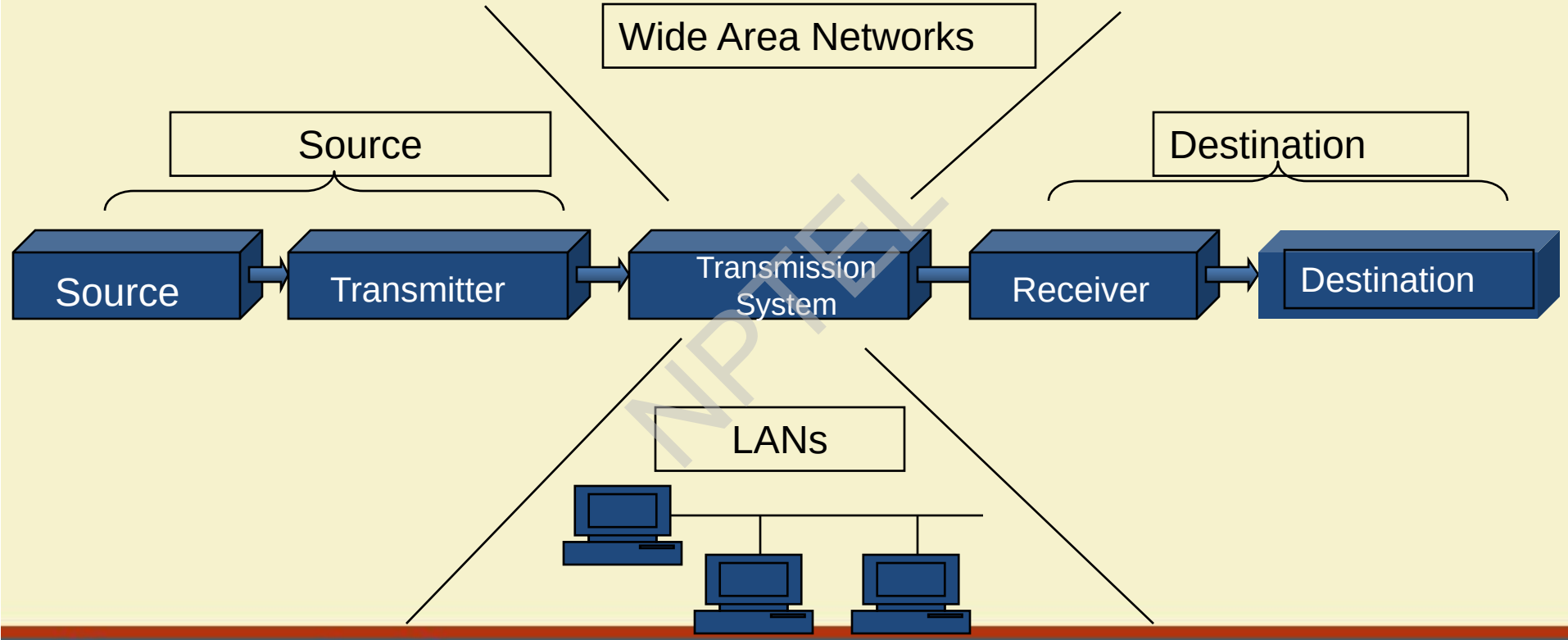
# Communication Model



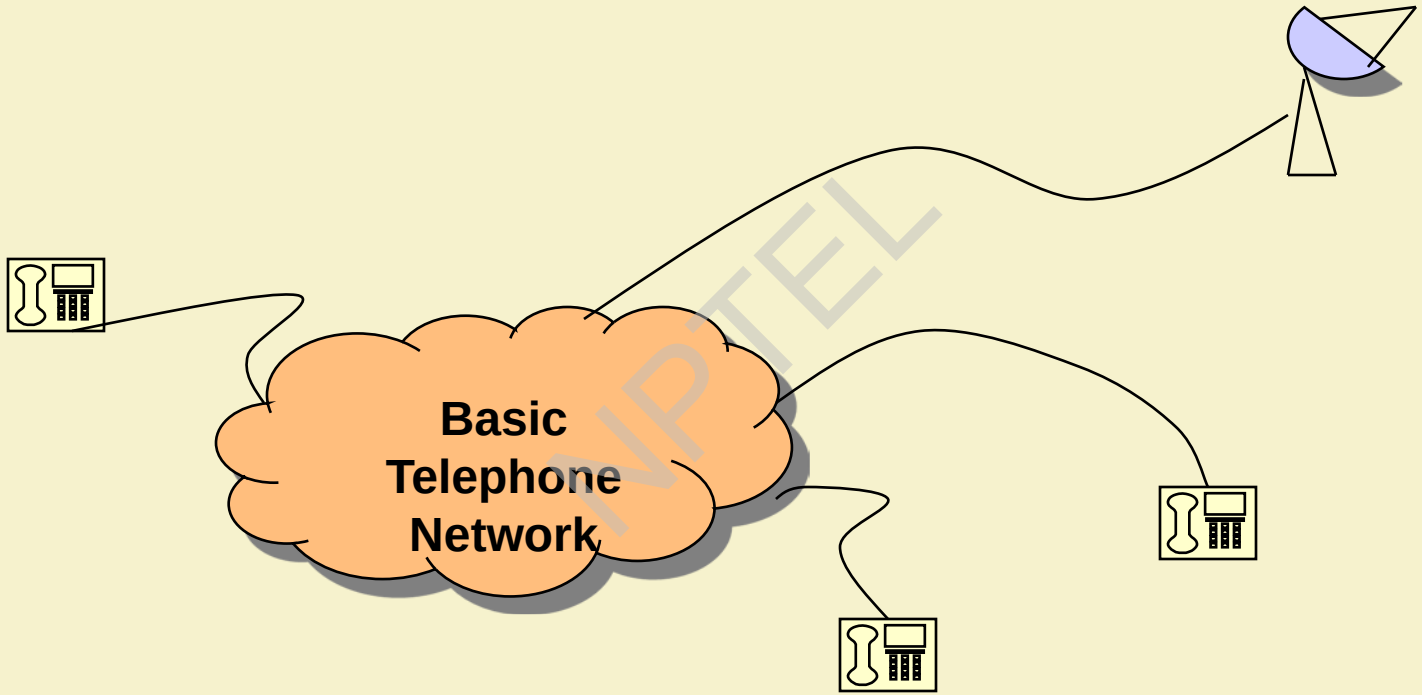
# Communication Tasks

- Transmission System Utilization
- Interfacing
- Signal Generation
- Synchronization
- Exchange Management
- Error detection and correction
- Addressing and routing
- Recovery
- Message formatting
- Security
- Network Management

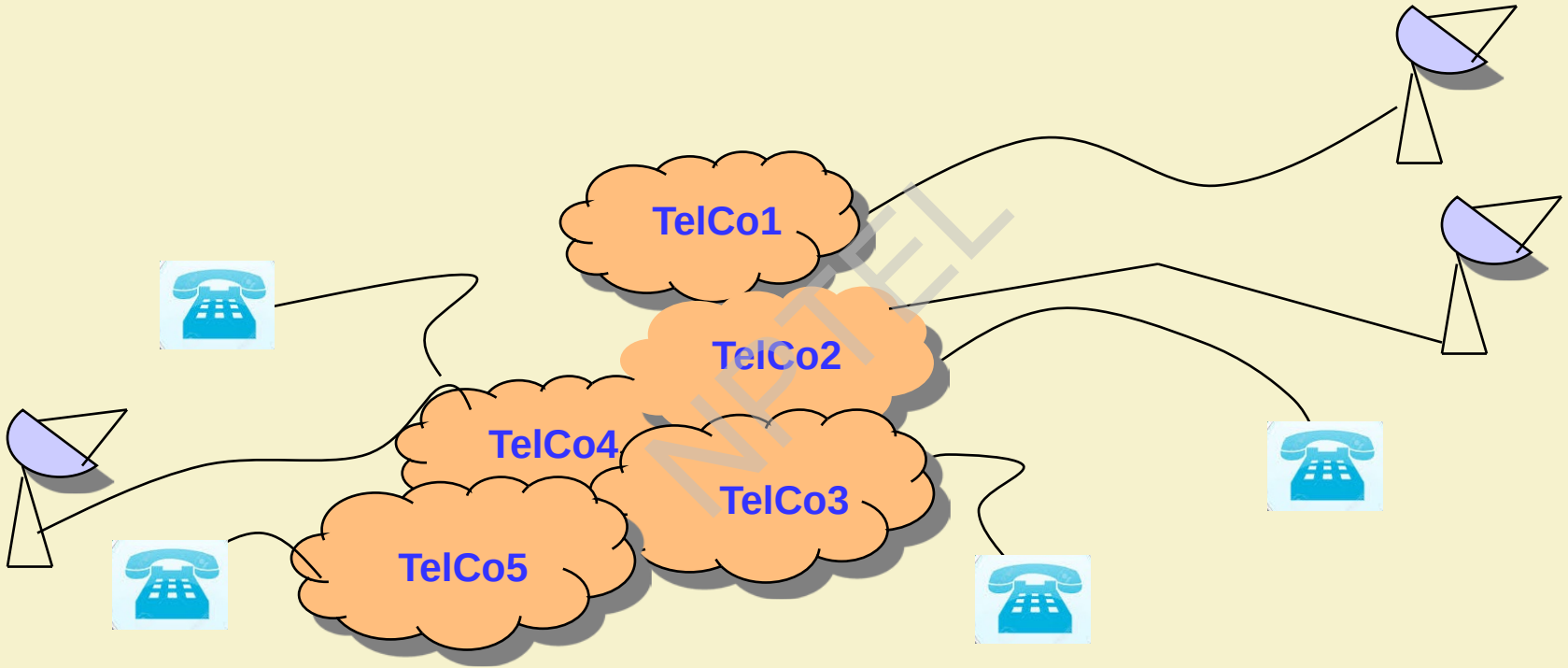
# Networks



# Telephone Networks



# Telephone Networks



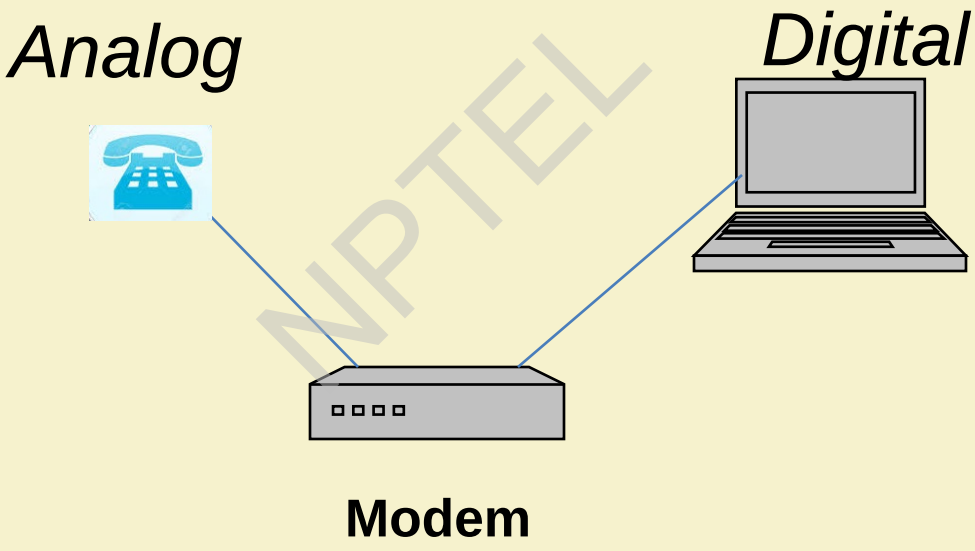
# Analog and Digital Signals

- Analog Transmission
  - Wires or wireless, Audio tones Info conveyed through signal amplitude, frequency, and phase
- Digital Transmission
  - 1's and 0's

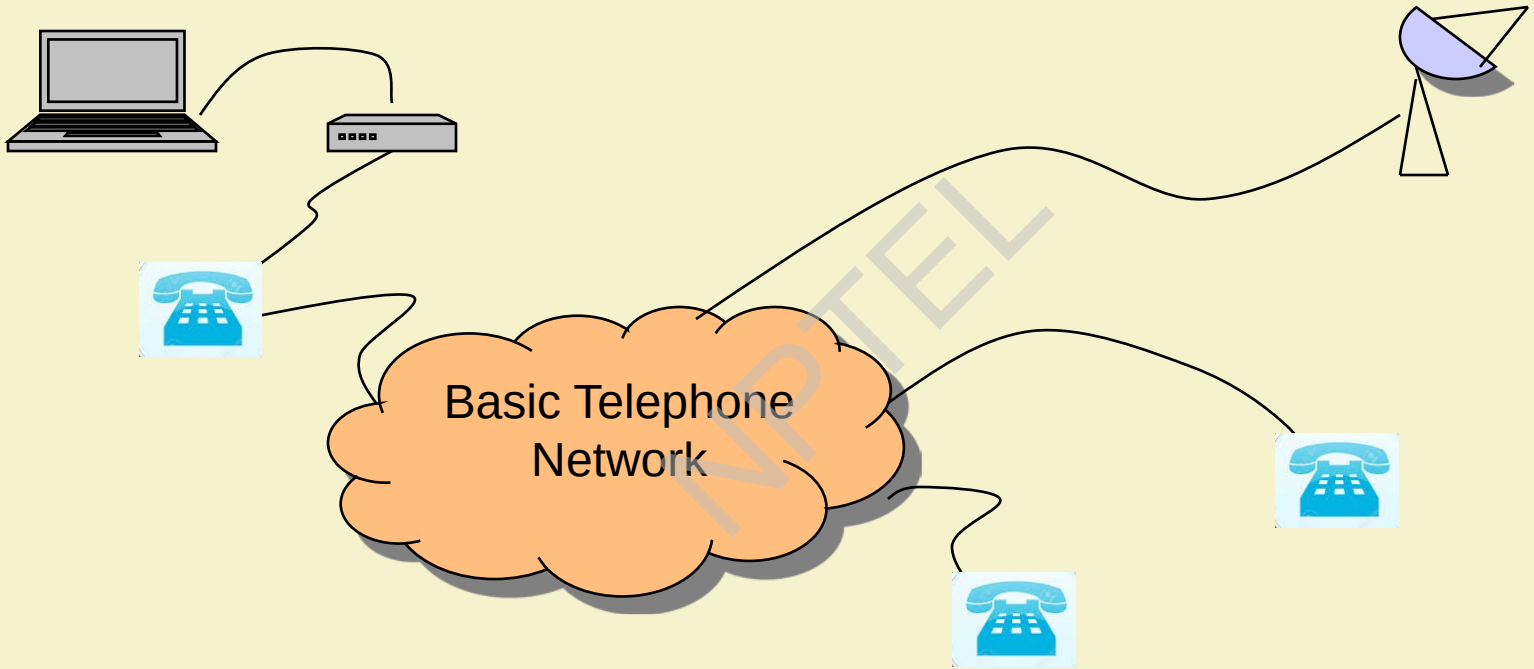


MODEM – MOdulator and DEModulator

# Analog ⟷ Digital

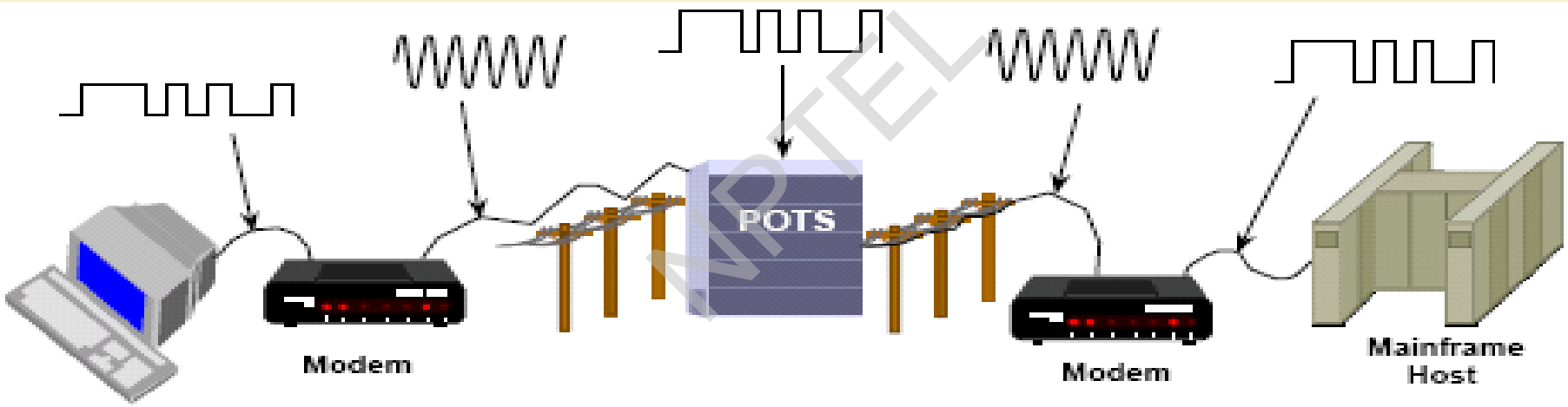


# Communication through Telephone Network



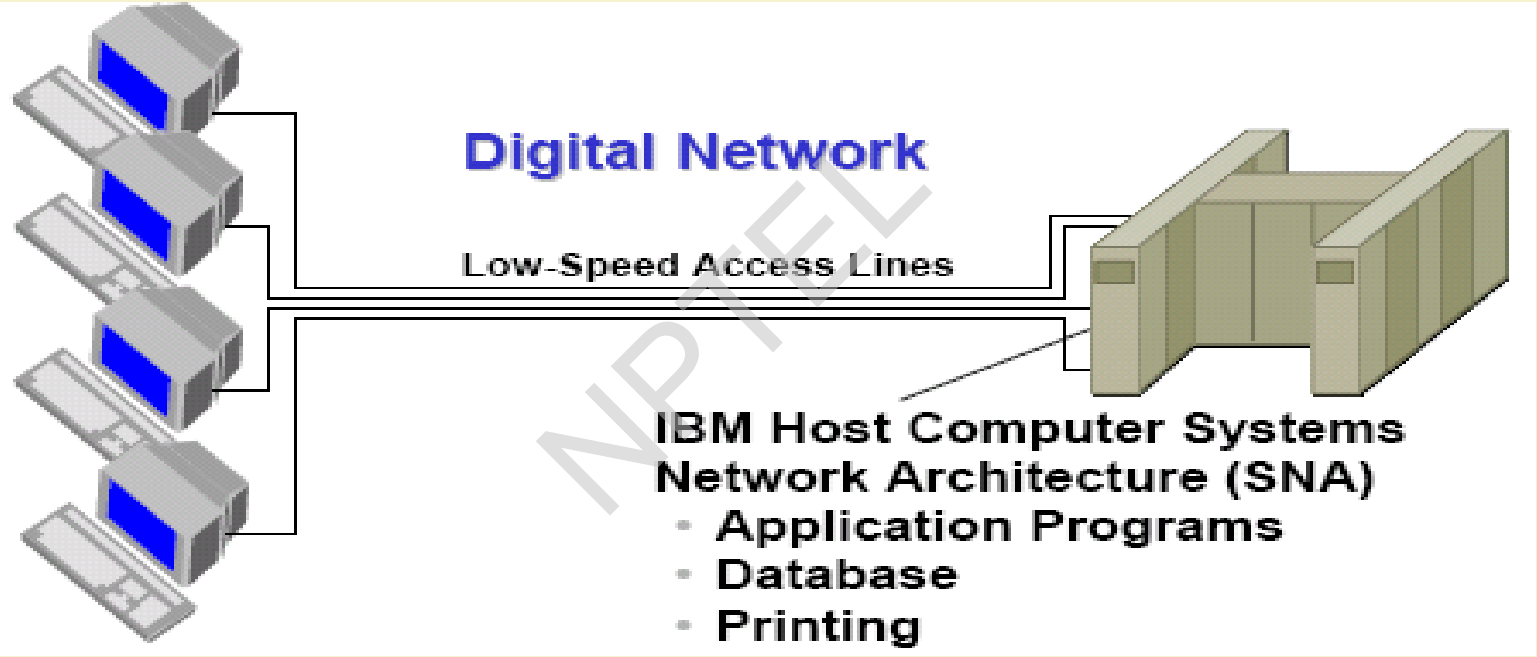
# Modem

- Modem translates digital computer signals to analog signals which the telephone world can understand and vice versa

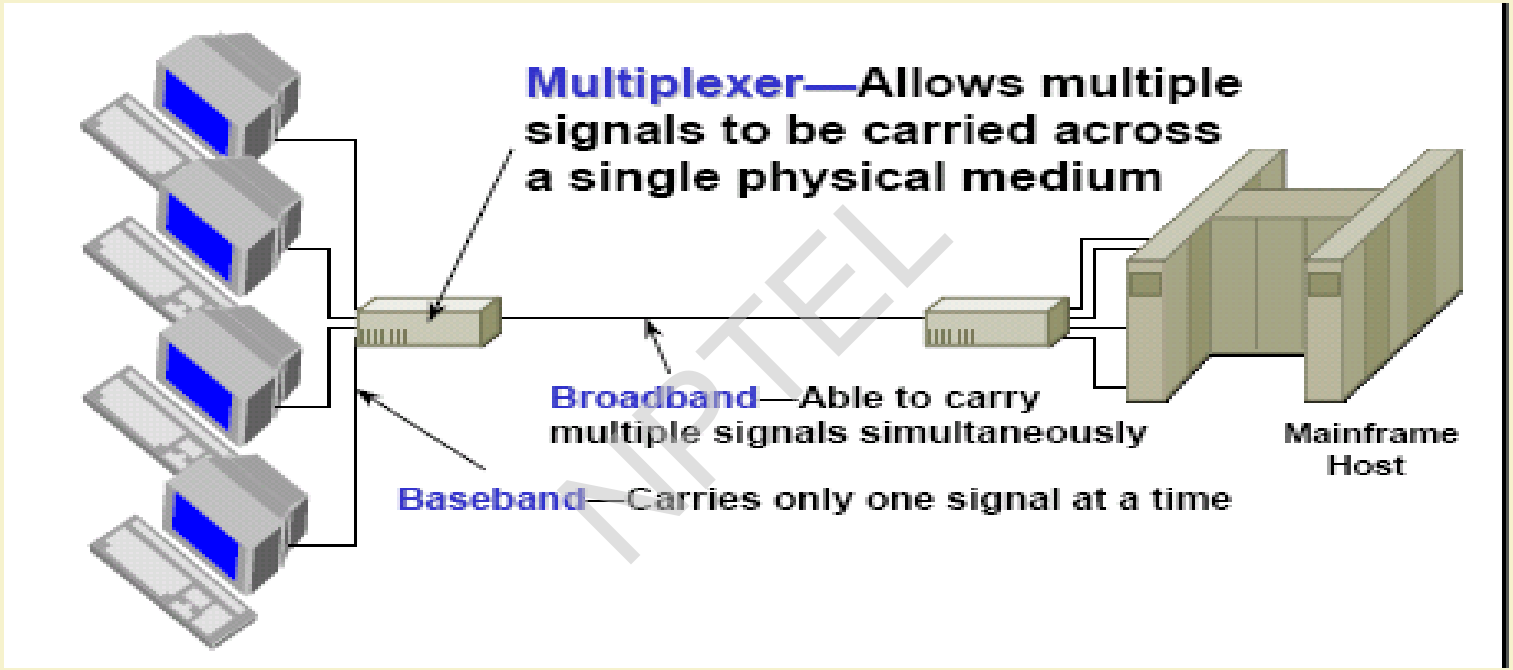



POTS (Plain Old Telephone Service)

# Connecting Multiple Systems



# Multiplexing



# Baseband vs Broadband

**Baseband** [Local Area Network]

Baseband transmissions typically use digital signaling over a single wire; the transmissions themselves take the form of either electrical pulses or light. The digital signal used in baseband transmission occupies the entire bandwidth of the network media to transmit a single data signal. Baseband communication is bidirectional, allowing computers to both send and receive data using a single cable. However, the sending and receiving cannot occur on the same wire at the same time.

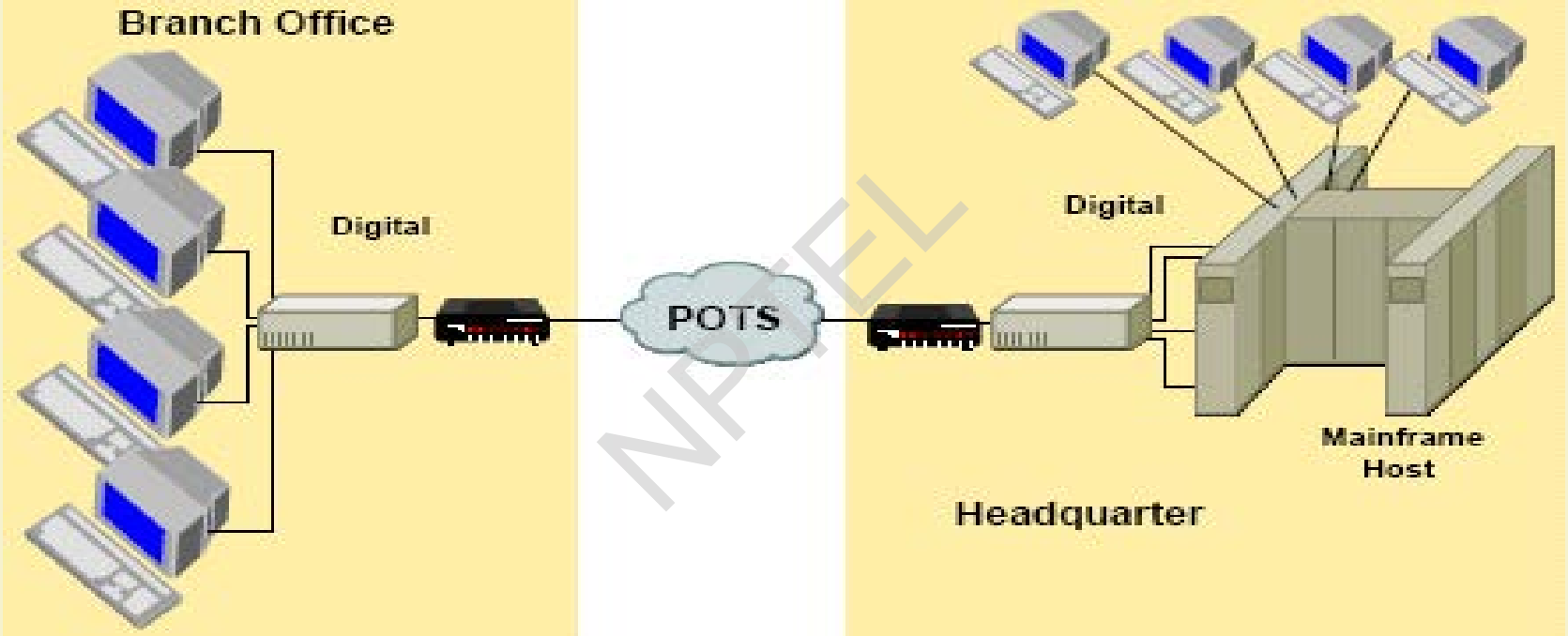
Using baseband transmissions, it is possible to transmit multiple signals on a single cable by using *multiplexing*. Baseband typically uses Time-Division Multiplexing (TDM),

**Broadband** [Wide area Network]

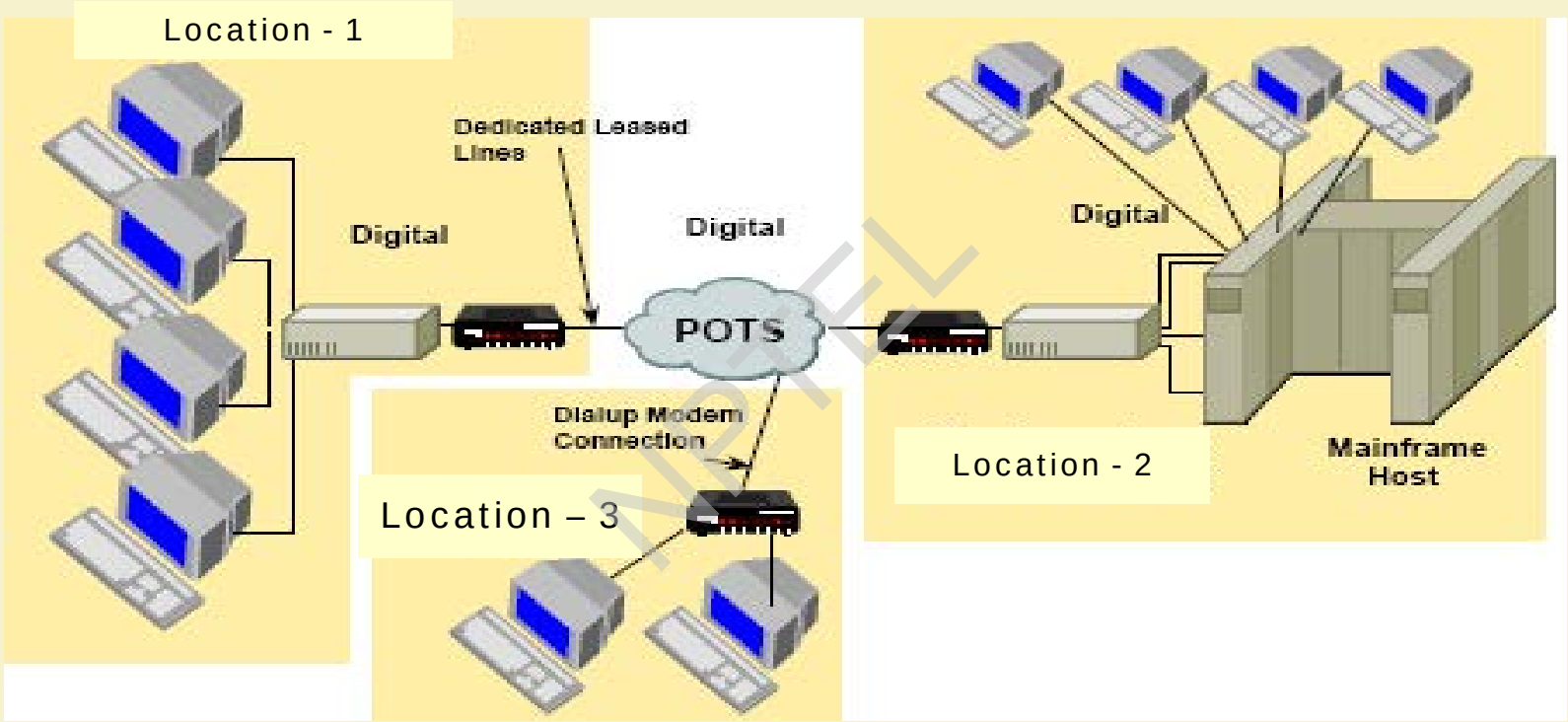
Broadband uses analog signals in the form of optical or electromagnetic waves over multiple transmission frequencies. For signals to be both sent and received, the transmission media must be split into two channels. Alternatively, two cables can be used: one to send and one to receive transmissions.

Multiple channels are created in a broadband system by using a multiplexing technique known as Frequency-Division Multiplexing (FDM).

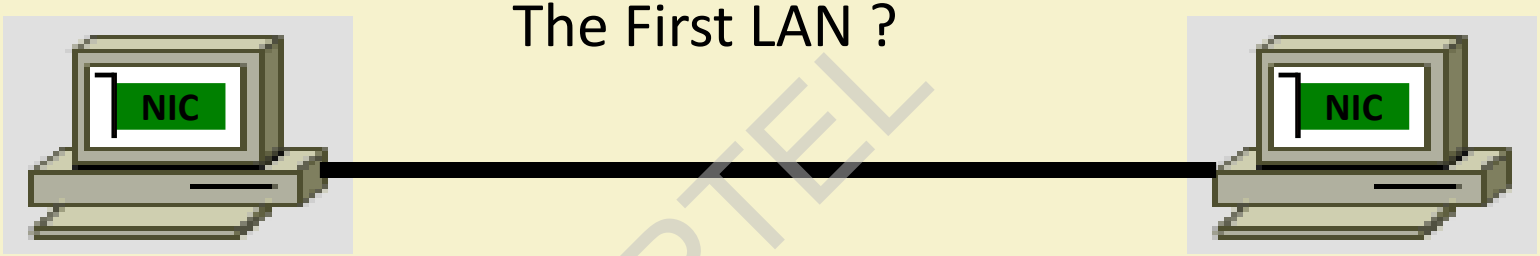
# Early Communication



# Communicating with Multiple Locations



# NICs, Repeaters, & Hubs






To connect two computers, you must...

- Install a NIC card in each.

➢ *Attach computers using a crossover cable*

# NICs, Repeaters, & Hubs

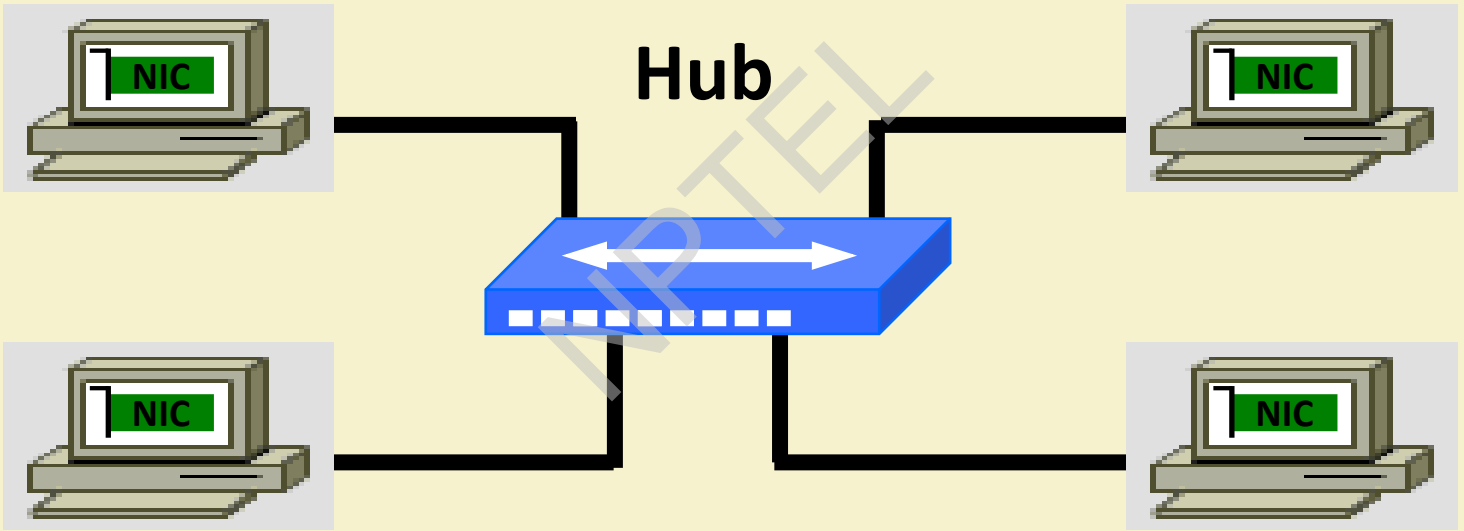
Repeaters can be used to increase the distance


100 meters or approx. 300 feet

*Repeaters regenerate signals*

# NICs, Repeaters, & Hubs

A multi-port repeater!



thank you!

# COMPUTER NETWORKS AND INTERNET PROTOCOLS

## Layer 1: Physical Layer-II

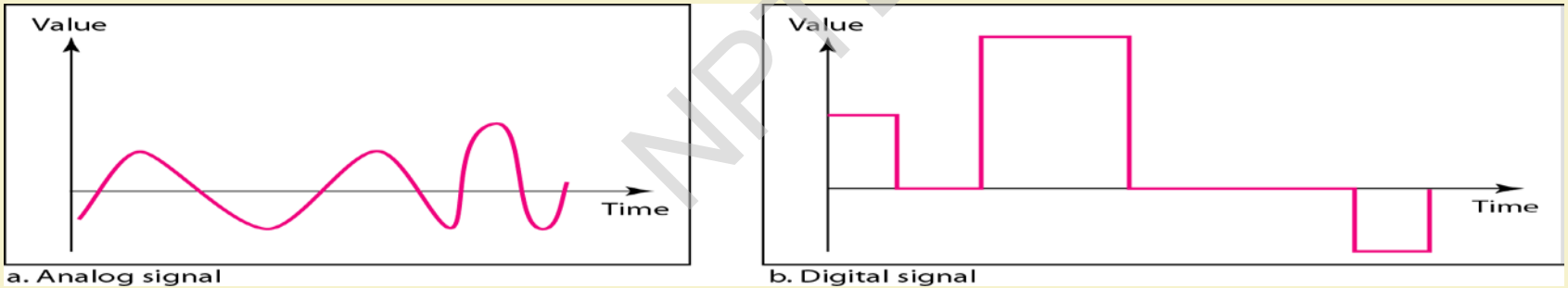


**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

# Data and Signals: Analog and Digital

- Data can be analog or digital.
- Analog data are continuous and take continuous values.
- Digital data have discrete states and take discrete values.
- To be transmitted, data must be transformed to electromagnetic signals.
- Data can be analog or digital.
- Signals can be analog or digital.
- Analog signals can have an infinite number of values in a range; digital signals can have a limited number of values.
- In data communications, we commonly use periodic analog signals and non-periodic digital signals.



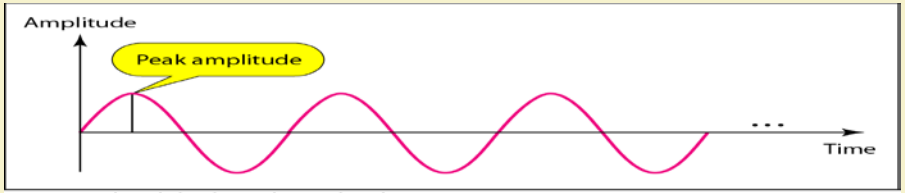

a. Analog signal

b. Digital signal

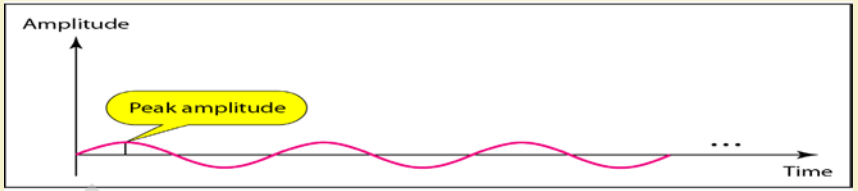


*Ref: Data and Computer Communications, W. Stallings; Computer Networks and Internets by Douglas E. Comer; Data Communications and Networking, B.A. Forouzan; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com*

## Signals with the same phase and frequency, but different amplitudes



a. A signal with high peak amplitude

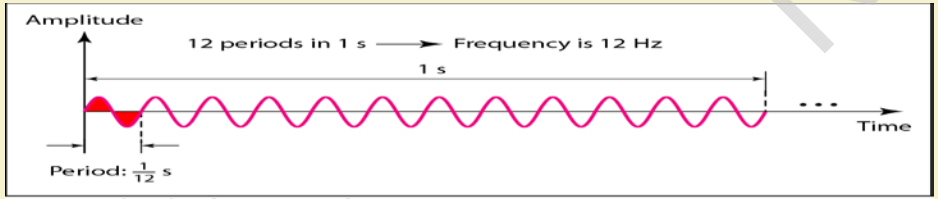


b. A signal with low peak amplitude

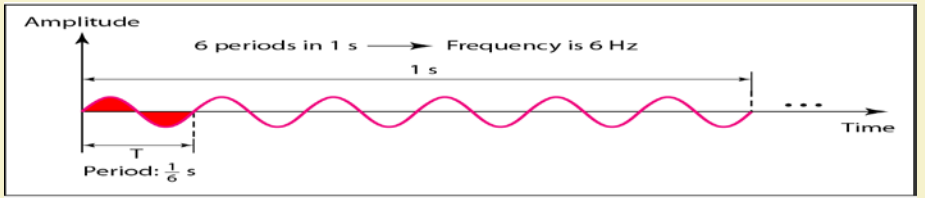
*Frequency and period are the inverse of each other.*

$$f = \frac{1}{T} \qquad \text{and} \qquad T = \frac{1}{f}$$

Signals with the same amplitude and phase, but different frequencies

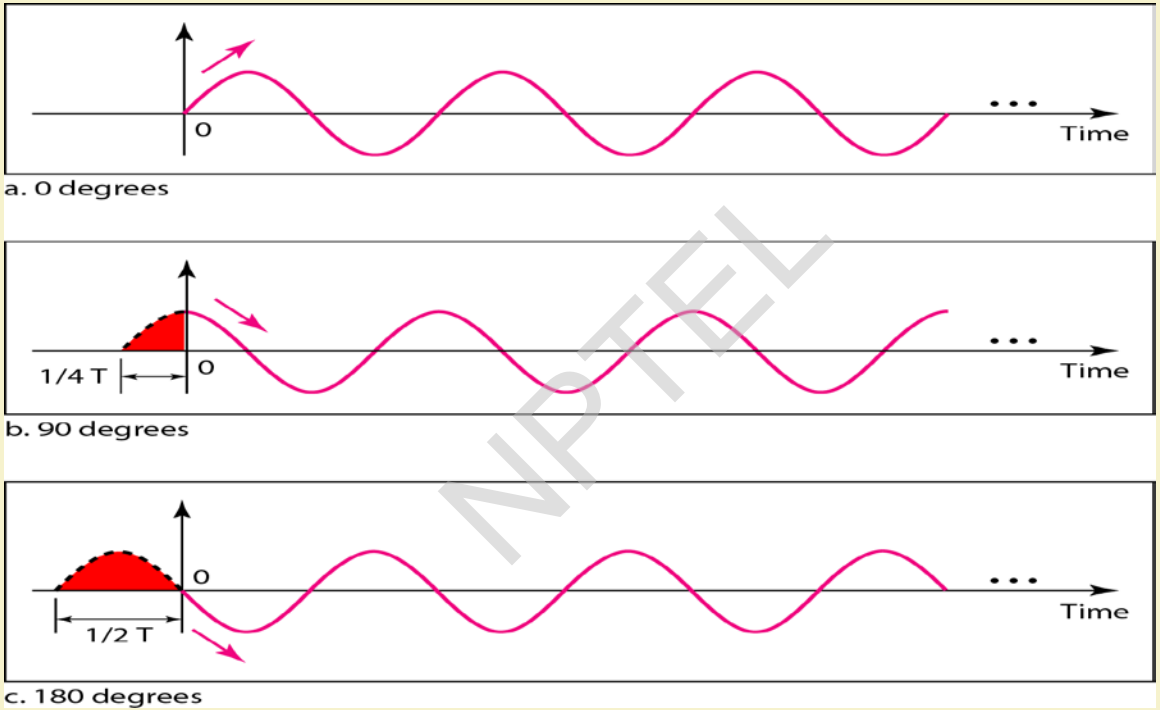


a. A signal with a frequency of 12 Hz

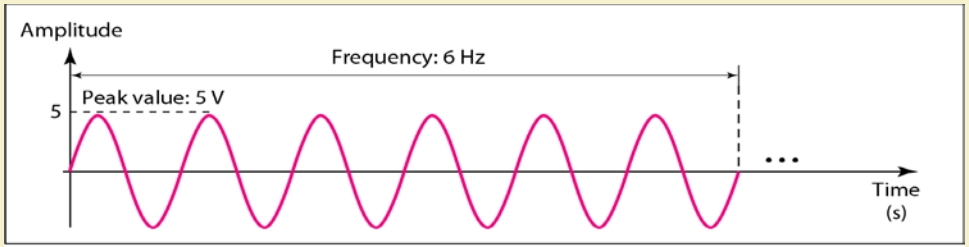


b. A signal with a frequency of 6 Hz

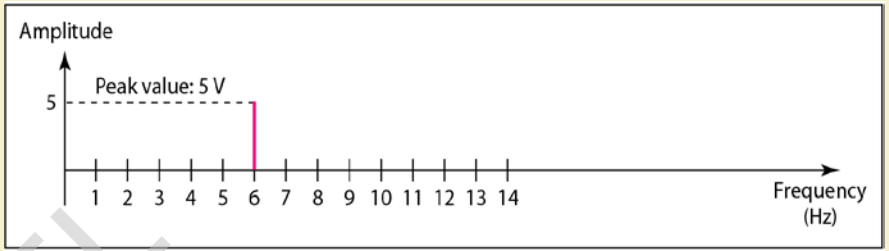
# Sine waves with the same amplitude and frequency, but different phases



## Time-domain and frequency-domain plots of a sine wave

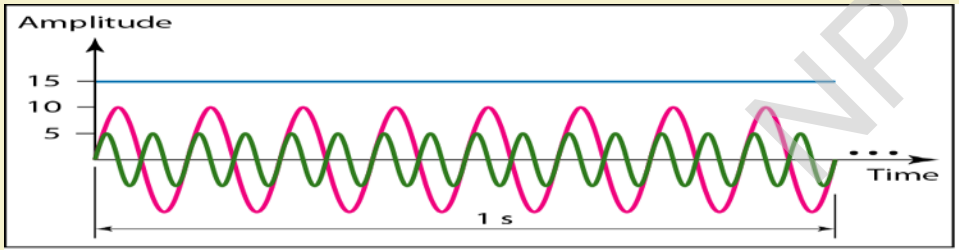



a. A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)

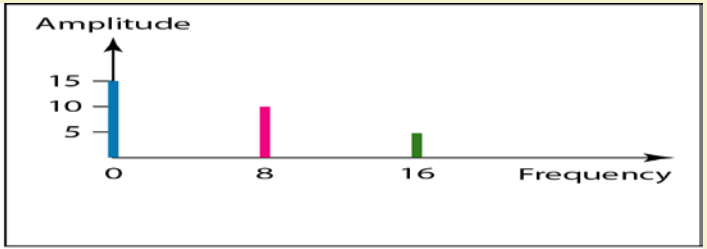



b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

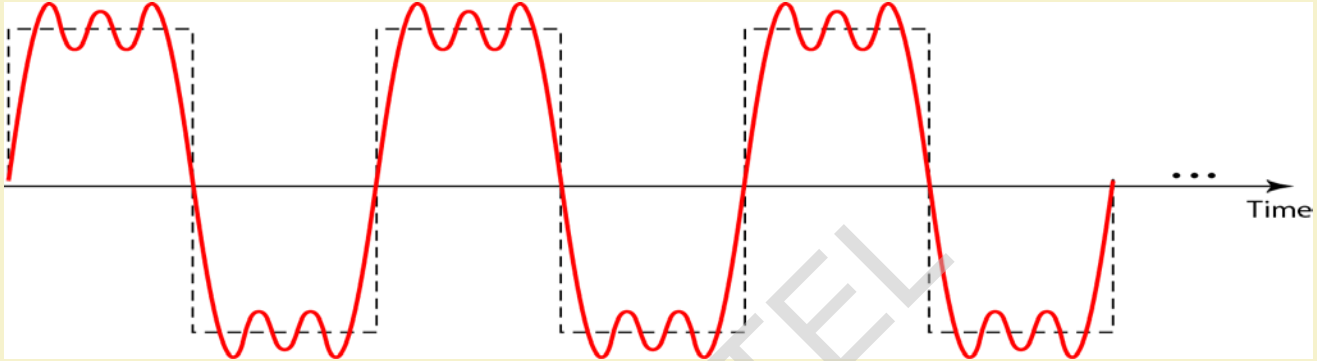
## Time domain and frequency domain of three sine waves




a. Time-domain representation of three sine waves with frequencies 0, 8, and 16

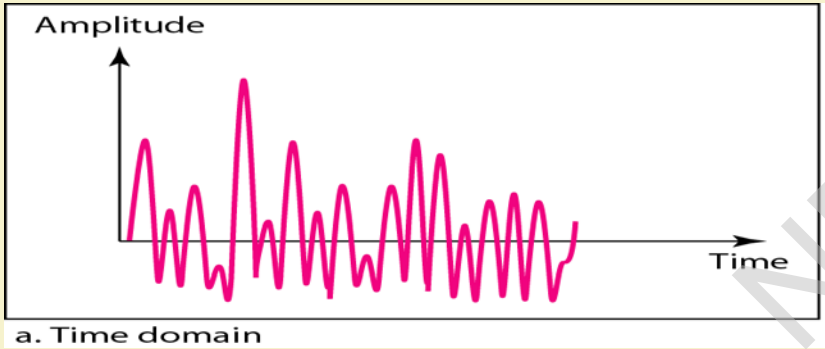



b. Frequency-domain representation of the same three signals

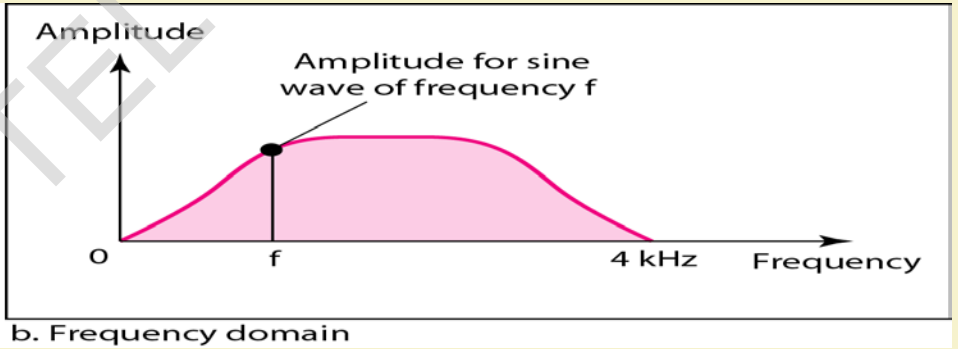



Composite Periodic Signal

Nonperiodic composite signal. It can be the signal created by a microphone or a telephone set when a word or two is pronounced. In this case, the composite signal cannot be periodic, because that implies that we are repeating the same word or words with exactly the same tone.



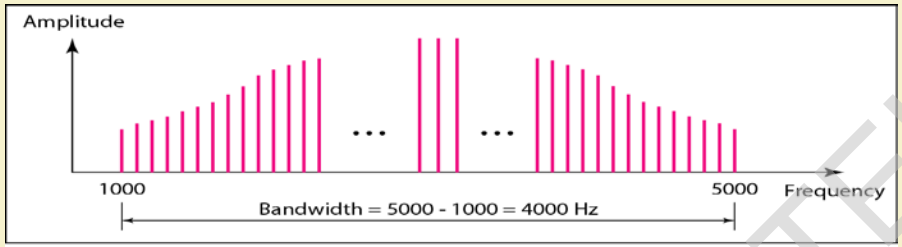
a. Time domain



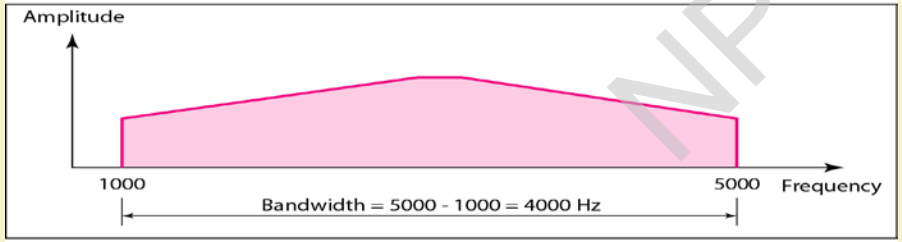
b. Frequency domain

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

Bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.




a. Bandwidth of a periodic signal

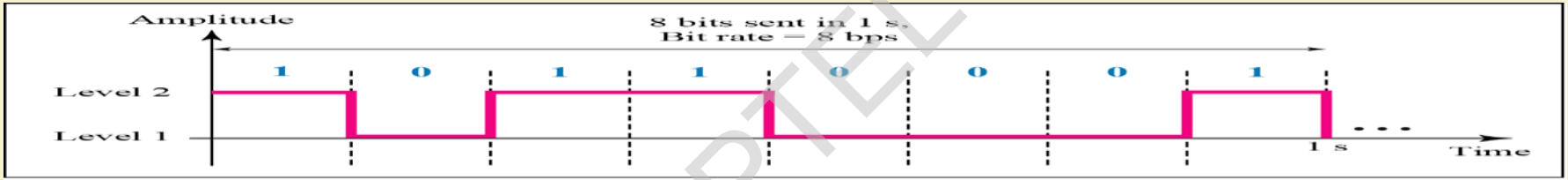



b. Bandwidth of a nonperiodic signal

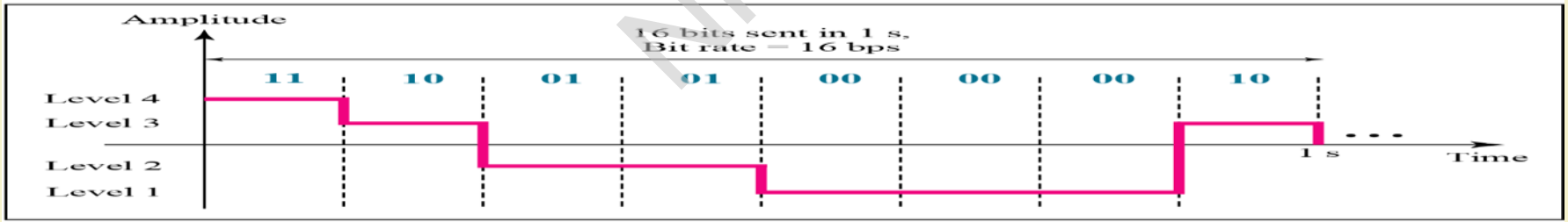
BW = freq(H) – freq(L)

# Digital Signals

In addition to being represented by an analog signal, information can also be represented by a *digital signal*. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels.




a. A digital signal with two levels




b. A digital signal with four levels

A digital signal has eight levels. How many bits are needed per level? We calculate the number of bits from the formula:

$$\text{Number of bits per level} = \log_2 8 = 3$$

Each signal level is represented by 3 bits.

*Bit rate is the number of bits sent in Is, expressed in bits per second (bps).*

Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel?

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

$$100 \times 24 \times 80 \times 8 = 1{,}636{,}000 \text{ bps} = 1.636 \text{ Mbps}$$

A digitized voice channel, is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?

Bit rate can be calculated as:

$$2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}$$

## What is the bit rate for high-definition TV (HDTV)?

HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally a ratio of 16 : 9. There are 1920 by 1080 pixels per screen, and the screen is renewed 30 times per second. Twenty-four bits represents one color pixel.

$$1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000 \text{ or } 1.5 \text{ Gbps}$$

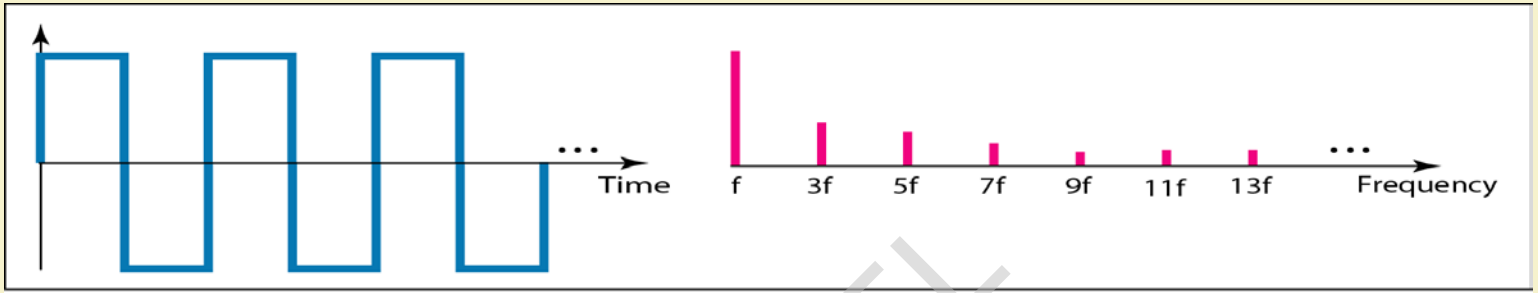
*TV stations reduce this rate to 20 to 40 Mbps through compression.*

# Bit Length

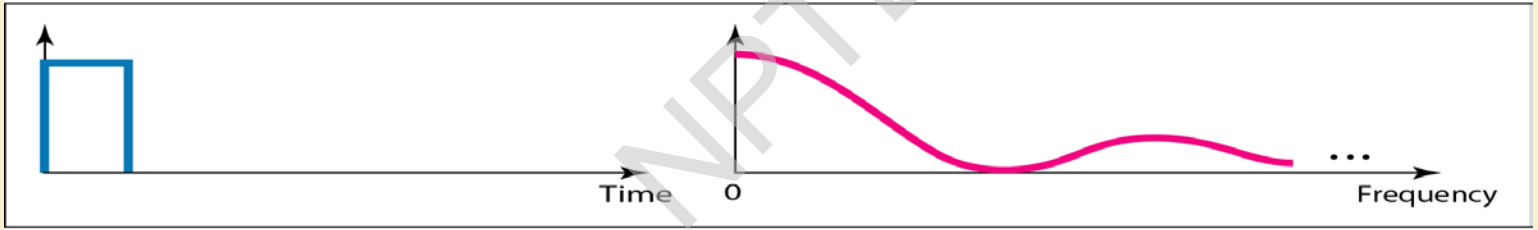
Bit length is the distance one bit occupies on the transmission medium.

*Bit length = propagation speed * bit duration*

# Time and frequency domains of periodic and nonperiodic digital signals




a. Time and frequency domains of periodic digital signal



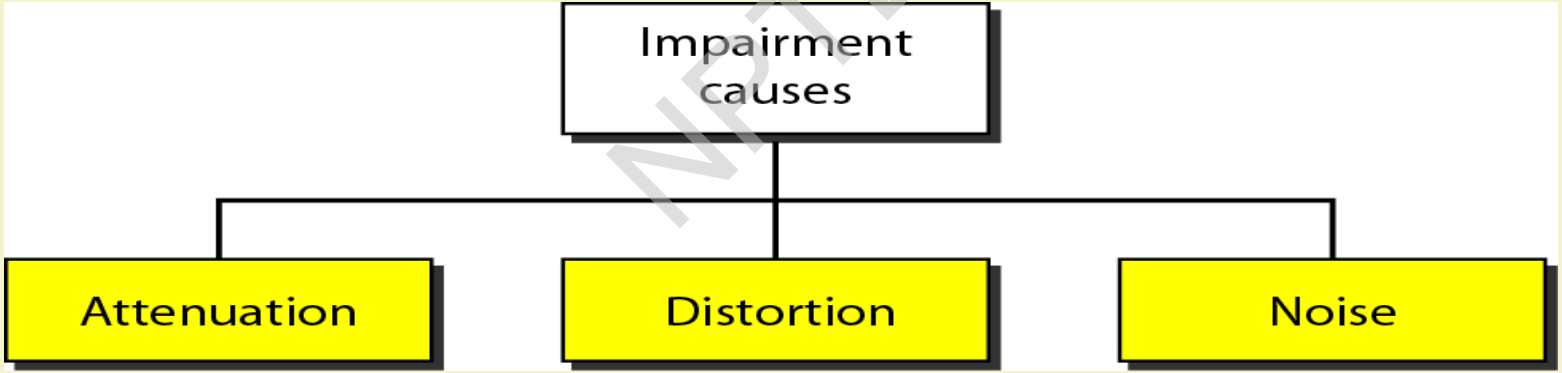

b. Time and frequency domains of nonperiodic digital signal



Note that both bandwidths are infinite, but the periodic signal has discrete frequencies while the nonperiodic signal has continuous frequencies.

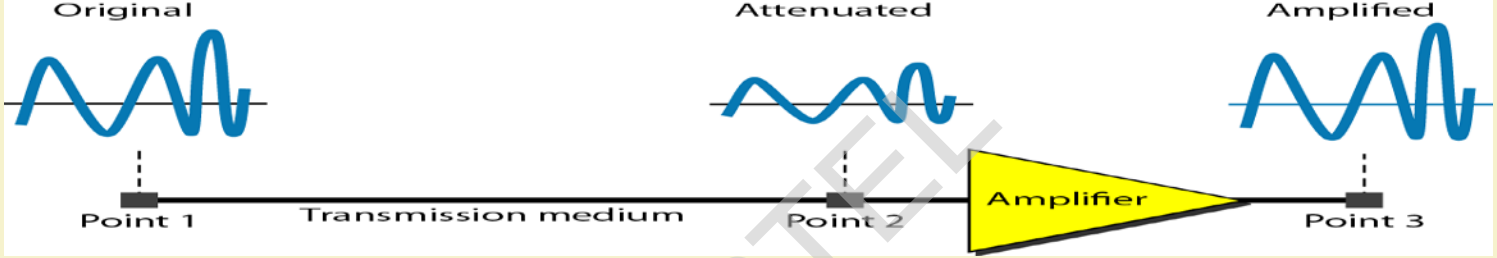
# Transmission Impairment

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium.



# Attenuation

Loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. To compensate for this loss, amplifiers are used to amplify the signal.



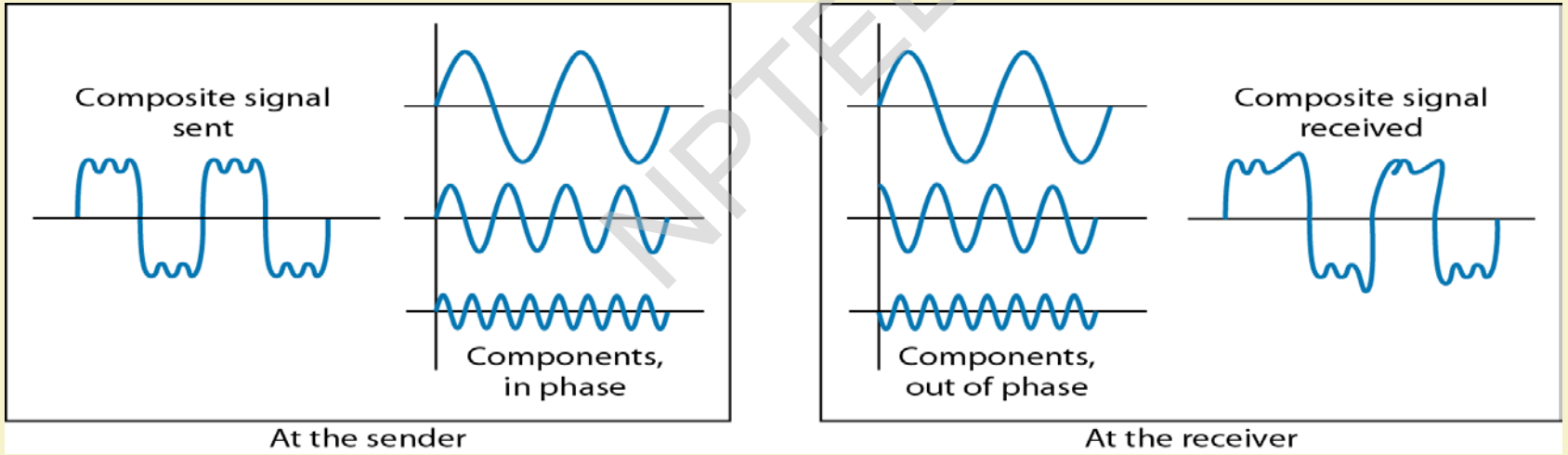

Suppose a signal travels through a transmission medium and its power is reduced to one-half. This means that P2 is (1/2)P1. In this case, the attenuation (loss of power) can be calculated as:

$$10 \log_{10} \frac{P_2}{P_1} = 10 \log_{10} \frac{0.5 P_1}{P_1} = 10 \log_{10} 0.5 = 10(-0.3) = -3 \text{ dB}$$

*A loss of 3 dB (–3 dB) is equivalent to losing one-half the power.*

# Distortion

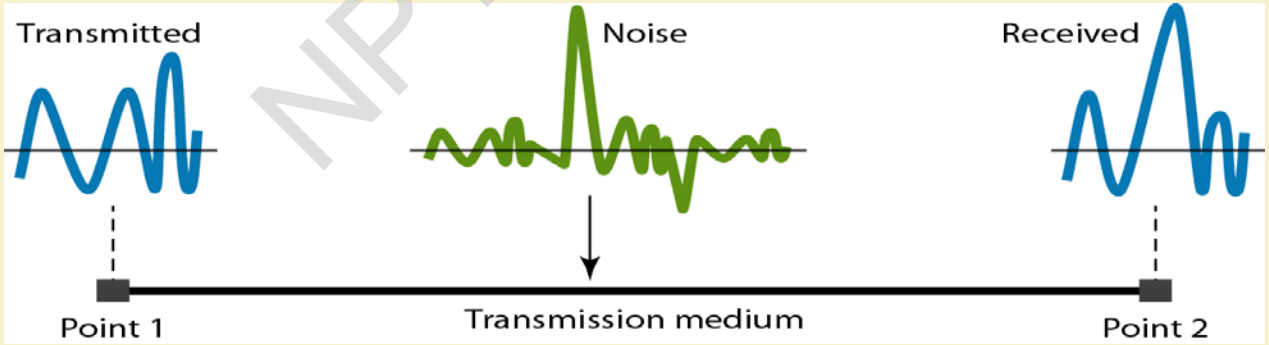
Signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.



# Noise

Several types of noise, such as *thermal noise, induced noise, crosstalk, and impulse noise*, may corrupt the signal.

- Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.
- Induced noise comes from sources such as motors and appliances.
- Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.
- Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.



## Signal-to-Noise Ratio (SNR)

To find the theoretical bit rate limit, we need to know the ratio of the signal power to the noise power.

*SNR = average signal power / average noise power*

Average signal power and the average noise power are considered as these may change with time.
A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

Since SNR is the ratio of two powers, it is often described in decibel units, SNRdB, defined as

$$\mathbf{SNR = 10\ log_{10}\ SNR}$$

The power of a signal is 10 mW and the power of the noise is 1 µW; what are the values of SNR and $SNR_{dB}$ ?

$$\text{SNR} = \frac{10{,}000\ \mu\text{W}}{1\ \text{mW}} = 10{,}000$$

$$\text{SNR}_{\text{dB}} = 10 \log_{10} 10{,}000 = 10 \log_{10} 10^4 = 40$$

# Data Rate Limits

Data rate depends on three factors:

- Bandwidth available
- Level of the signals
- Quality of the channel (the level of noise)

Increasing the levels of a signal may reduce the reliability of the system.

Two theoretical formulas were developed to calculate the data rate: one by **Nyquist** for a noiseless channel, another by **Shannon** for a noisy channel.

For a noiseless channel, the **Nyquist bit rate formula** defines the theoretical maximum bit rate

$$\text{BitRate} = 2 * \text{bandwidth} * \log_2 L$$

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}$$

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \times 3000 \times \log_2 4 = 12{,}000 \text{ bps}$$

## Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\textbf{Capacity} = \textbf{bandwidth} * \log_2 (1 + \text{SNR})$$

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. Channel capacity C:

$$C = B \log_2 (1 + \text{SNR}) = B \log_2 (1 + 0) = B \log_2 1 = B \times 0 = 0$$

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

For practical purposes, when the SNR is very high, we can assume that SNR + 1 is almost the same as SNR. In these cases, the theoretical channel capacity can be simplified to

$$C = B \times \frac{\text{SNR}_{\text{dB}}}{3}$$

*We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level?*

First, we use the Shannon formula to find the upper limit.

$$C = B \log_2 (1 + \text{SNR}) = 10^6 \log_2 (1 + 63) = 10^6 \log_2 64 = 6 \text{ Mbps}$$

**Shannon formula** gives 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps, for example. Then we use the **Nyquist formula** to find the number of signal levels.

$$4 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 L \quad \rightarrow \quad L = 4$$

- *Shannon capacity gives the upper limit; the Nyquist formula tells the signal levels.*

# COMPUTER NETWORKS AND INTERNET PROTOCOLS

## Layer 1: Physical Layer-III



**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

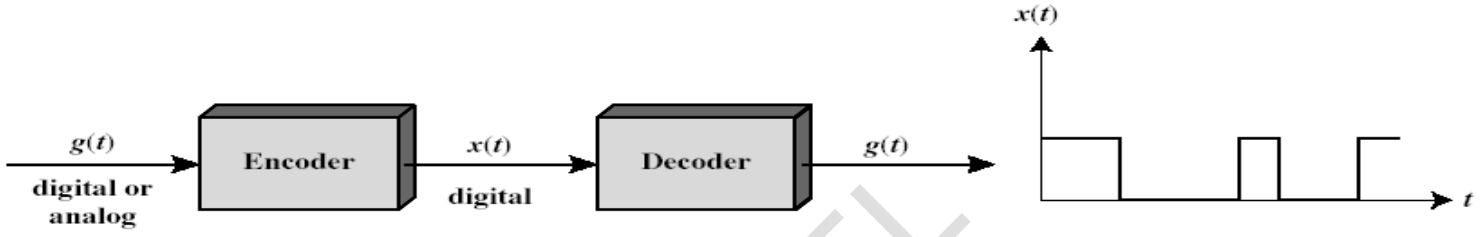
# Encoding / Decoding Techniques

- **Encoding** is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for efficient transmission of data.
- **Decoding** is the reverse process of encoding which is to extract the information from the converted format.

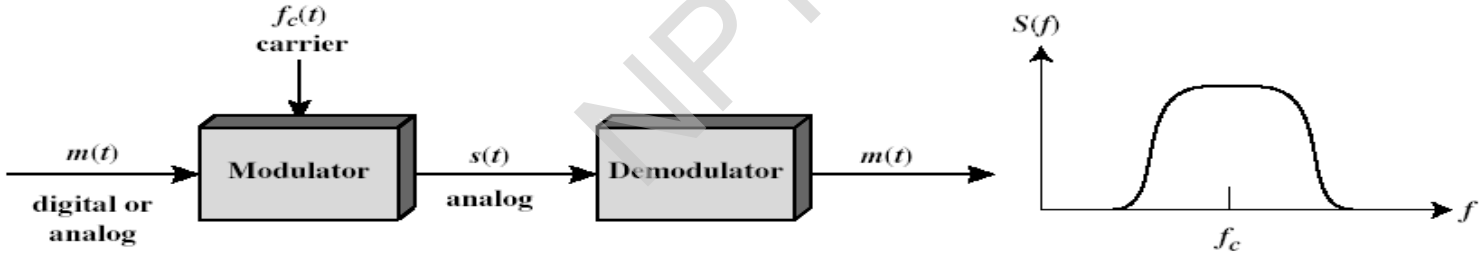


*Ref: Data and Computer Communications, W. Stallings; Computer Networks and Internets by Douglas E. Comer; Data Communications and Networking, B.A. Forouzan; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com*

# Encoding and Modulation




(a) Encoding onto a digital signal




(b) Modulation onto an analog signal

# Modulation

- Modulation is the process of encoding source data onto a carrier signal with frequency $f_c$.
  - Frequency of the carrier signal is chosen to be compatible with the transmission medium being used.
  - Modulation techniques involve operation on one or more of the three parameters: *amplitude, frequency* and *phase*
- According to the input source signal m(t) (either analog or digital), which is called baseband signal (or modulating signal) , the carrier signal $f_c(t)$ will be modulated into modulated signal s(t).

# Encoding / Modulation Techniques

- Digital data, Digital signal
  - The equipment for encoding digital data into a digital signal is less complex and less expensive than digital-to-analog modulation equipment.
- Analog data, Digital signal
  - Conversion of analog data (e.g., voice, video) to digital form permits the use of modern digital transmission & switching.
- Digital data, Analog signal
  - Optical system and unguided media (wireless system) only propagate analog signals.
- Analog data, Analog signal
  - Baseband: easy and cheap, e.g., in voice-grade telephone lines, voice signals are transmitted over telephone lines at their original spectrum
  - Modulation permits frequency division multiplexing, e.g., AM/FM radios

# Digital Data, Digital Signal

- Digital signal is a sequence of discrete, discontinuous **voltage pulses.**
- Each pulse is a **signal element.**
- Binary data are transmitted by encoding the bit stream into signal elements.
- In the simplest case, one bit is represented by one signal element.
  - Say, *1 is represented by a lower voltage level, and 0 is represented by a higher voltage level*

# Terminologies

- Unipolar
  - If all signal elements have the same algebraic sign (all positive or all negative), then the signal is unipolar.
- Polar
  - One logic state represented by positive voltage, the other by negative voltage
- Data rate
  - Rate of data transmission measured in **bps**: ***bits per second***
- Duration or length of a bit
  - Time taken for transmitter to emit the bit
- Modulation rate
  - Rate at which the signal level changes
  - Measured in **baud:** ***signal elements per second***
- Mark and Space
  - Mark: Binary 1
  - Space: Binary 0

# Interpreting the Signals

- Receiver needs to know
  - The timing of each signal element, i.e., when a signal element begins and ends
  - signal levels
- Factors affecting successful interpreting of signals
  - Signal-to-noise ratio (SNR)
  - Data rate
  - Bandwidth
- Some principles:
  - An increase in data rate increases bit error rate (BER)
  - An increase in SNR decreases BER
  - An increase in bandwidth allows an increase in data rate
- Another factor that can improve performance:
  - **Encoding scheme**: the mapping from data bits to signal elements

# Encoding Schemes

- Nonreturn to Zero (NRZ)
  - Nonreturn to Zero-Level (NRZ-L)
  - Nonreturn to Zero Inverted (NRZI)
- Multilevel Binary
  - Bipolar-AMI
  - Pseudoternary
- Biphase
  - Manchester
  - Differential Manchester
- Scrambling techniques
  - B8ZS
  - HDB3

# Encoding Schemes

**Nonreturn to Zero-Level (NRZ-L)**
0 = high level
1 = low level

**Nonreturn to Zero Inverted (NRZI)**
0 = no transition at beginning of interval (one bit time)
1 = transition at beginning of interval

**Bipolar-AMI**
0 = no line signal
1 = positive or negative level, alternating for successive ones

**Pseudoternary**
0 = positive or negative level, alternating for successive zeros
1 = no line signal

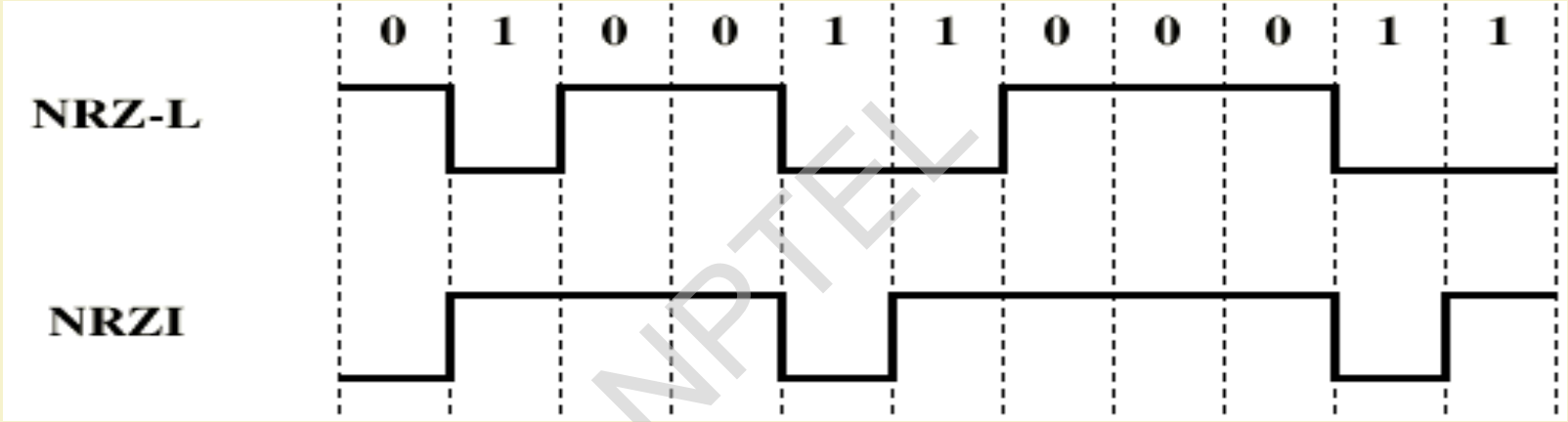
**Manchester**
0 = transition from high to low in middle of interval
1 = transition from low to high in middle of interval

**Differential Manchester**
Always a transition in middle of interval
0 = transition at beginning of interval
1 = no transition at beginning of interval

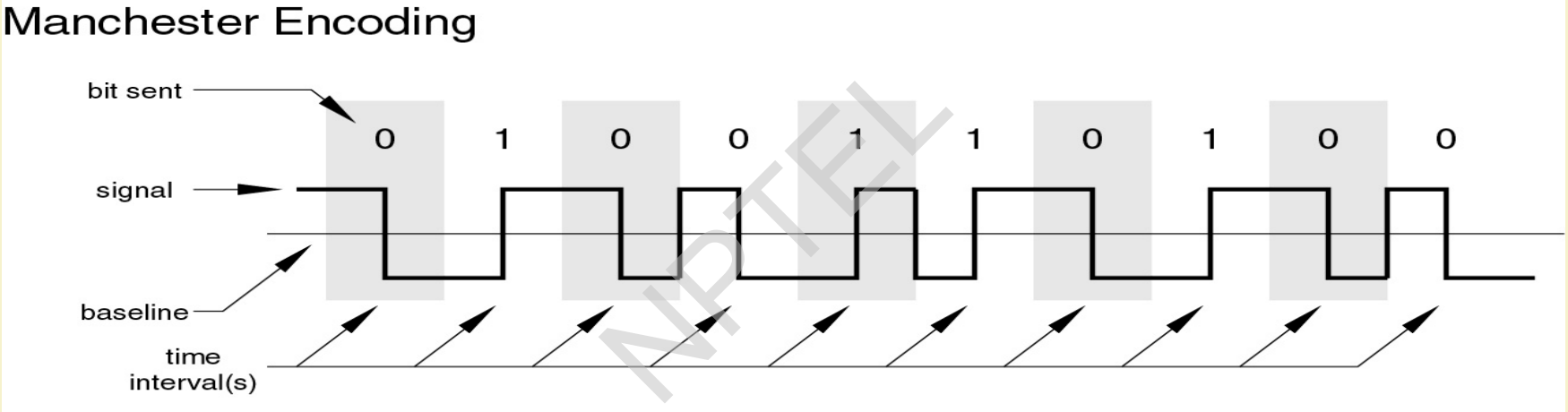
**B8ZS**
Same as bipolar AMI, except that any string of eight zeros is replaced by a string with two code violations

**HDB3**
Same as bipolar AMI, except that any string of four zeros is replaced by a string with one code violation

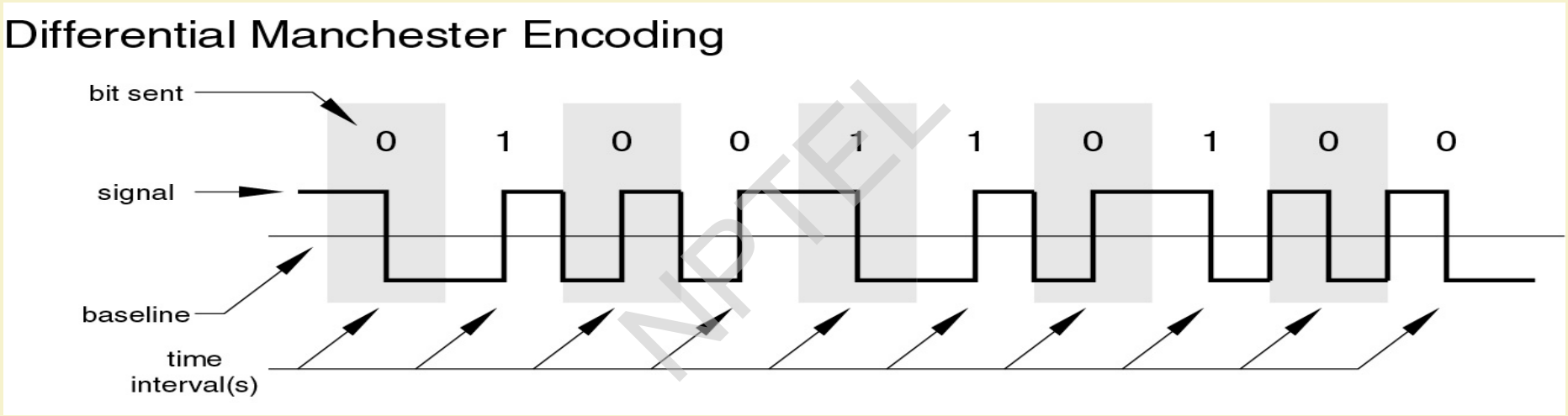
# NRZ



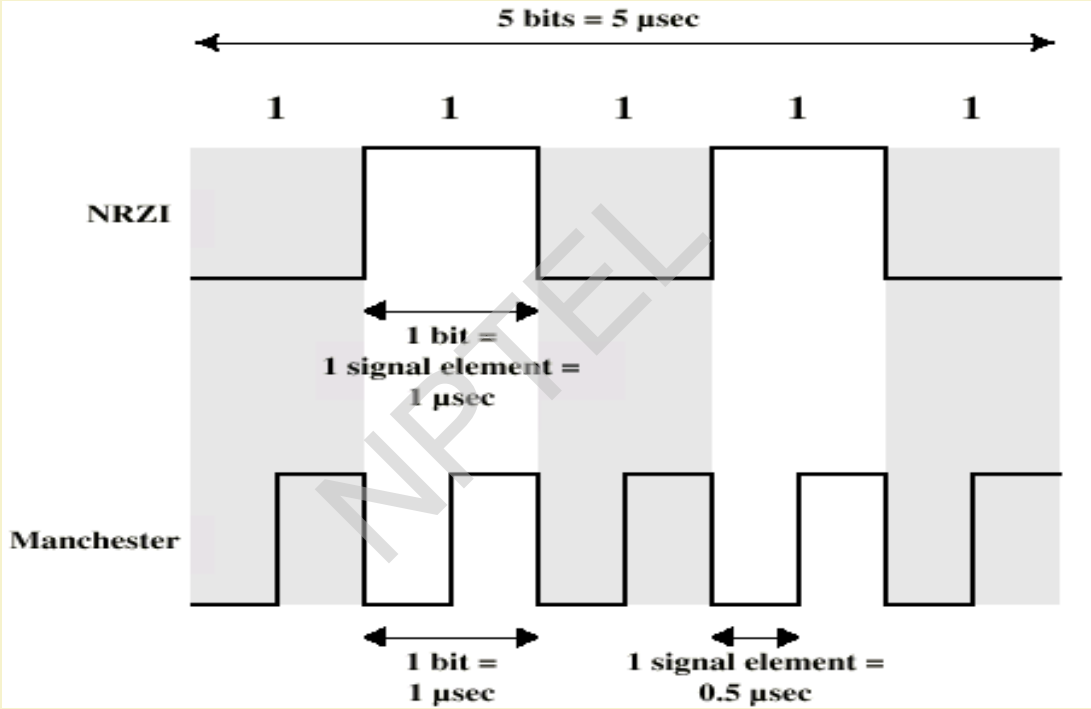
# Manchester Encoding



# Differential Manchester Encoding



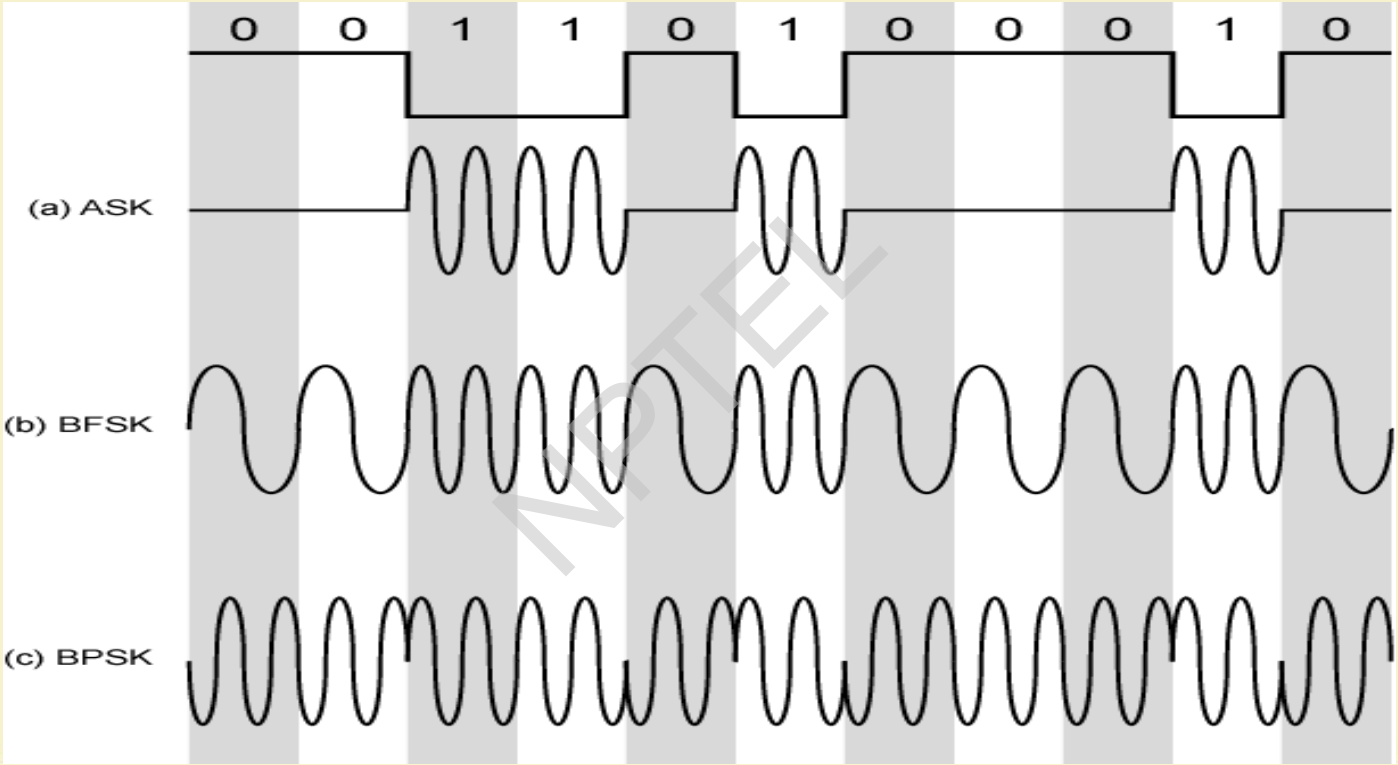
# Modulation Rate



# Digital Data, Analog Signal

- Modulation involves operation of the three characteristics of a carrier signal on one or more
  - Amplitude shift keying (ASK)
  - Frequency shift keying (FSK)
    - Binary FSK (BFSK)
    - Multiple FSK (MFSK)
  - Phase shift keying (PSK)
    - Binary PSK (BPSK)
    - Four-level PSK (QPSK)
    - Multilevel PSK (MPSK)
- QAM: a combination of ASK and PSK
- E.g., Public telephone system
  - Designed to transmit analog signals in 300Hz to 3400Hz
  - Use modem for digital data (modulator-demodulator)

# Modulation Techniques



# Amplitude Shift Keying

- Values are represented by different amplitudes of the carrier frequency
- Usually, one amplitude is zero
  - i.e. presence and absence of carrier is used
- Inefficient: up to 1200bps on voice grade lines
- ASK is used to transmit digital data over optical fiber.

# Binary Frequency Shift Keying

- The most common form of FSK is *binary FSK (*BFSK)
- Two binary values represented by two different frequencies (near carrier frequency)
- BFSK is less susceptible to error than ASK.
- Up to 1200bps on voice grade lines
- Also used for high frequency (3 to 30MHz) radio

# Phase Shift Keying

- In PSK, the phase of the carrier signal is shifted to represent data.
- Binary PSK
  - Two phases represent two binary digits
- Differential PSK
  - Phase shifted relative to previous transmission rather than some constant reference signal

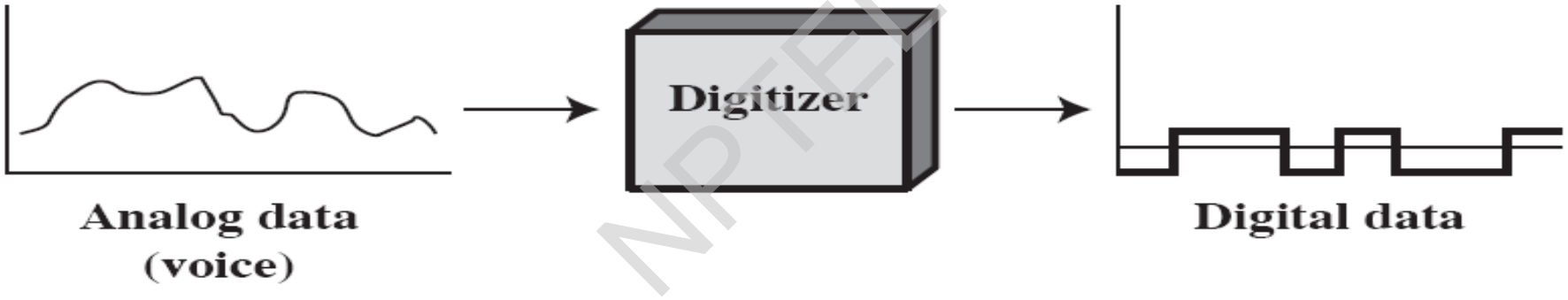
# Quadrature Amplitude Modulation

- QAM is used in the *asymmetric digital subscriber line* (ADSL) and some wireless standards.
- Combination of ASK and PSK
- A logical extension of QPSK
- Send two different signals simultaneously on the same carrier frequency
  - Use two copies of the carrier, one shifted by 90°
  - Each carrier is ASK modulated
  - Two independent signals over same medium
  - Demodulate and combine for original binary output

# Analog Data, Digital Signal

- Digitization
  - Conversion of analog data into digital data
    - Digital data can then be transmitted using NRZ-L
    - Digital data can then be transmitted using code other than NRZ-L
    - Digital data can then be converted to analog signal
  - Analog to digital conversion done using a *codec* (coder-decoder)
  - Two principle codec techniques
    - Pulse Code Modulation
    - Delta modulation

# Digitizing Analog Data



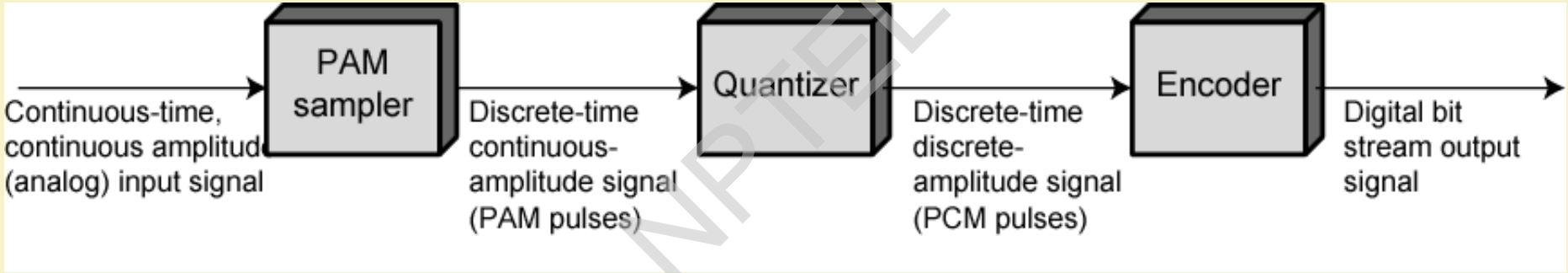
# Pulse Code Modulation

- Sampling Theorem: If a signal is sampled at regular intervals of time and at a rate higher than twice the highest signal frequency, then the samples contain all the information of the original signal.
- For example, voice data are limited to below 4000Hz
  - 8000 samples per second is sufficient to characterize the voice signal.
- Samples are analog samples, called *Pulse Amplitude Modulation* (PAM) samples.
- To convert to digital, each analog sample must be assigned a binary code.

# Pulse Code Modulation

- Each sample is quantized into some level
  - The original signal is now only approximated and cannot be recovered exactly
  - This effect is called quantizing error or quantizing noise
- For example, 8 bit sample gives 256 levels
- 8000 samples per second and 8 bits per sample gives 64kbps, for a single voice signal.

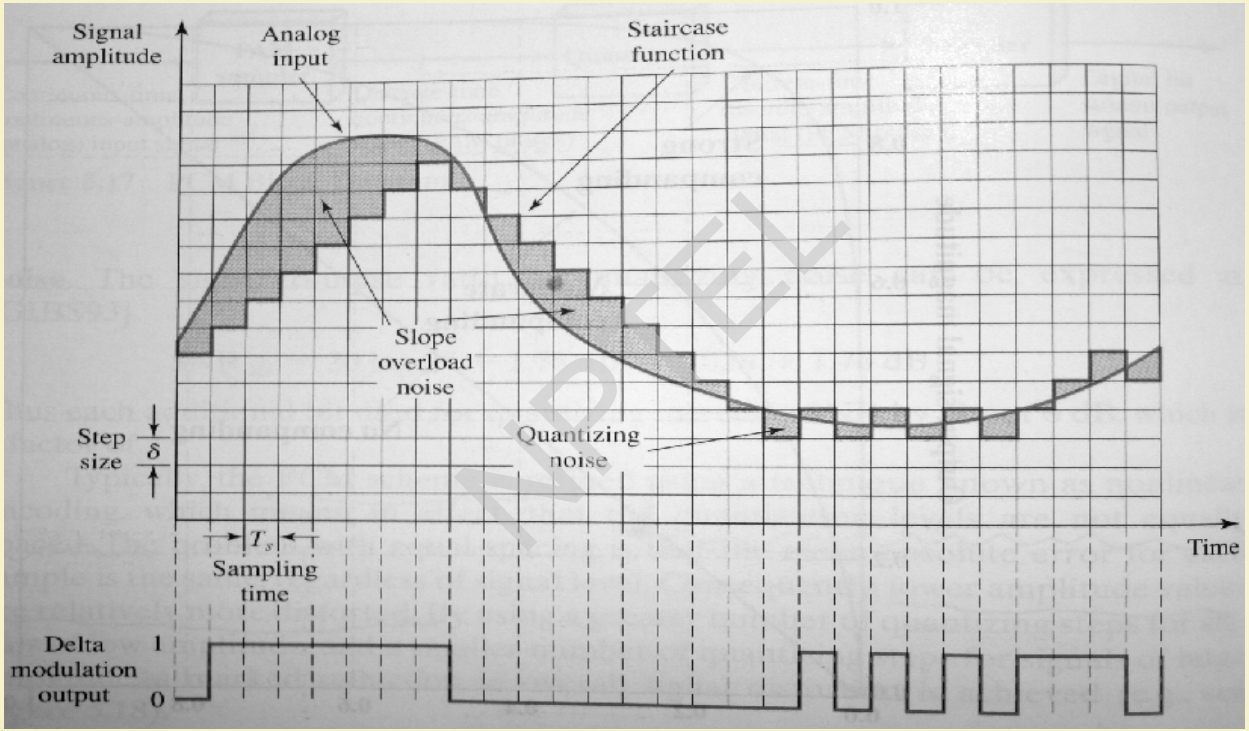
# PCM Block Diagram



# Delta Modulation

- Modulation:
  - An analog signal is approximated by a staircase function that moves up or down by quantization level at each sampling interval.
  - If the value of the sampled waveform exceeds that of the staircase function, 1 is generated, otherwise, 0 is generated.
- Two important parameters:
  - The size of the step.
  - The sampling rate.

# Delta Modulation



# Analog Data, Analog Signals

- Modulation:
  - Combine an input signal m(t) and a carrier frequency $f_c$ to produce a signal s(t) whose bandwidth is usually centered on $f_c$
- Types of modulation
  - Amplitude modulation: AM
  - Angle Modulation
    - Frequency modulation: FM
    - Phase modulation: PM
- E.g., voice signals are transmitted over telephone lines at their original spectrum.

# KEY POINTS

- Both analog and digital information can be encoded as either analog or digital signals. The particular encoding that is chosen depends on the specific requirements to be met and the media and communications facilities available.
- Digital data, digital signal: The simplest form of digital encoding of digital data is to assign one voltage level to binary one and another to binary zero. More complex encoding schemes are used to improve performance, by altering the spectrum of the signal and providing synchronization capability.
- Digital data, analog signal: A modem converts digital data to an analog signal so that it can be transmitted over an analog line. The basic techniques are ASK, FSK, and PSK.

# KEY POINTS

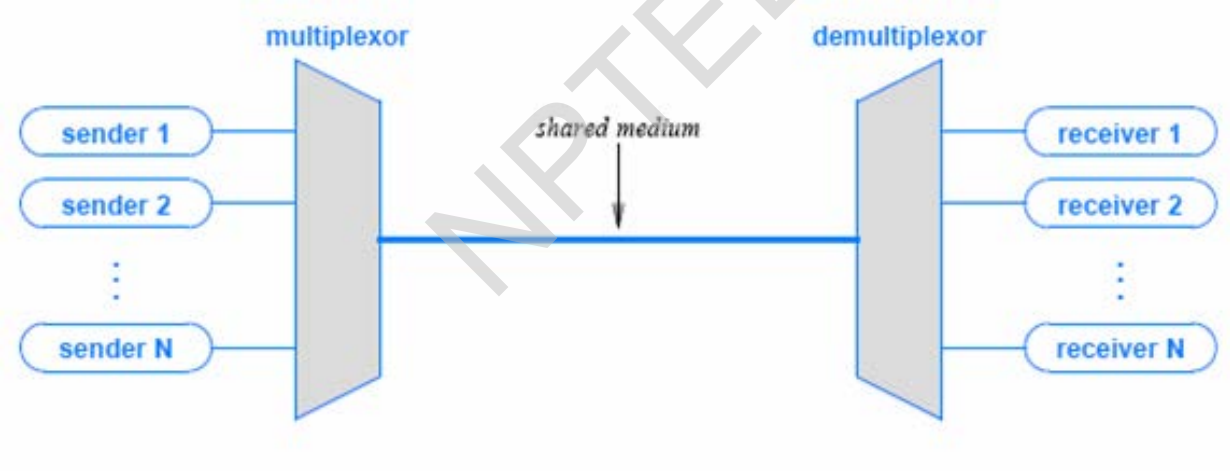
- Analog data, digital signals: Analog data, such as voice and video, are often digitized to be able to use digital transmission facilities. The simplest technique is PCM (Pulse Code Modulation), which involve sampling the analog data periodically and quantizing the samples. Another technique is Delta Modulation.
- Analog data, analog signals: Analog data are modulated by a carrier frequency to produce an analog signal in a different frequency band, which can be utilized on an analog transmission system. The basic techniques are AM (Amplitude Modulation), FM (Frequency Modulation), and PM (Phase Modulation).

# Multiplexing / Demultiplexing

- **Multiplexing** (or muxing) is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal; the receiver recovers the separate signals, a process called **demultiplexing** (or demuxing).

# Basic Concept

- Multiplexing to refer to the combination of information streams from multiple sources for transmission over a shared medium
- Demultiplexing to refer to the separation of a combination back into separate information streams

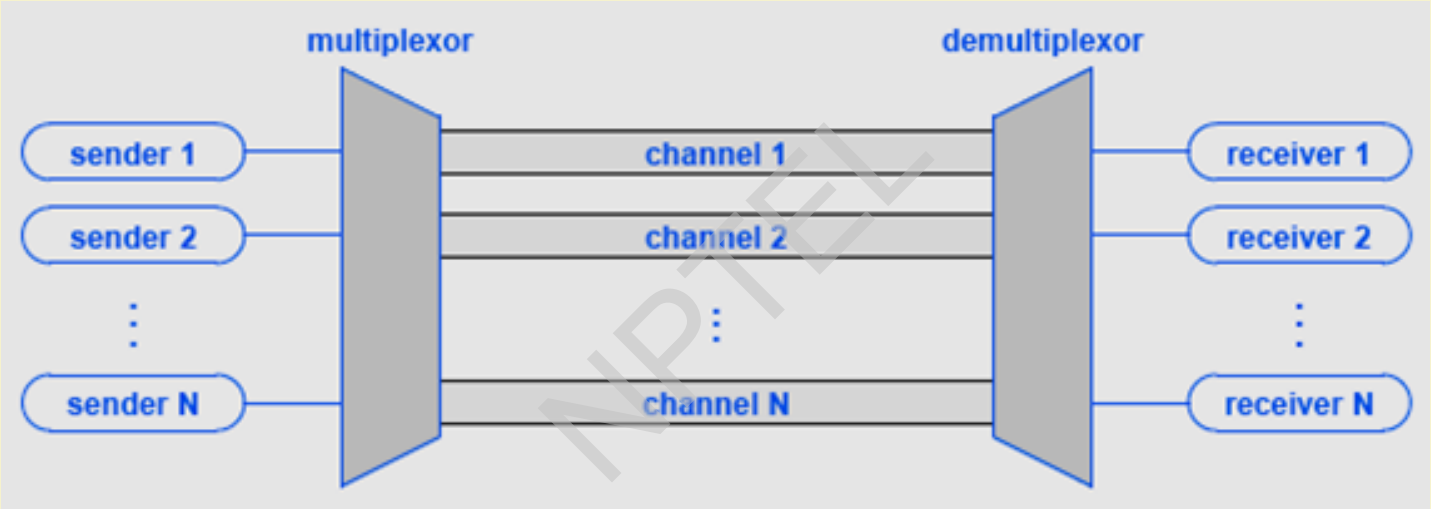


# Types of Multiplexing

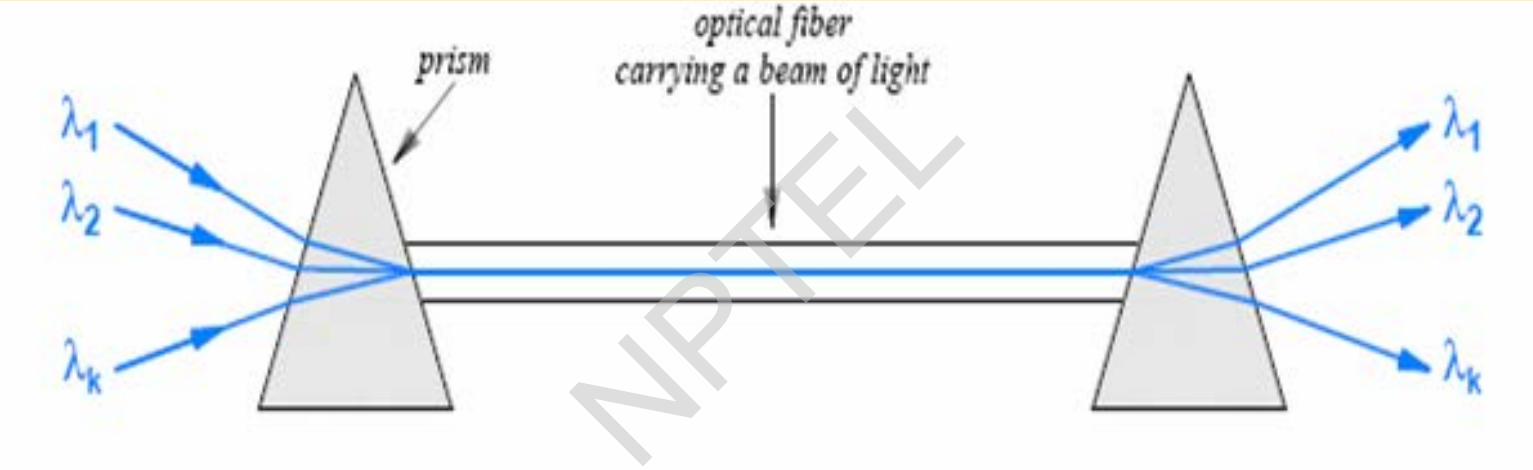
- Frequency Division Multiplexing (FDM)
- Wavelength Division Multiplexing (WDM)
- Time Division Multiplexing (TDM)
- Code Division Multiplexing (CDM)

- TDM and FDM are widely used
- WDM is a form of FDM used for optical fiber
- CDM is a mathematical approach used in cell phone mechanisms

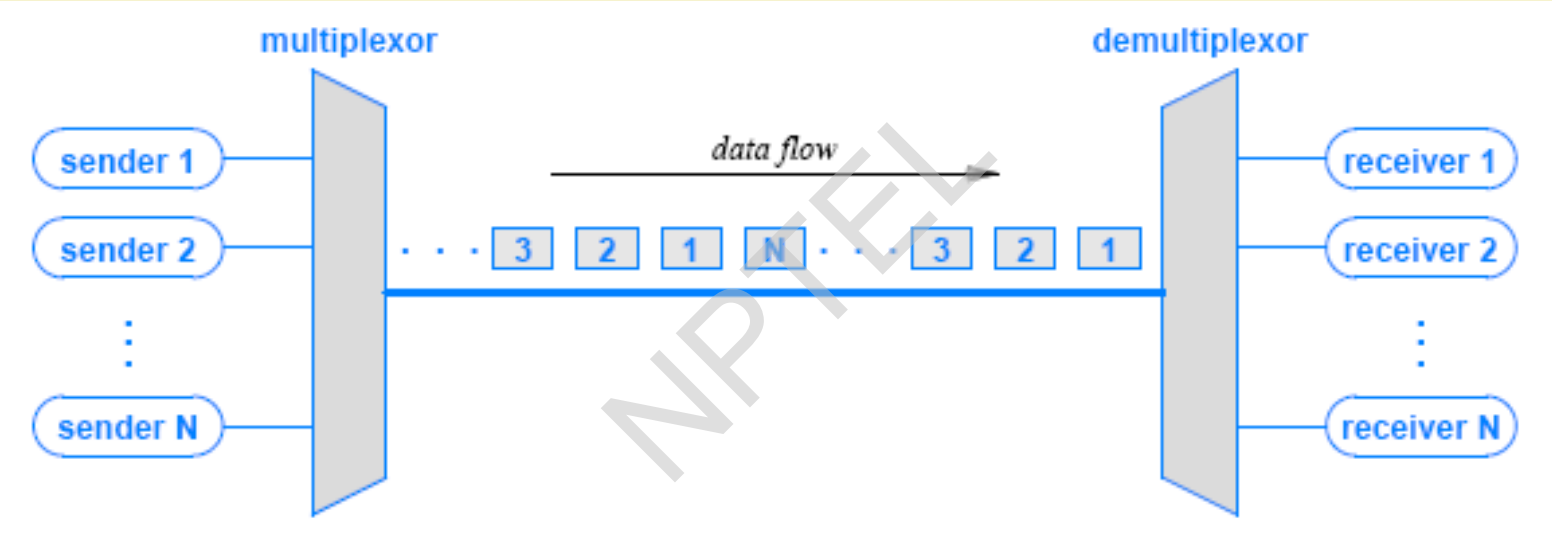
# Frequency Division Multiplexing (FDM)



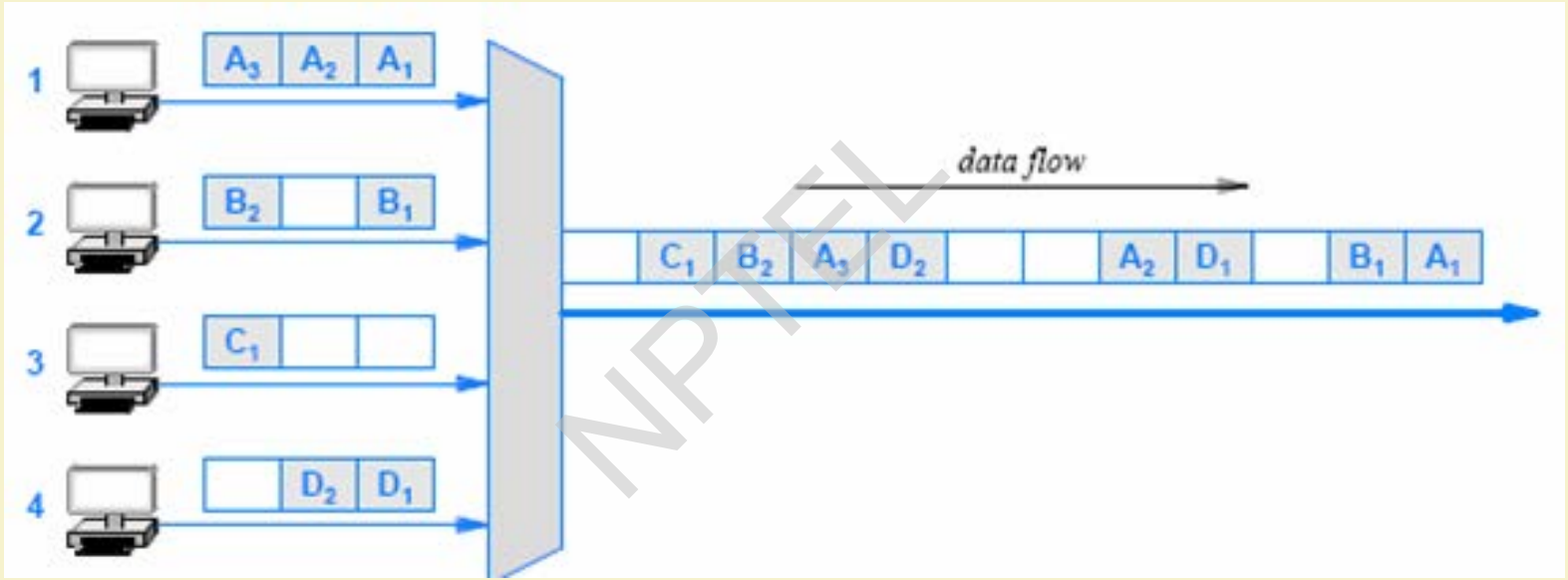
# Wavelength Division Multiplexing (WDM)



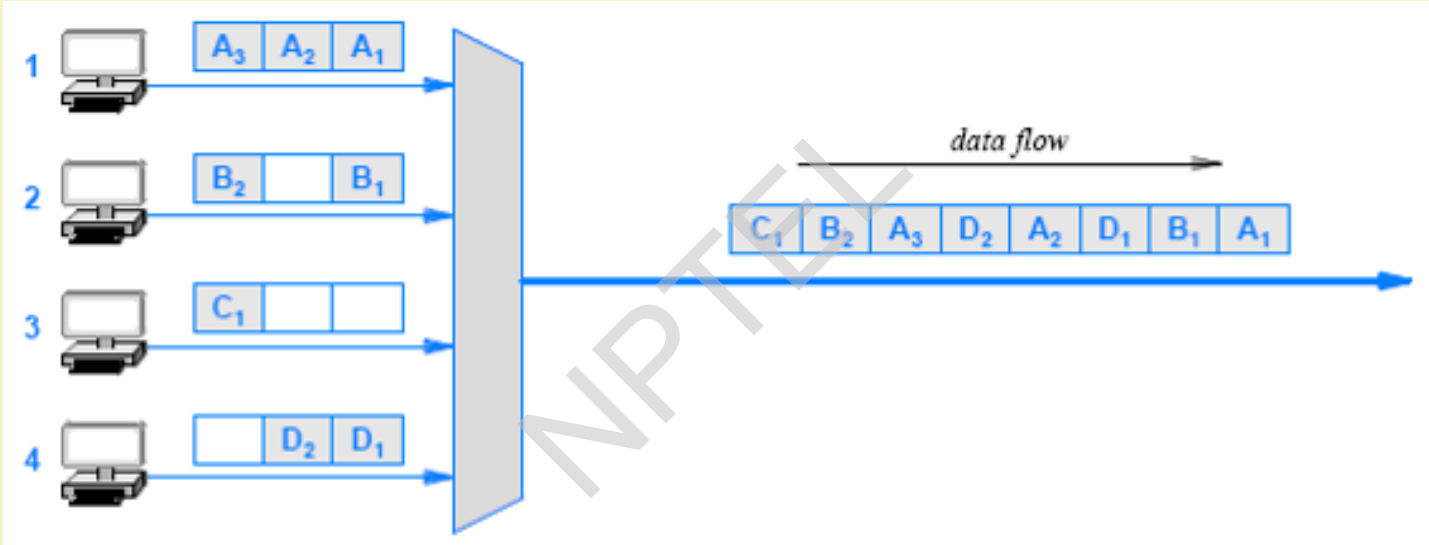
# Time Division Multiplexing (TDM)



# Synchronous TDM



# Statistical TDM



# Code Division Multiplexing (CDM)

- CDM used in parts of the cellular telephone system and for some satellite communication
  - The specific version of CDM used in cell phones is known as *Code Division Multi-Access* (CDMA)
- CDM does not rely on physical properties
  - such as frequency or time
- CDM relies on an interesting mathematical idea
  - values from orthogonal vector spaces can be combined and separated without interference
- Each sender is assigned a unique binary code $\mathbf{C_i}$
  - that is known as a chip sequence
  - chip sequences are selected to be orthogonal vectors
  - (i.e., the dot product of any two chip sequences is zero)

# COMPUTER NETWORKS AND INTERNET PROTOCOLS

## Network Security - Overview



**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

# Security - Basic Components

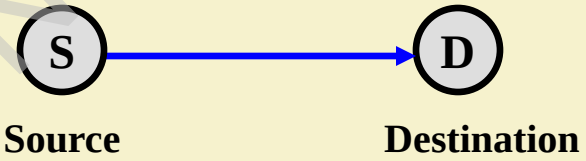
- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources



*Ref: Computer Security: Art and Science by Matt Bishop ;Data Communications and Networking, B.A. Forouzan; Data and Computer Communications, W. Stallings; Local and Metropolitan Area Networks, W. Stallings; TCP/IP Tutorials, IBM Redbooks; CISCO: http:www.cisco.com;* Worcester Polytechnic Institute (WPI), Worcester, MA, USA

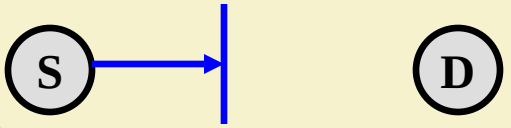
# Security Attacks

- Any action that compromises the security of information.
- Four types of attack:
  1. Interruption
  2. Interception
  3. Modification
  4. Fabrication
- Basic model:

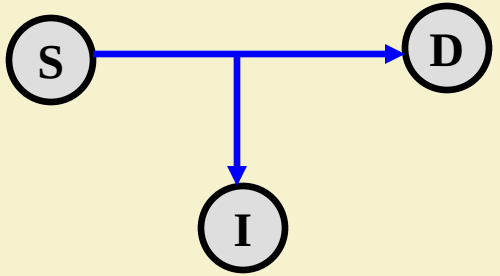


# Security Attacks (contd.)

- Interruption:
  - Attack on availability

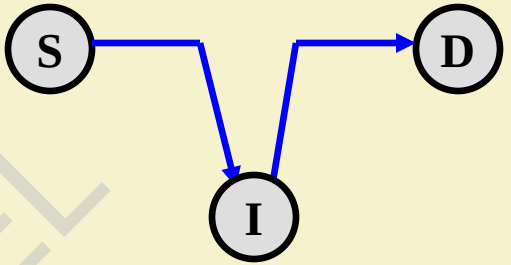



- Interception:
  - Attack on confidentiality

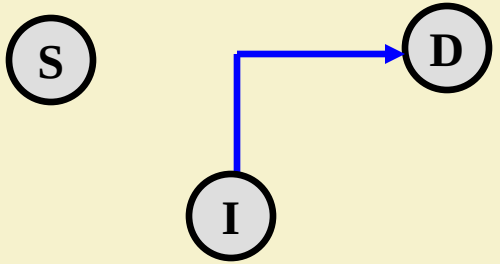


# Security Attacks (contd.)

- Modification:
  - Attack on integrity




- Fabrication:
  - Attack on authenticity



# Classes of Threats

- Disclosure
  - Snooping
- Deception
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption
  - Modification
- Usurpation
  - Modification, spoofing, delay, denial of service

# Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines "security" for the site/system/*etc*.
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

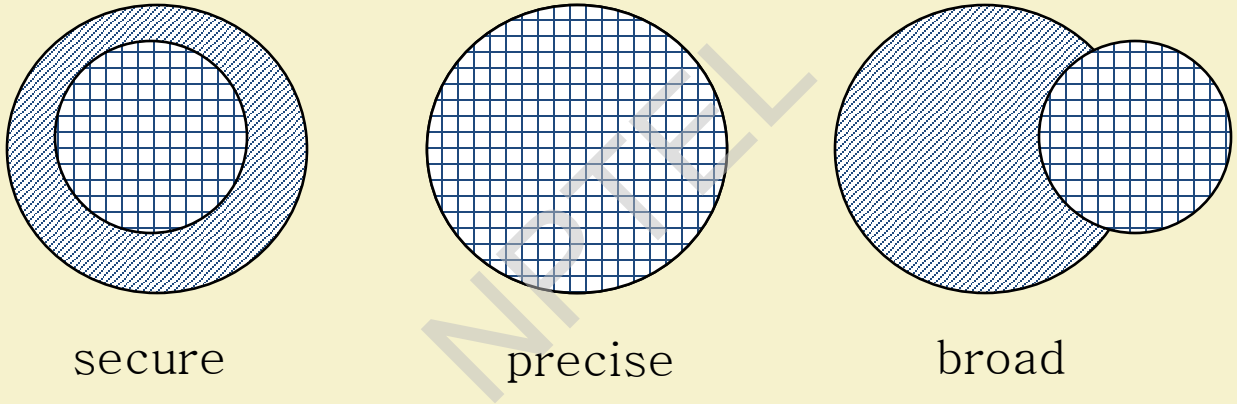
# Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

# Trust and Assumptions

- Underlie *all* aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

# Types of Mechanisms



# Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

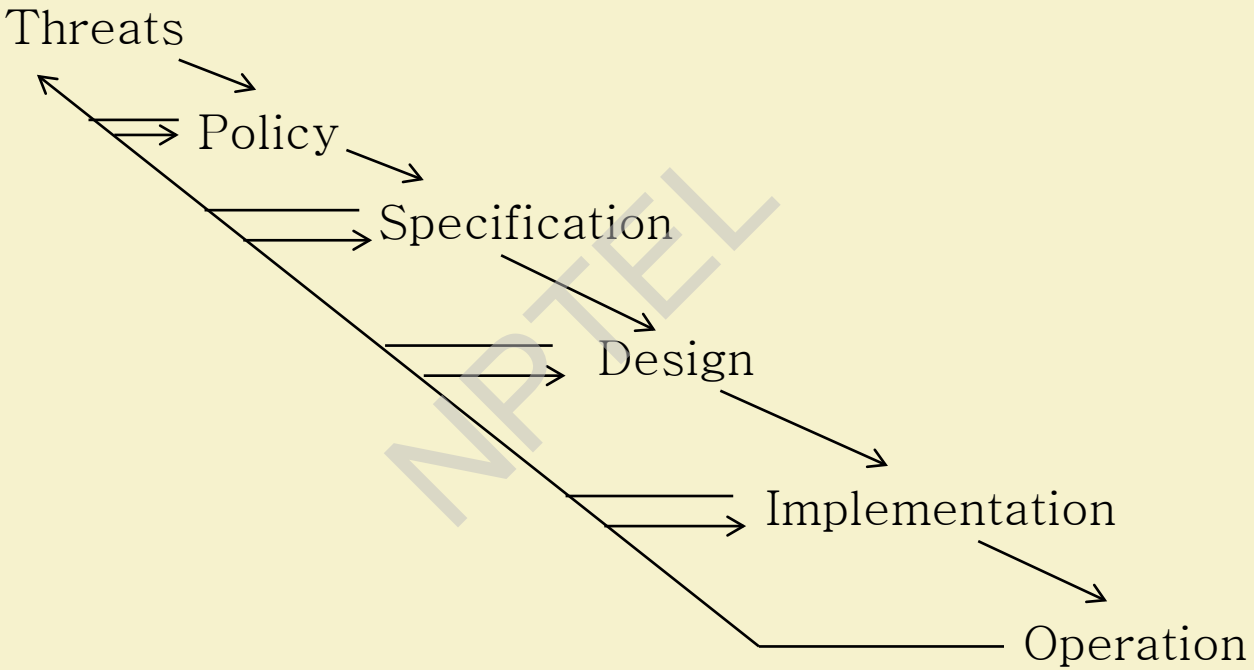
# Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

# Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

# Tying Together



# Passive and Active Attacks

- Passive attacks
  - Obtain information that is being transmitted (eavesdropping).
  - Two types:
    - Release of message contents:- It may be desirable to prevent the opponent from learning the contents of the transmission.
    - Traffic analysis:- The opponent can determine the location and identity of communicating hosts, and observe the frequency and length of messages being exchanged.
  - Very difficult to detect.

# Passive and Active Attacks (contd.)

- Active attacks
  - Involve some modification of the data stream or the creation of a false stream.
  - Four categories:
    - Masquerade:- One entity pretends to be a different entity.
    - Replay:- Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
    - Modification:- Some portion of a legitimate message is altered.
    - Denial of service:- Prevents the normal use of communication facilities.

# Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

# Role of Security

- A security infrastructure provides:
  - Confidentiality – protection against loss of privacy
  - Integrity – protection against data alteration/ corruption
  - Availability – protection against denial of service
  - Authentication – identification of legitimate users
  - Authorization – determination of whether or not an operation is allowed by a certain user
  - Non-repudiation – ability to trace what happened, & prevent denial of actions
  - Safety – protection against tampering, damage & theft

# Types of Attack

- Social engineering/phishing
- Physical break-ins, theft, and curb shopping
- Password attacks
- Buffer overflows
- Command injection
- Denial of service
- Exploitation of faulty application logic
- Snooping
- Packet manipulation or fabrication
- Backdoors

# Network Security Outline

- Network security works like this:
  - Determine network security policy
  - Implement network security policy
  - Reconnaissance
  - Vulnerability scanning
  - Penetration testing
  - Post-attack investigation

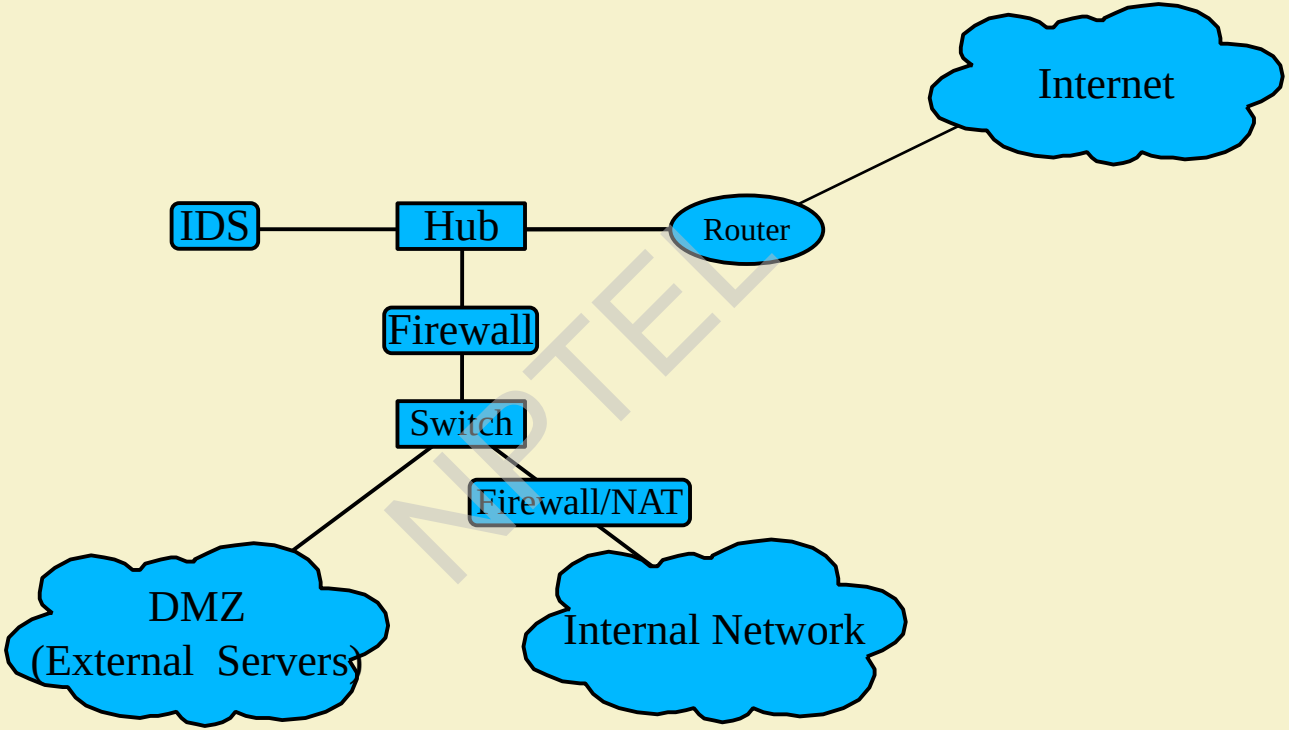
# Step 1: Determine Security Policy

- A security policy is a full security roadmap
  - Usage policy for networks, servers, etc.
  - User training about password sharing, password strength, social engineering, privacy, etc.
  - Privacy policy for all maintained data
  - A schedule for updates, audits, etc.
- The network design should reflect this policy
  - The placement/protection of database/file servers
  - The location of demilitarized zones (DMZs)
  - The placement and rules of firewalls
  - The deployment of intrusion detection systems (IDSs)

# Step 2: Implement Security Policy

- Implementing a security policy includes:
  - Installing and configuring firewalls
    - *iptables* is a common free firewall configuration for Linux
    - Rules for incoming packets should be created
      - These rules should drop packets by default
    - Rules for outgoing packets *may* be created
      - This depends on your security policy
  - Installing and configuring IDSes
    - *snort* is a free and upgradeable IDS for several platforms
    - Most IDSs send alerts to log files regularly
    - Serious events can trigger paging, E-Mail, telephone

# Step 2: Implement Security Policy



# COMPUTER NETWORKS AND INTERNET PROTOCOLS

## Network Security - II


**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

# Network Security Outline

- Network security works like this:
  - Determine network security policy
  - Implement network security policy
  - Reconnaissance
  - Vulnerability scanning
  - Penetration testing
  - Post-attack investigation

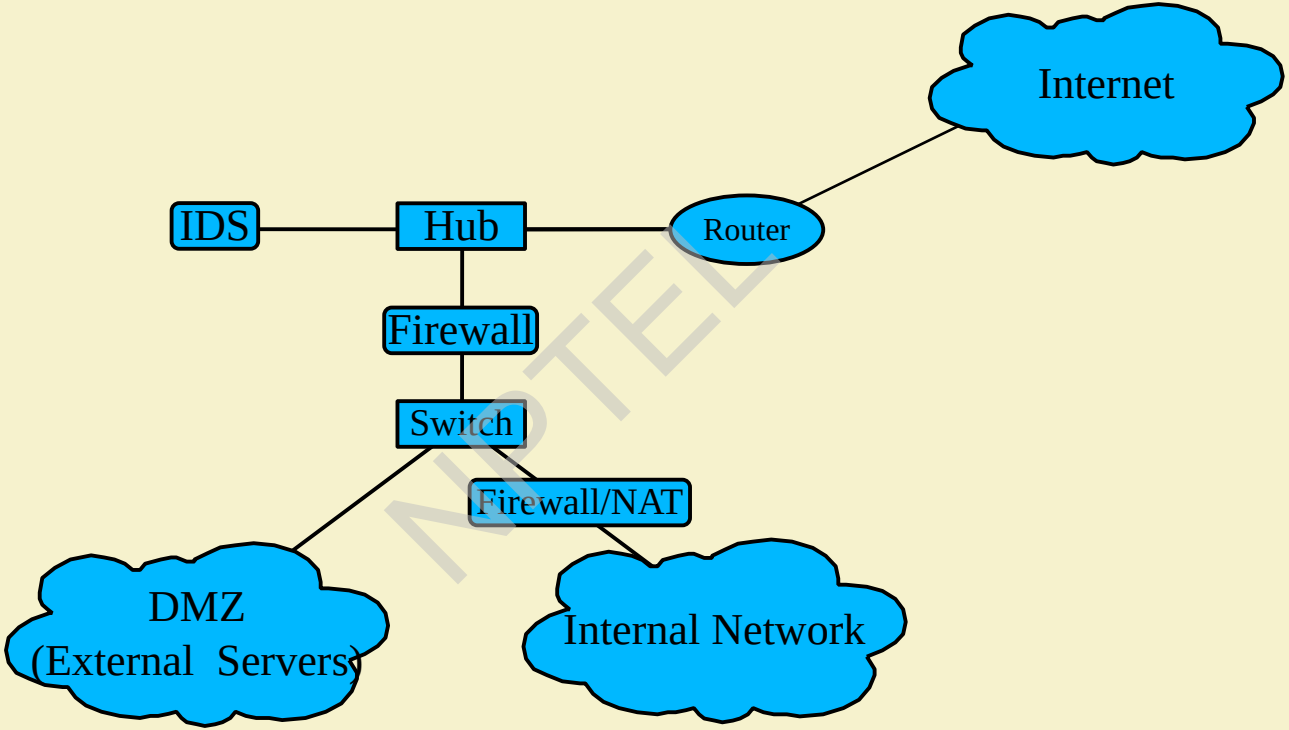
# Step 1: Determine Security Policy

- A security policy is a full security roadmap
  - Usage policy for networks, servers, etc.
  - User training about password sharing, password strength, social engineering, privacy, etc.
  - Privacy policy for all maintained data
  - A schedule for updates, audits, etc.
- The network design should reflect this policy
  - The placement/protection of database/file servers
  - The location of demilitarized zones (DMZs)
  - The placement and rules of firewalls
  - The deployment of intrusion detection systems (IDSs)

# Step 2: Implement Security Policy

- Implementing a security policy includes:
  - Installing and configuring firewalls
    - *iptables* is a common free firewall configuration for Linux
    - Rules for incoming packets should be created
      - These rules should drop packets by default
    - Rules for outgoing packets *may* be created
      - This depends on your security policy
  - Installing and configuring IDSes
    - *snort* is a free and upgradeable IDS for several platforms
    - Most IDSs send alerts to log files regularly
    - Serious events can trigger paging, E-Mail, telephone

# Step 2: Implement Security Policy



# Step 2: Implement Security Policy

- Firewall
  - Applies filtering rules to packets passing through it
  - Comes in three major types:
    - Packet filter – Filters by destination IP, port or protocol
    - Stateful – Records information about ongoing TCP sessions, and ensures out-of-session packets are discarded
    - Application proxy – Acts as a proxy for a specific application, and scans all layers for malicious data
- Intrusion Detection System (IDS)
  - Scans the incoming messages, and creates alerts when suspected scans/attacks are in progress
- Honeypot/honeynet (e.g. honeyd)
  - Simulates a decoy host (or network) with services

# Step 3: Reconnaissance

- First, we learn about the network
  - IP addresses of hosts on the network
  - Identify key servers with critical data
  - Services running on those hosts/servers
  - Vulnerabilities on those services
- Two forms: passive and active
  - Passive reconnaissance is undetectable
  - Active reconnaissance is often detectable by IDS

# Step 4: Vulnerability Scanning

- We now have a list of hosts and services
  - We can now target these services for attacks
- Many scanners will detect vulnerabilities (e.g. nessus)
  - These scanners produce a risk report
- Other scanners will allow you to exploit them (e.g. metasploit)
  - These scanners find ways in, and allow you to choose the payload to use (e.g. obtain a root shell, download a package)
  - The payload is the code that runs once inside
- The best scanners are updateable
  - For new vulnerabilities, install/write new plug-ins
  - e.g. Nessus Attack Scripting Language (NASL)

# Step 5: Penetration Testing

- We have identified vulnerabilities
  - Now, we can exploit them to gain access
  - Using frameworks (e.g. Metasploit), this is as simple as selecting a payload to execute
  - Otherwise, we manufacture an exploit
- We may also have to try to find new vulnerabilities
  - This involves writing code or testing functions accepting user input

# Step 6: Post-Attack Investigation

- Forensics of Attacks
- This process is heavily guided by laws
  - Also, this is normally done by a third party
- Retain chain of evidence
  - The evidence in this case is the data on the host
  - The log files of the compromised host hold the footsteps and fingerprints of the attacker
  - Every minute with that host must be accounted for
  - For legal reasons, you should examine a low-level copy of the disk and not modify the original

# Vulnerability Assessment

- Today's Enterprises are IT-enabled !
- Need for "Self-Security", Vulnerability Assessment
  - Content-aware IPS
  - File system Scanning
  - Penetration Testing

# Penetration Testing
## (*Tiger team attack / Red team attack*)

- Test for evaluating the strengths of all security controls on the computer system
- Goal : Violate the site security policy
- NOT a replacement for careful design and implementation with structured testing
- Methodology for testing the system *in toto* - once it is in place
- Examines procedural and operational controls as well as technological control

# Penetration Testing tools

- Proprietary Tools
  - Extremely expensive.
  - Likely to have backdoors.
  - Inextensible.
  - No access to source
  - Usually not adaptable

- Public domain Tools
  - Good – but others also knows it !
  - Not integrated / automated
  - Not fully functional

- Need to evolve our own framework – proprietary to the organization !

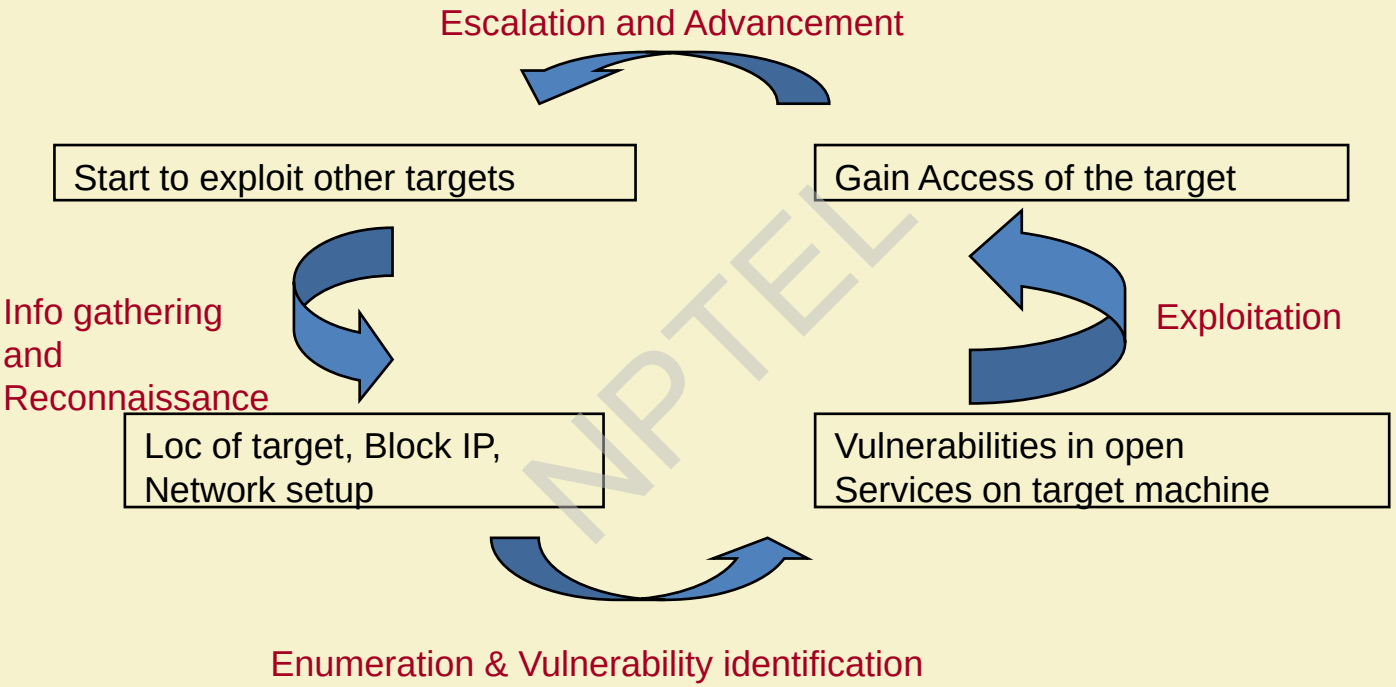
# System Vulnerability

- A vulnerability is a hole or a weakness in the application,
  - Design flaw
  - Implementation bug / Integration flaw
- Vulnerability Types
  - SQL Injection, Buffer Overflow etc
- Penetration Testing - Method of evaluating the vulnerability of a computer system or network by simulating an attack by a malicious hacker

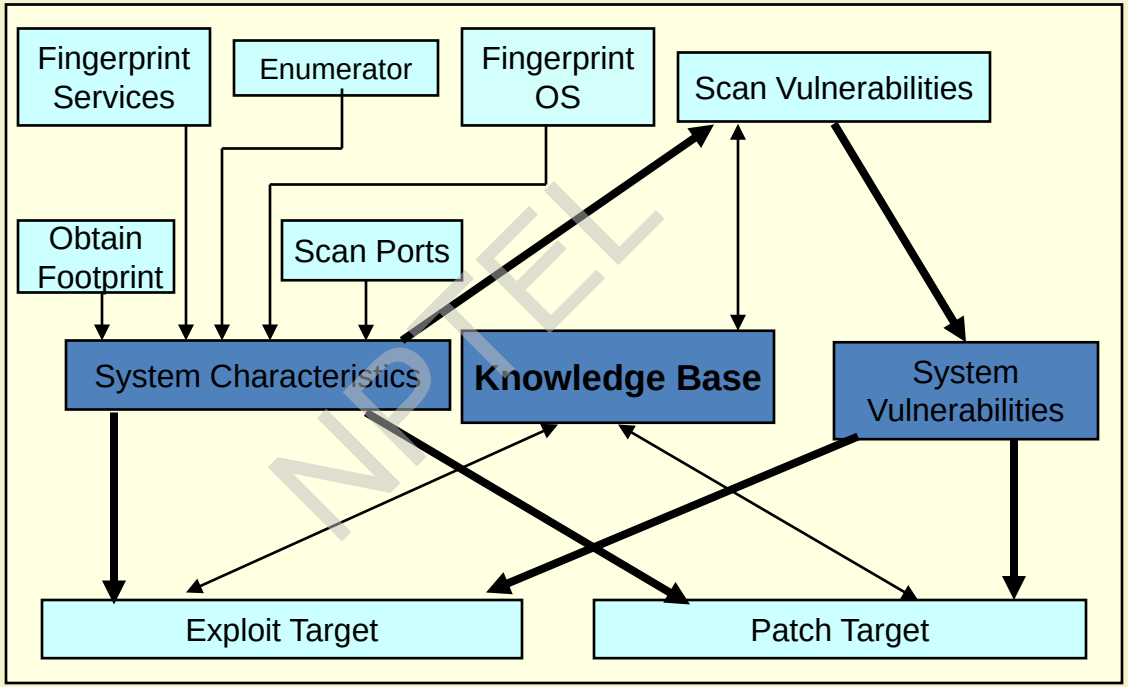
# Penetration Test Methodology

- Information gathering
- Reconnaissance
- Scanning
- Enumeration
- Vulnerability identification
- Exploitation
- Escalation / Advancement
- Suggestions & Workarounds

# Penetration Test Methodology



# Typical Architectural Model of Penetration Testing Tool



# Proxy Server, Network Address Translator (NAT), Firewall

# Proxy Server

- What is a proxy server?
  - Acts on behalf of other clients, and presents requests from other clients to a server.
  - Acts as a server while talking with a client, and as a client while talking with a server.
- Commonly used HTTP proxy server:
  - Squid
    - *available on all platforms.*

# Proxy Server

- It is a server that sits between a client application (Web browser), and a real server.
  - It intercepts all requests to the real server to see if it can fulfill the requests itself.
  - If not, it forwards the request to the real server.

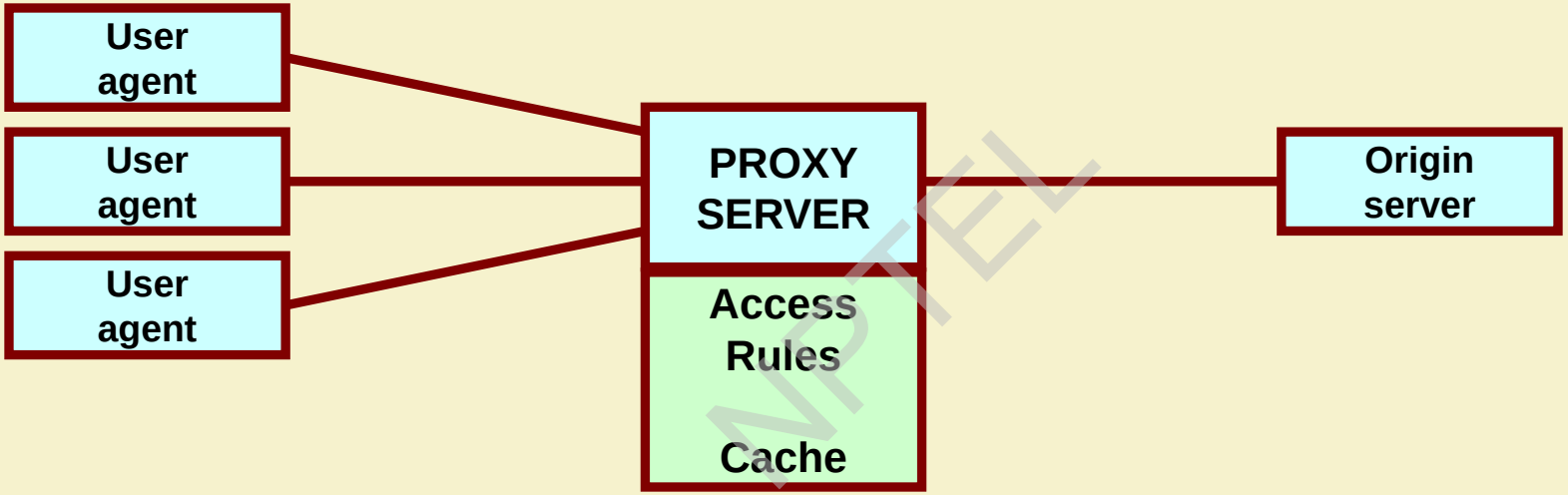
# Proxy Server - Types

- Mainly serves two purposes:
  - Improve performance
    - Can dramatically improve performance for a group of users.
    - It saves all the results of requests in a cache.
    - Can greatly conserve bandwidth.
  - Filter requests
    - Prevent users from accessing a specific set of web sites.
    - Prevent users for accessing pages containing some specified strings.
    - Prevent users from accessing video files (say).

# Anonymous Proxy Servers

- Hide the user's IP address, thereby preventing unauthorized access to user's computer through the Internet.
- All requests to the outside world originate with the IP address of the proxy server.
- Very convenient for group subscription:
  - On-line journals.
  - Digital library.

# Location of Proxy Server



# Functions of a HTTP Proxy

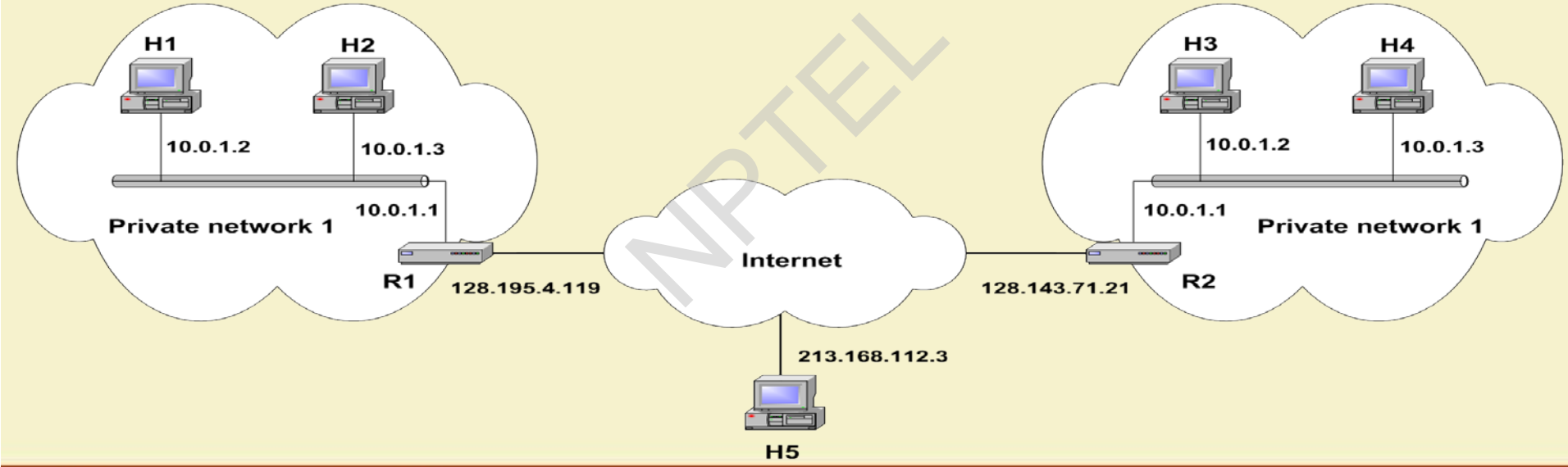
- Request forwarding
  - Primary function.
  - Acts as a rudimentary firewall.
- Access control
  - Allow or deny accesses, based on
    - Contents
    - Location
- Cache management
  - Efficient utilization of bandwidth.
  - Faster access.

# Network Address Translator (NAT)

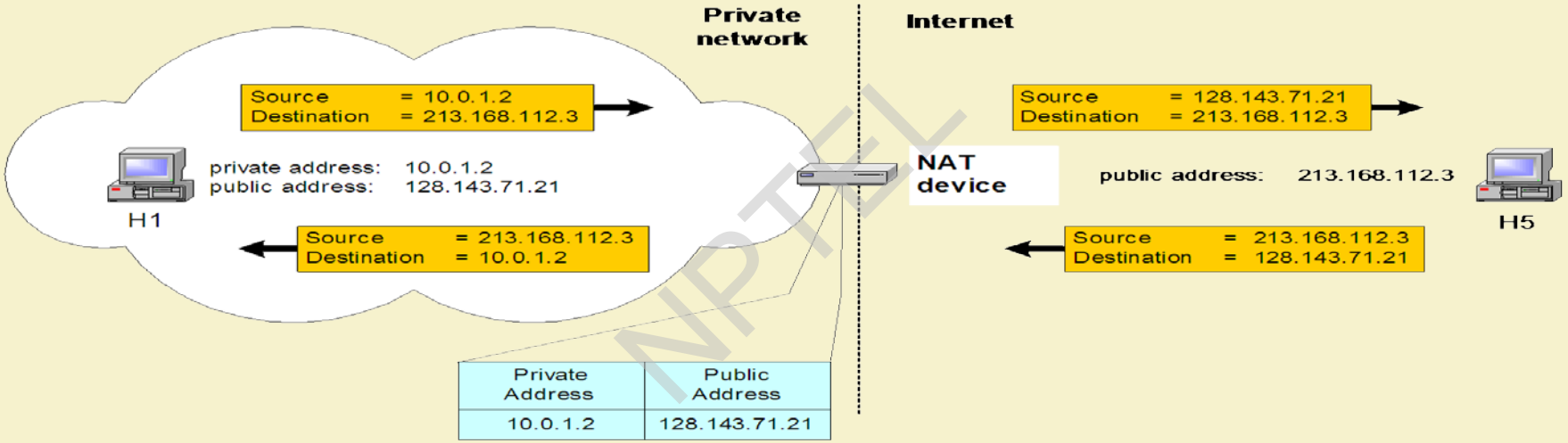
# NAT

- Allows a single device (router or a dedicated box) to act as an agent between the Internet (public network) and a local (private) network.
  - Tries to address the IP address distribution problem.
  - RFC 1631.
  - Only one unique IP address is required to represent an entire group of computers.
  - Several variations possible.

# Private Addresses



# Basic operation of NAT




- NAT device has address translation table

**Typical Address Translation Table (ATT):**

| Source Computer | Source IP address | Source port number | NAT IP address | NAT port number |
|---|---|---|---|---|
| A | 10.5.17.112 | 500 | 203.11.16.5 | 1 |
| B | 10.5.17.85 | 75 | 203.11.16.5 | 2 |
| C | 10.23.10.5 | 2480 | 203.11.16.5 | 3 |
| D | 10.22.5.118 | 1120 | 203.11.16.5 | 4 |

# Capability Limit of a NAT

- Maximum number of concurrent translations:
  - Mainly determined by the size of the memory to store the ATT.
  - Typical entry in the ATT takes about 160 bits.
  - Memory size of 8 Mbyte will support about

    8 x 1024 x 1024 x 8 / 160 = 4,19,000

    concurrent translations.

# Main uses of NAT

- Pooling of IP addresses
- Supporting migration between network service providers
- IP masquerading
- Load balancing of servers

# Concerns about NAT

- Performance:
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum.
  - Modifying port number requires that NAT boxes recalculate TCP checksum.
- Fragmentation
  - Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

# Concerns about NAT

- End-to-end connectivity:
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.

# Concerns about NAT

- IP address in application data:
  - Applications that carry IP addresses in the payload of the application data generally do not work across a private-public network boundary.
  - Some NAT devices inspect the payload of widely used application layer protocols and, if an IP address is detected in the application-layer header or the application payload, translate the address according to the address translation table.

# Other Benefits of NAT

- Use of NAT automatically creates a firewall between the internal and external networks.
  - NAT will only allow connections that has originated from within the internal network.
  - An outside host cannot initiate a connection with an internal host.
- Inbound mapping requires static NAT.

# Is NAT a Proxy Server?

- Ideally “NO”.
  - NAT is transparent to both source and destination hosts. But a proxy server is not transparent.
  - NAT is a layer 3 (network) protocol. In contrast, a proxy server works at layer 4 (transport) or higher.

# Firewall

# Firewall

- Firewalls are effective to
  - protect local systems;
  - protect network-based security threats;
  - provide secured and controlled access to Internet;
  - provide restricted and controlled access from the Internet to local servers.

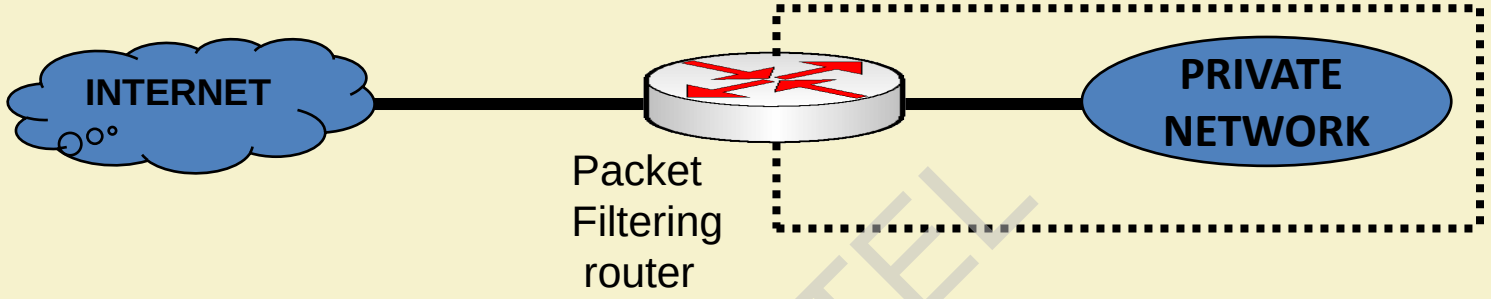
# Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall).
  - Only authorized traffic (defined by the local security police) will be allowed to pass.
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system).

# Types of Firewalls

1. Packet filters.
2. Application-level gateways.
3. Circuit-level gateways.

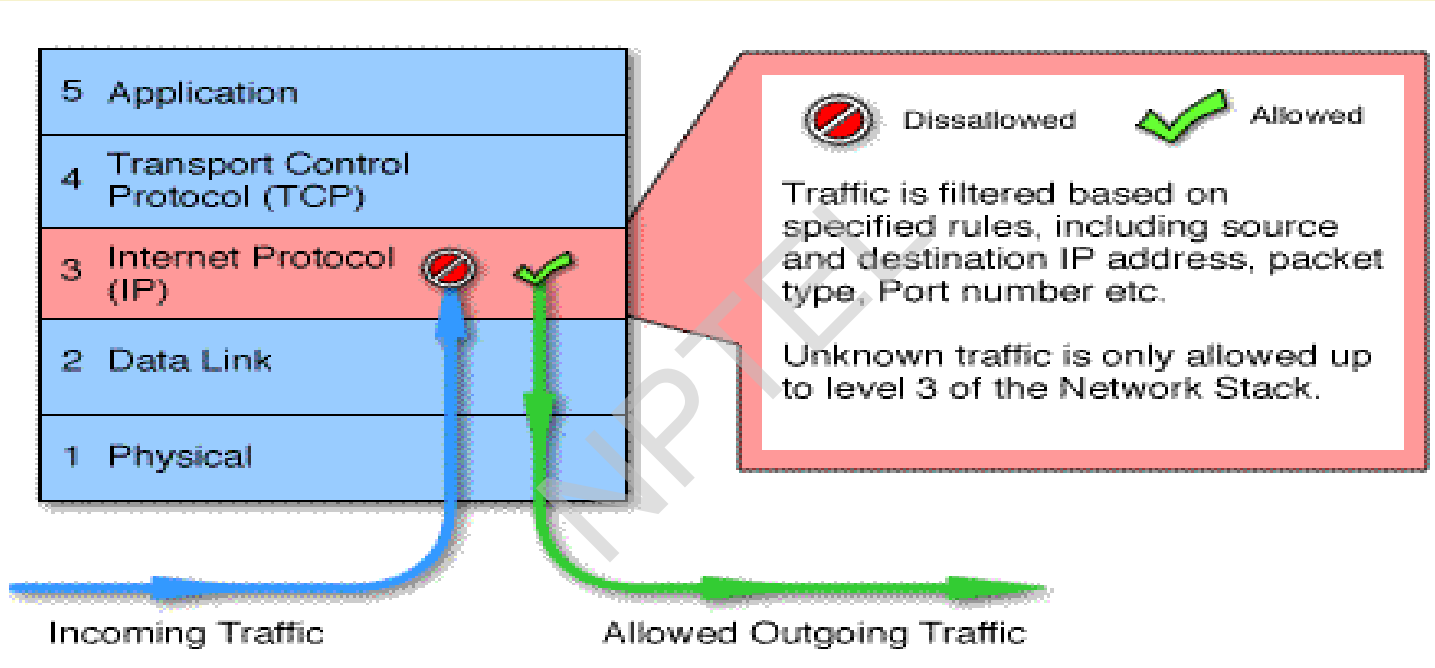
# Packet Filtering Router




Some of the attacks that can be made on packet filtering routers:

- IP address spoofing
- Source Routing attacks
- Tiny fragment attacks

# Packet Filtering Firewall



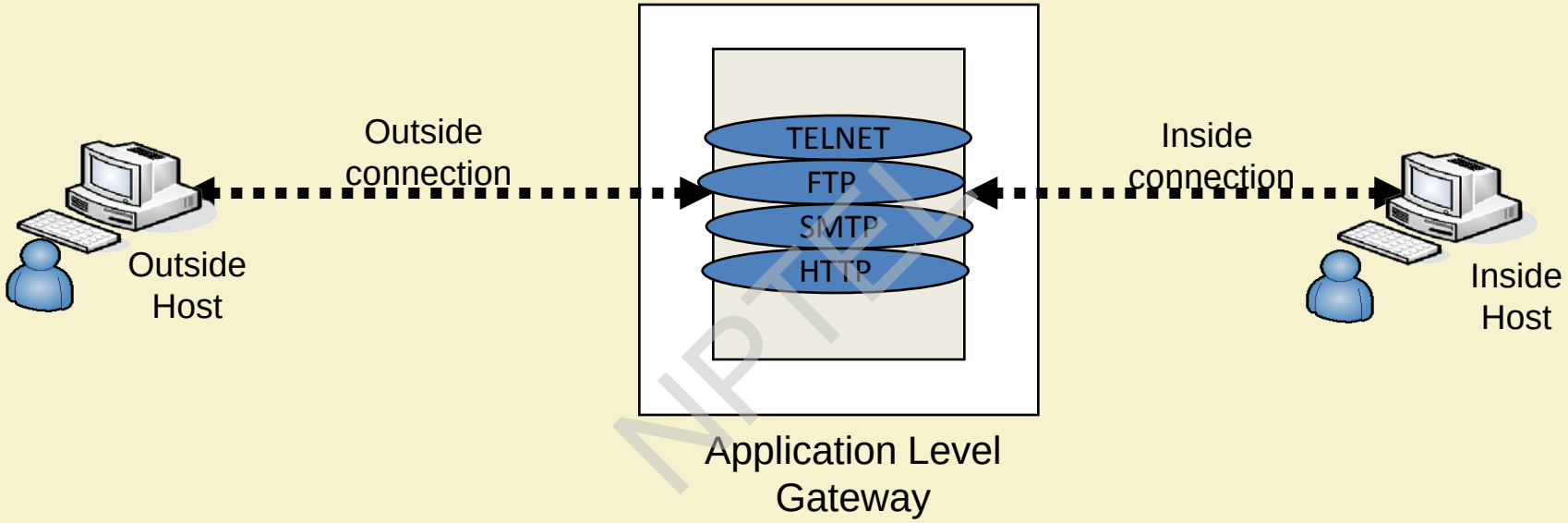
# Packet Filtering Router (contd.)

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
  - Typically based on IP addresses and port numbers.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- Two default policies (discard or forward).

# Packet Filtering Router (contd.)

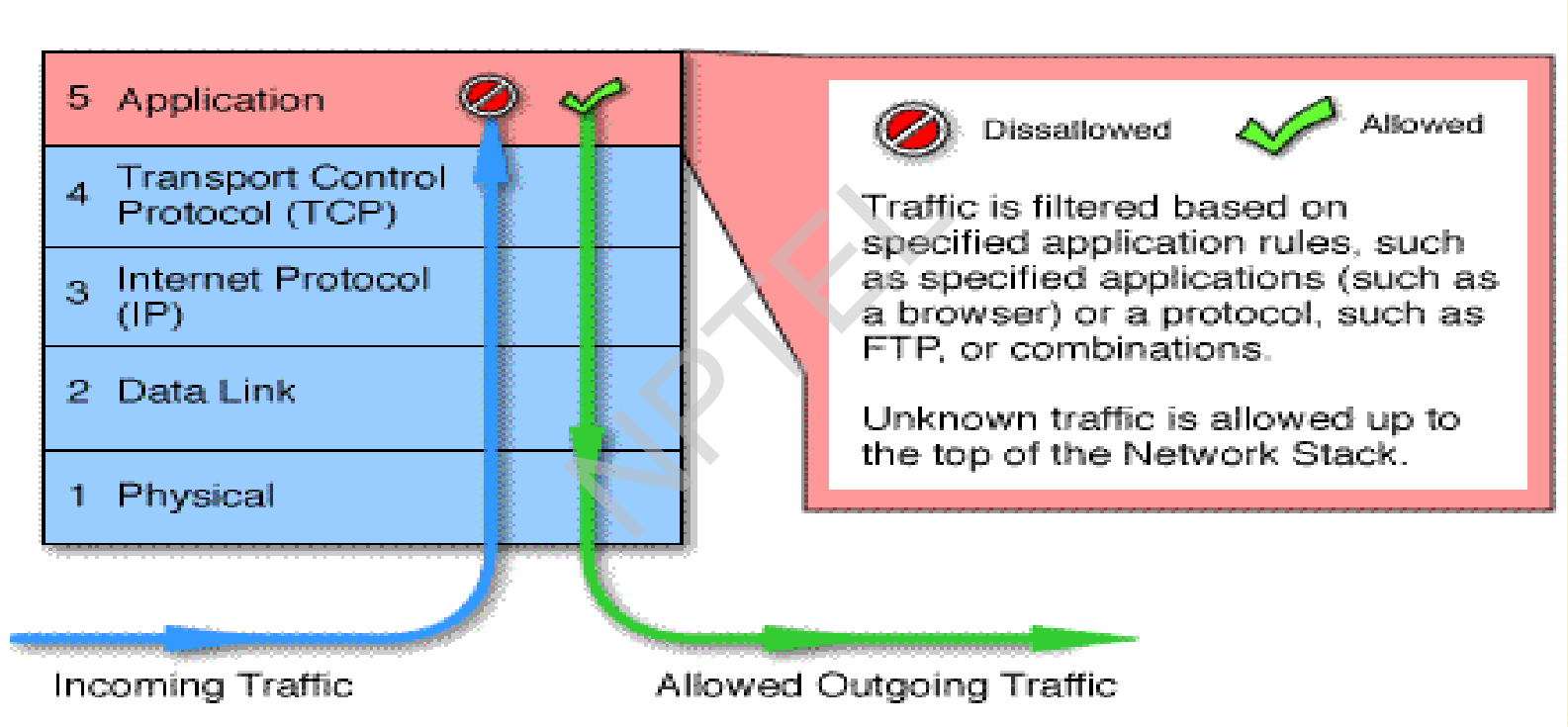
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of authentication

# Application-Level gateway




- Also called a Proxy Server; acts as relay of application level traffic.
- It is service specific.

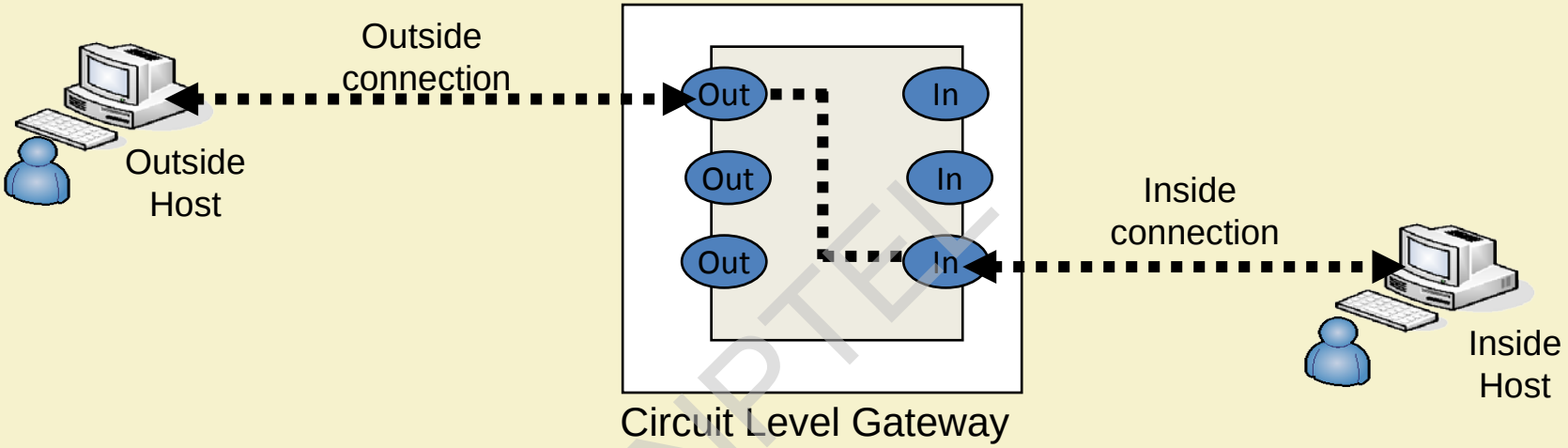
# Application Level Gateway



# Application-level Gateway (contd.)

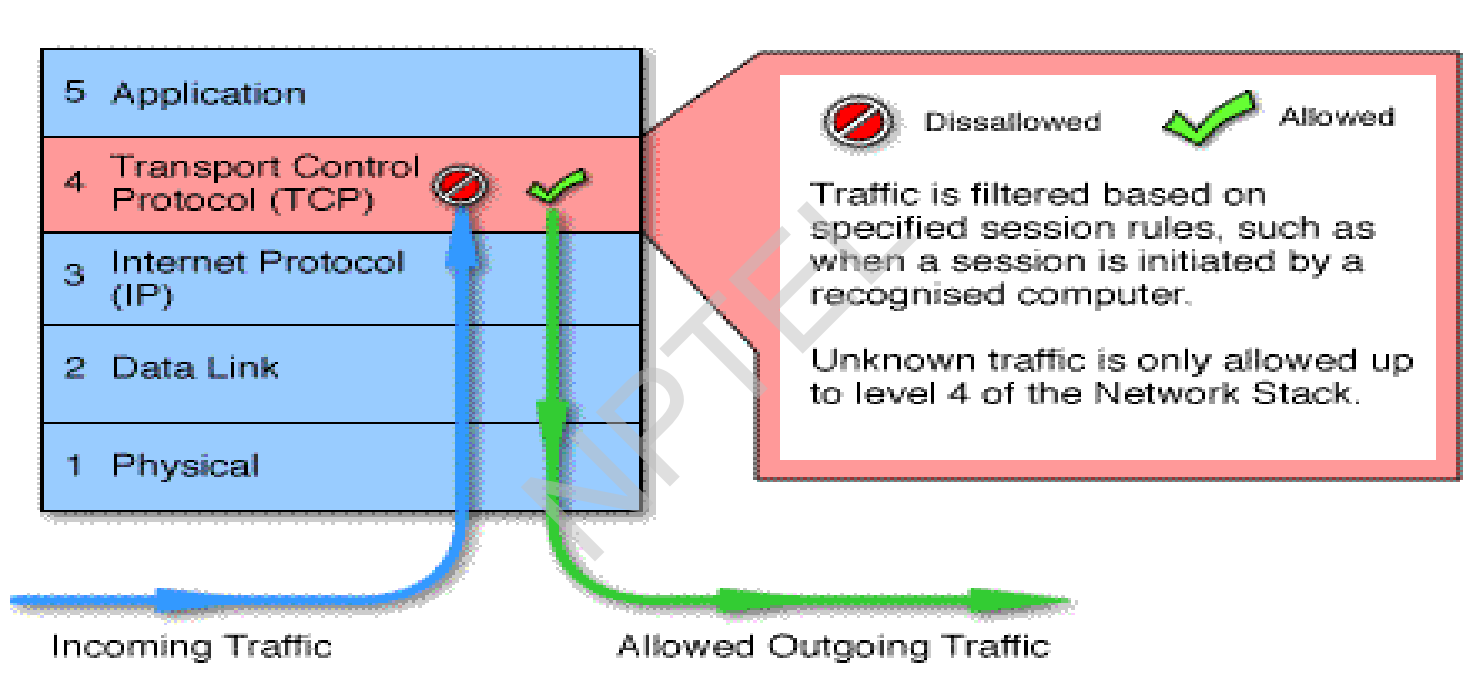
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

# Circuit-Level gateway




- This can be a standalone system / specialized system.
- It does not permit an end-to-end TCP connection; rather the gateway sets up two TCP connections.
- Once the TCP connections are established, the Gateway relays TCP segments from one connection to the other without examining the contents.

# Circuit Level Gateway



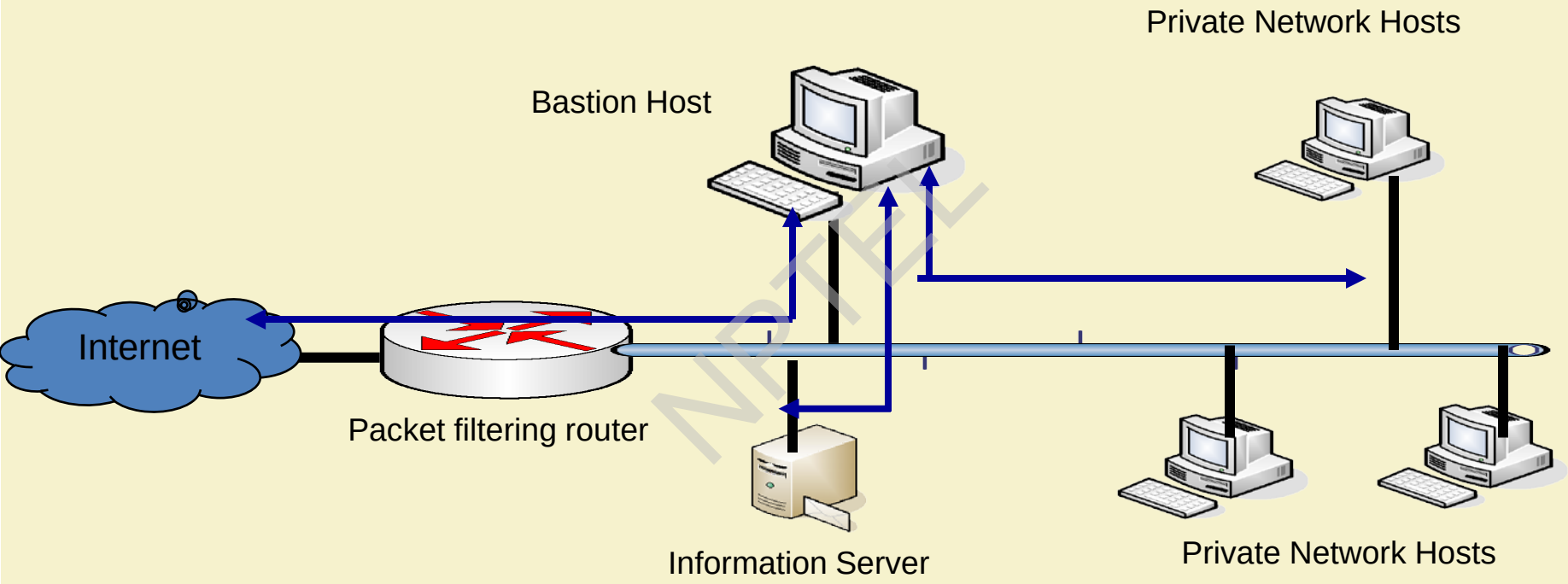
# Circuit-level Gateway (contd.)

- Stand-alone system, or specialized function performed by an Application-level Gateway.
- Sets up two TCP connections:
  - The gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- Typically use is a situation in which the system administrator trusts the internal users.
  - An example is the SOCKS package.

# Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations are in popular use.

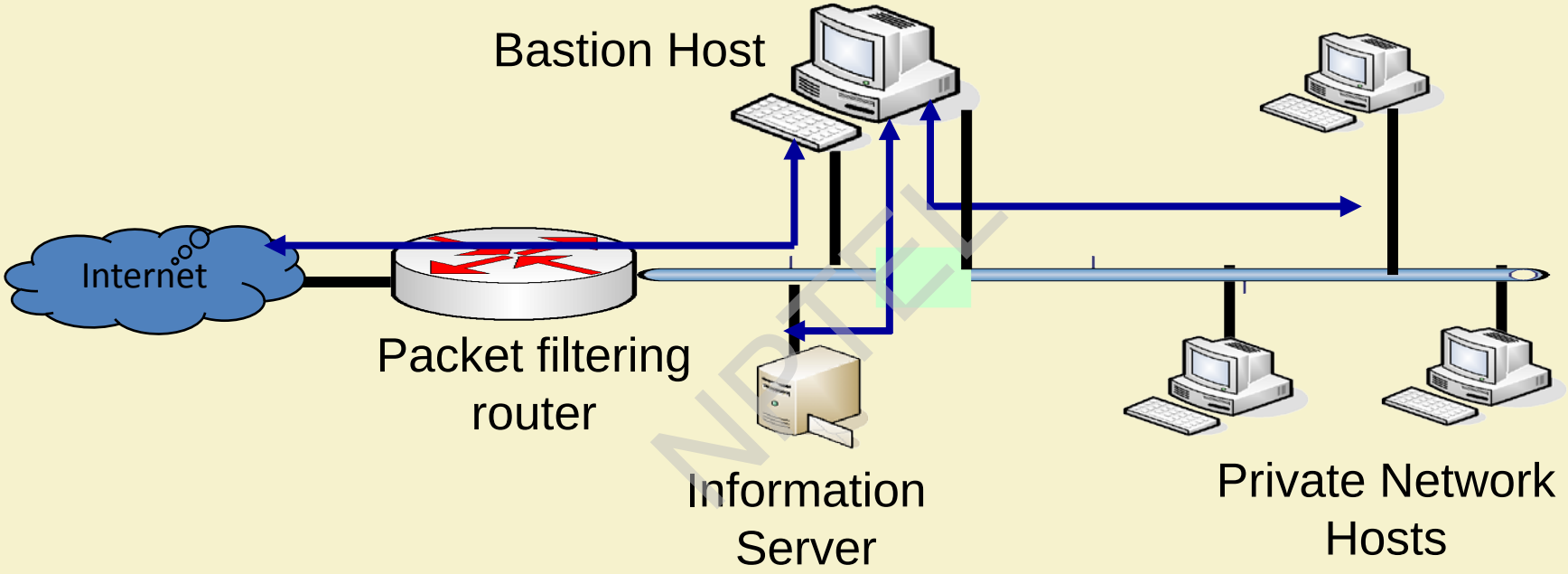
# Screened Host Firewall (Single-homed host)



- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host
- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router.
- The bastion host performs authentication and proxy functions.

- Greater security than single configurations because of two reasons:
  - Implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.

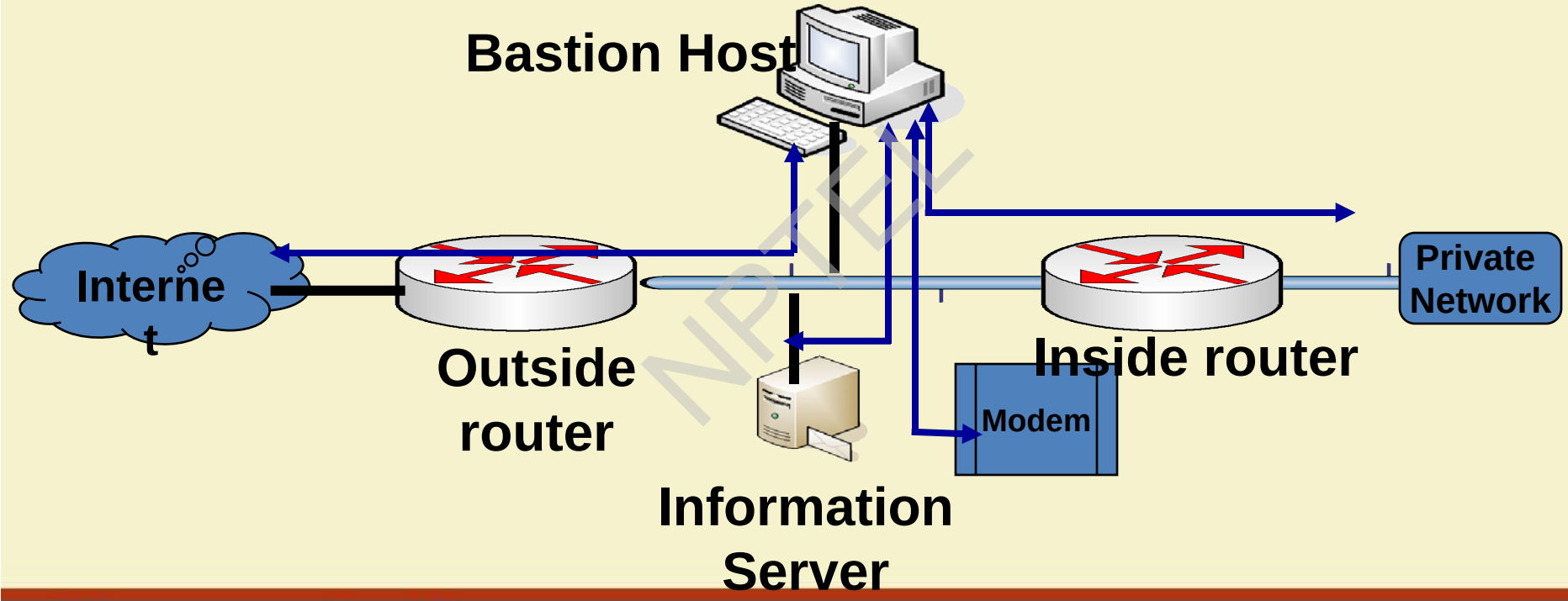
# Screened Host Firewall (dual-homed host)




This configuration physically prevents security breach.

- The packet-filtering router is not completely compromised.
- Traffic between the Internet and other hosts on the private network has to flow through the bastion host.

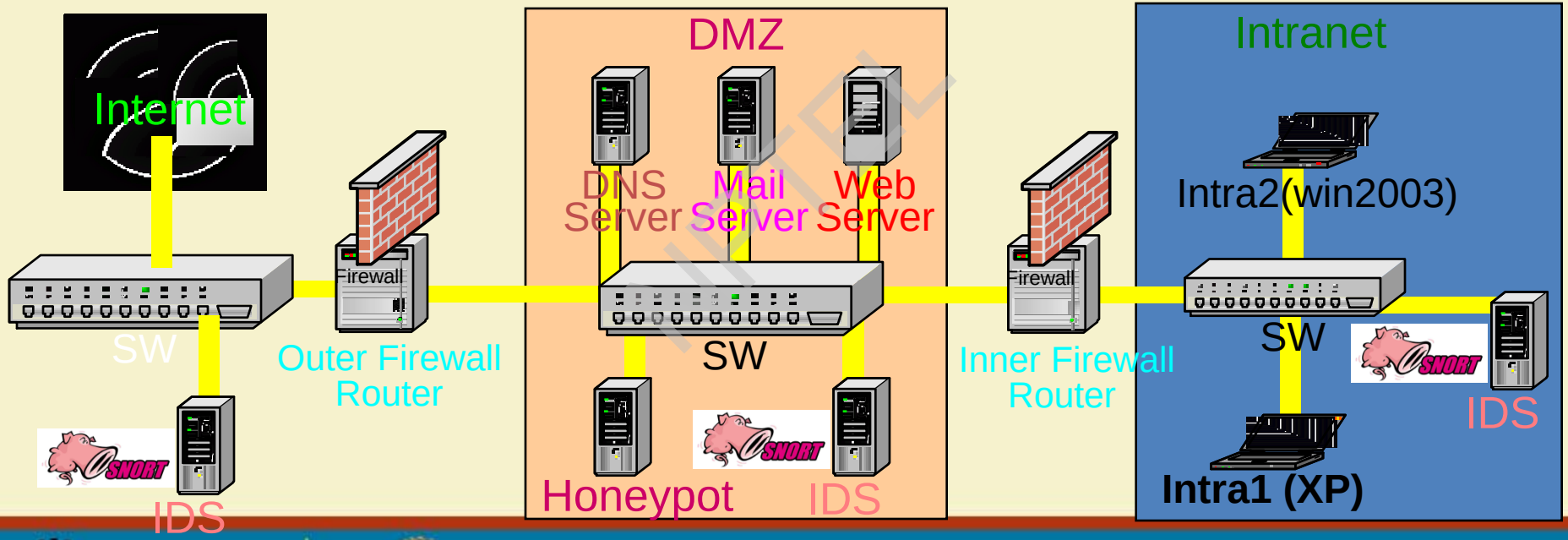
# Screened Subnet Firewall



- Most secure configuration of the three.
- Two packet-filtering routers are used.
- Creation of an isolated sub-network.

- Advantages:
  - Three levels of defense to thwart intruders.
  - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet).
  - The inside router advertises only the existence of the screened subnet to the internal network.
    - The systems on the inside network cannot construct direct routes to the Internet.

# Perimeter Defense and Firewall



thank you!

# COMPUTER NETWORKS AND INTERNET PROTOCOLS

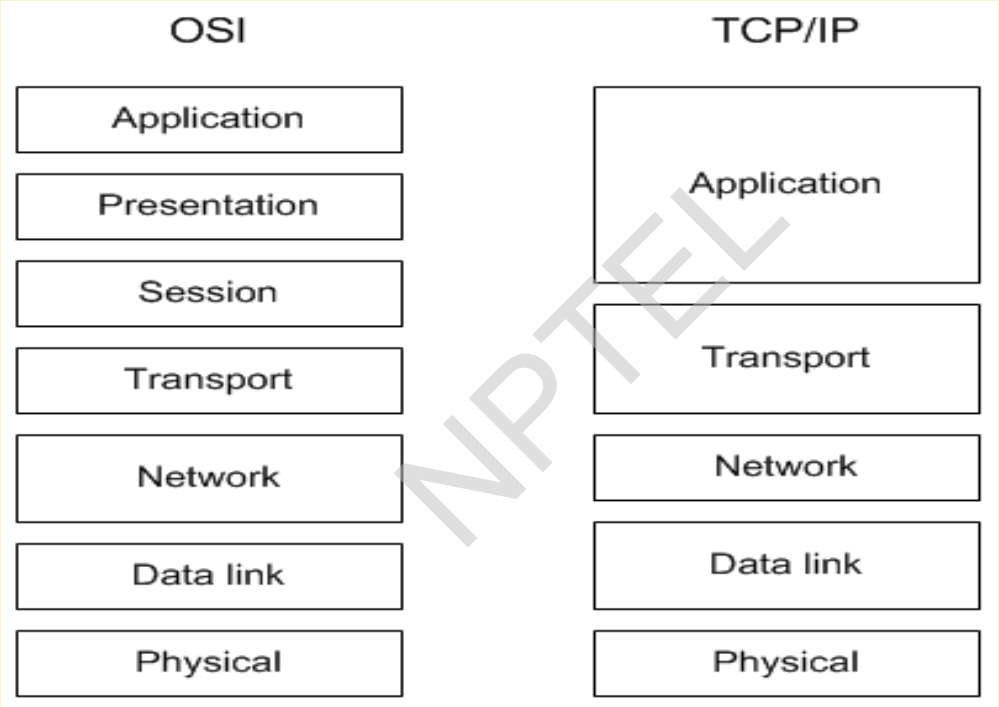
## Network Security – III [TCP/IP Security]



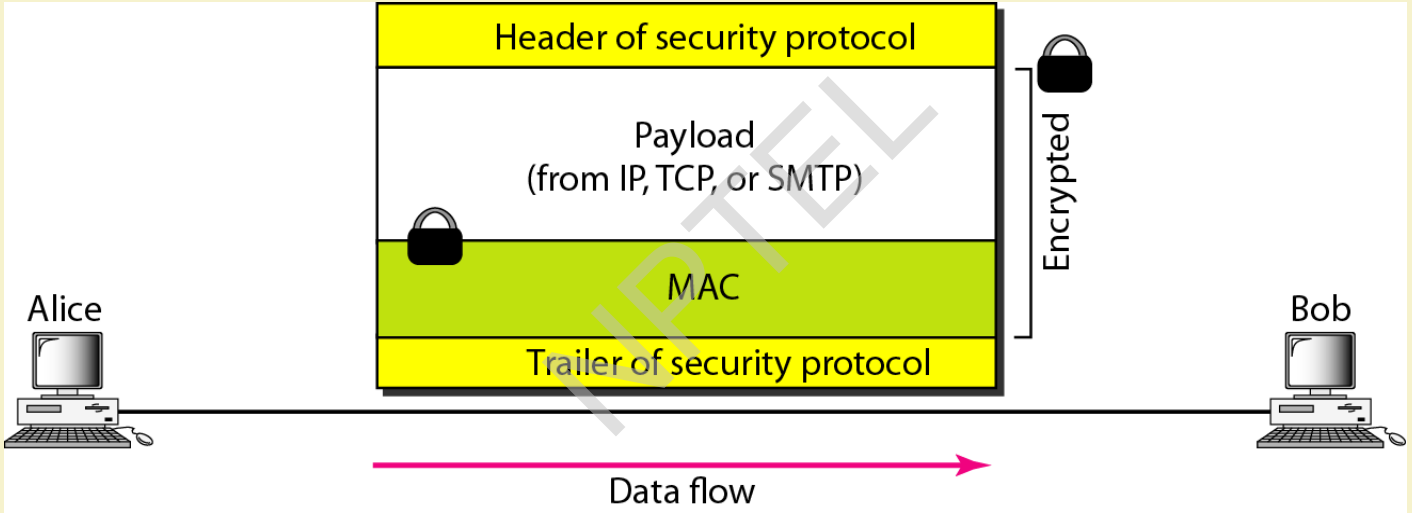
**SOUMYA K GHOSH**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

**SANDIP CHAKRABORTY**
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

# Protocol Stack

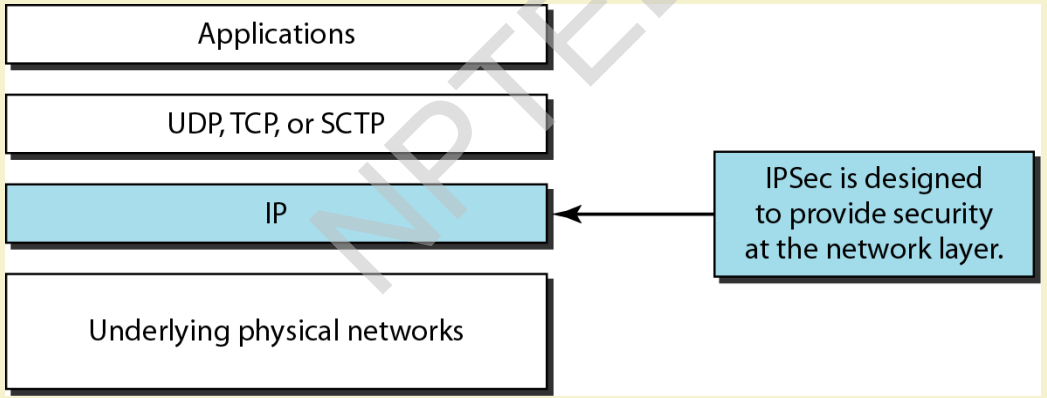


# Common structure of security protocols

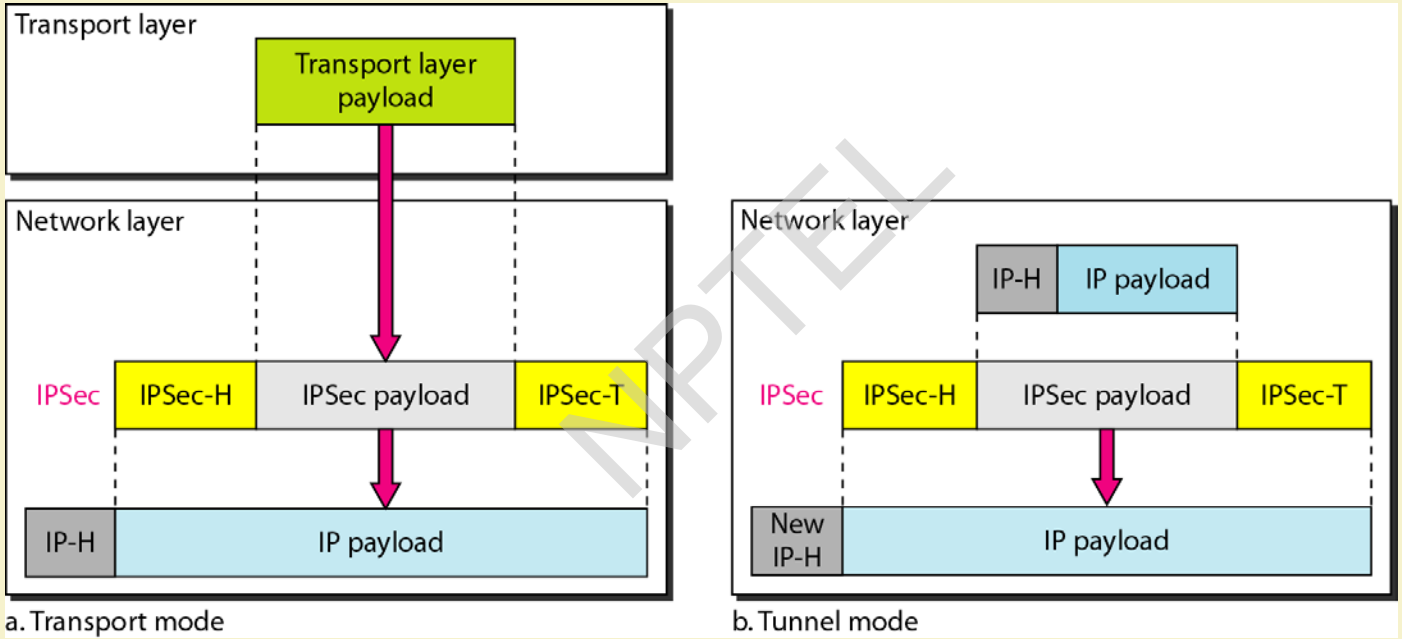


# IPSecurity (IPSec)

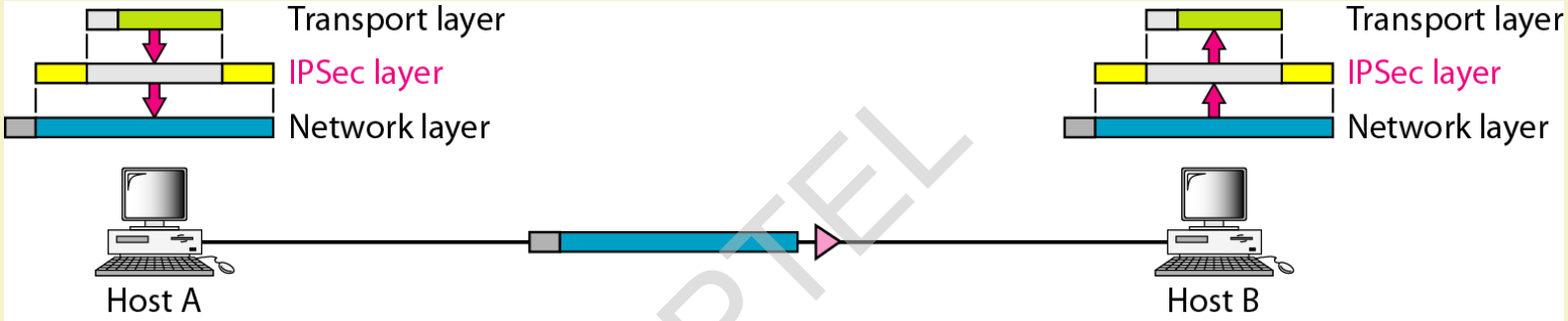
IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.



# IPSec: Transport mode and Tunnel modes

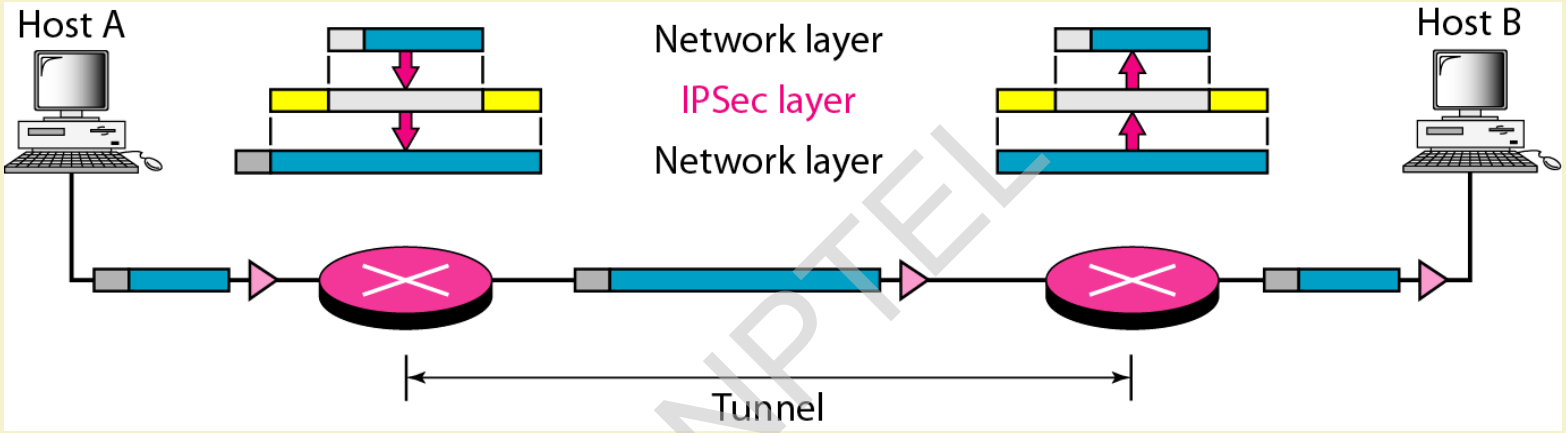


# Transport mode




IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.

# Tunnel mode



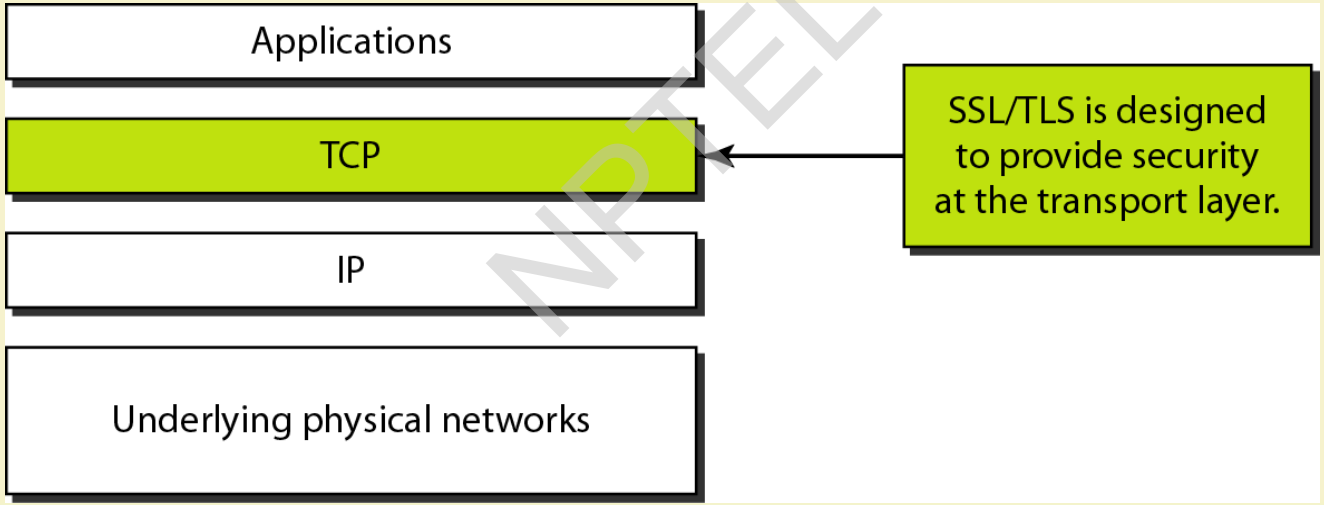

IPSec in tunnel mode protects the original IP header.

# IPSec services

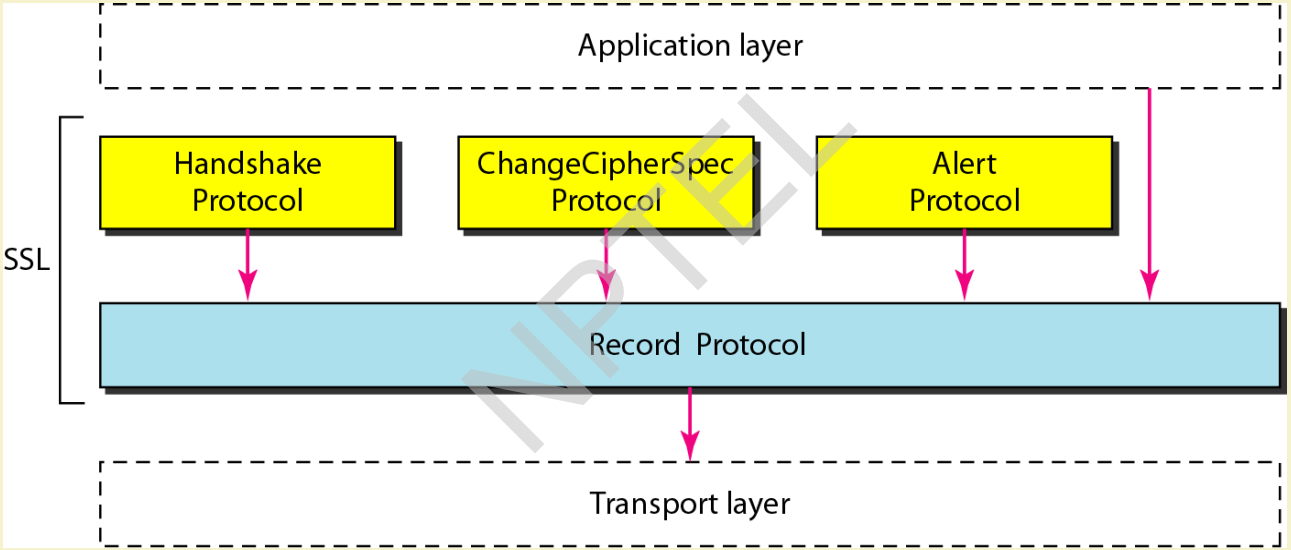
| *Services* | *AH* | *ESP* |
|---|---|---|
| Access control | Yes | Yes |
| Message authentication (message integrity) | Yes | Yes |
| Entity authentication (data source authentication) | Yes | Yes |
| Confidentiality | No | Yes |
| Replay attack protection | Yes | Yes |

# Transport Layer Security: SSL/TLS

Secure Sockets Layer (SSL) Protocol and the Transport Layer Security (TLS) Protocol.

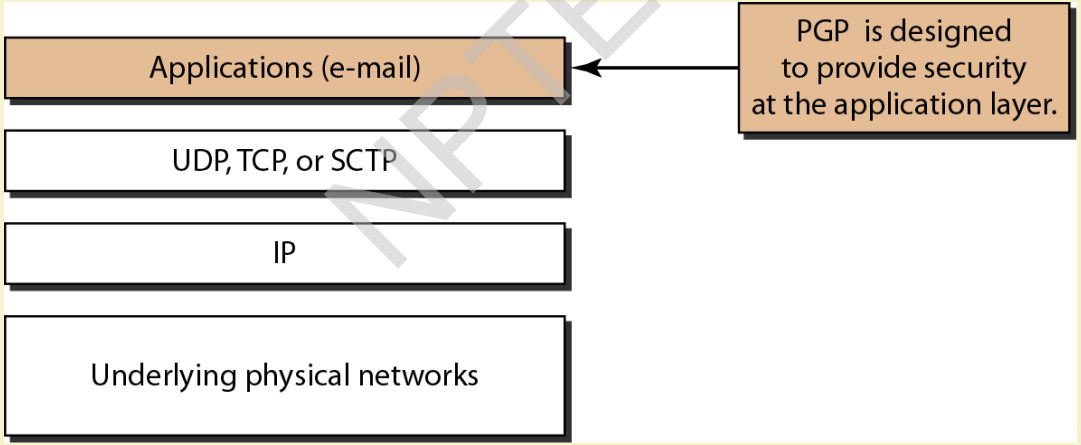


# Four SSL protocols

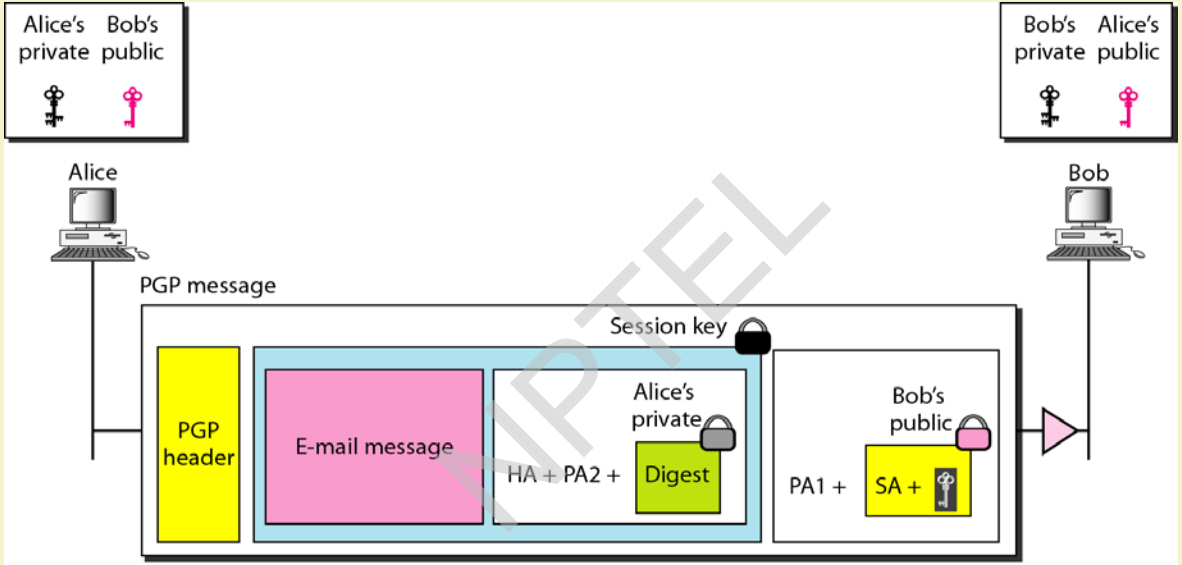


# Application Layer Security: PGP

One of the protocols to provide security at the application layer is Pretty Good Privacy (PGP). PGP is designed to create authenticated and confidential e-mails.



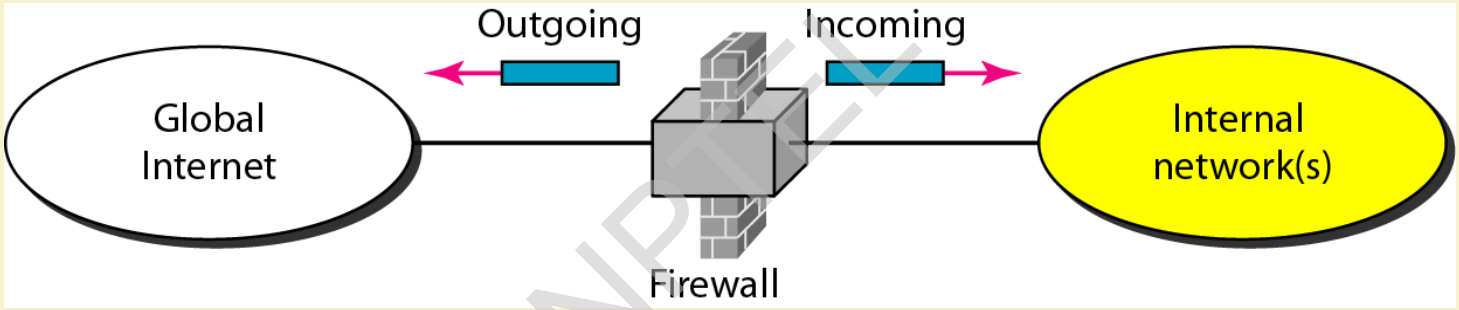
# PGP: E-mail message is authenticated and encrypted




PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

# Firewall

# Firewall - Overview



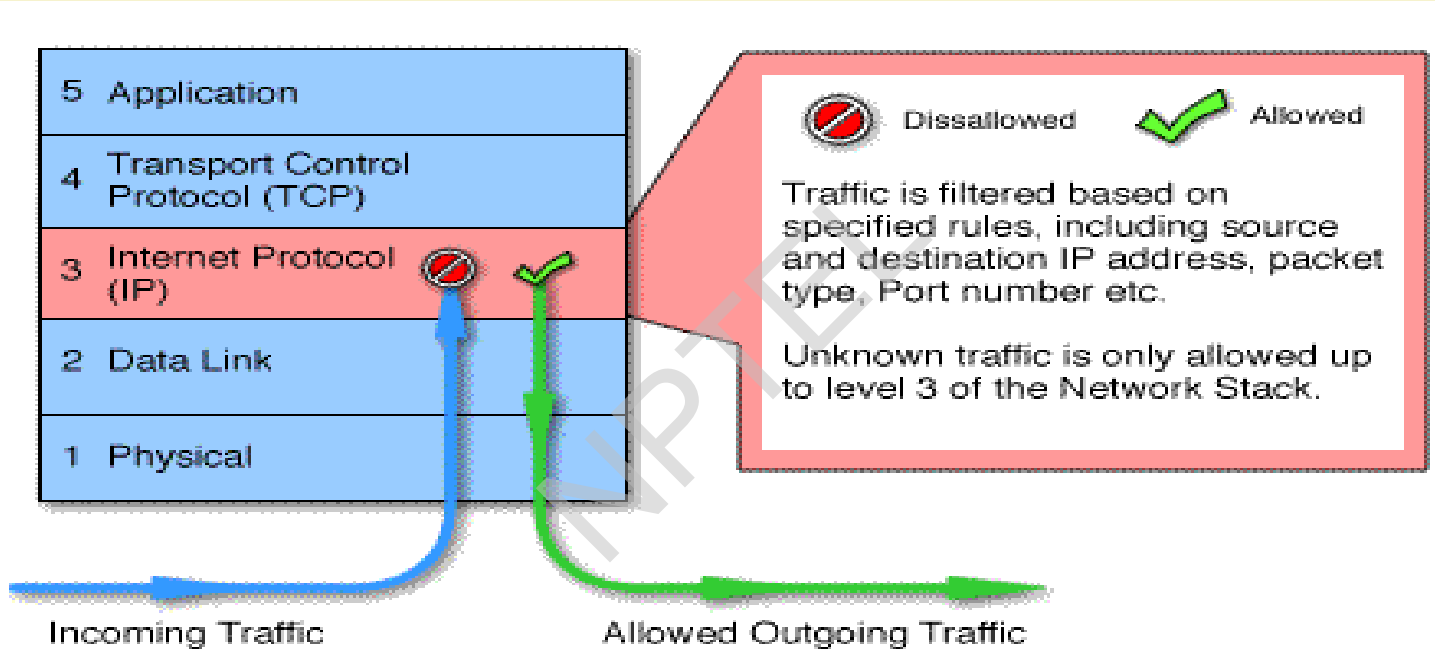
# Firewall

- Firewalls are effective to
  - protect local systems;
  - protect network-based security threats;
  - provide secured and controlled access to Internet;
  - provide restricted and controlled access from the Internet to local servers.

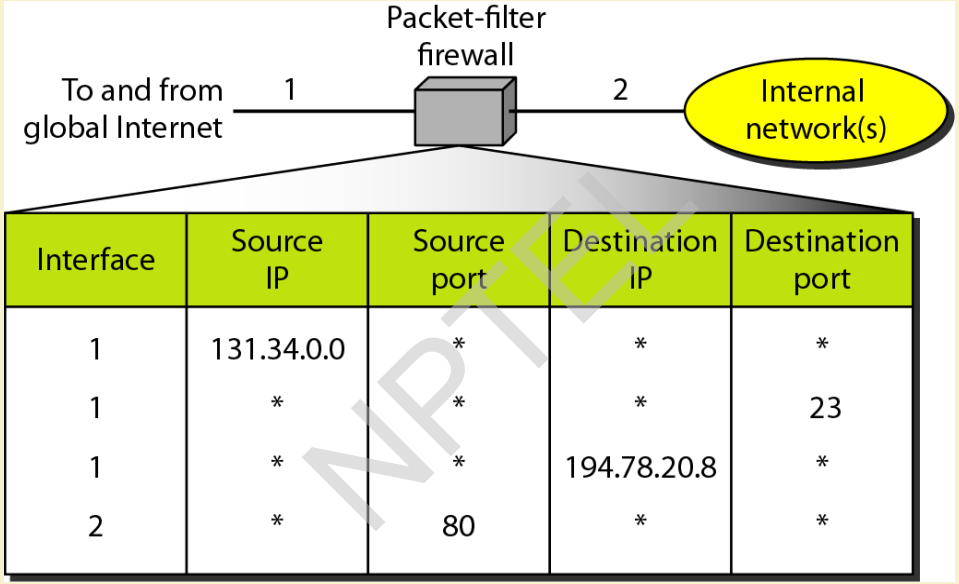
# Types of Firewalls

1. Packet filters
2. Application-level gateways/ Proxy Firewall
3. Circuit-level gateways

# Packet Filtering Firewall



# Packet-filter firewall




| Interface | Source IP | Source port | Destination IP | Destination port |
|---|---|---|---|---|
| 1 | 131.34.0.0 | * | * | * |
| 1 | * | * | * | 23 |
| 1 | * | * | 194.78.20.8 | * |
| 2 | * | 80 | * | * |



A packet-filter firewall filters at the network or transport layer.

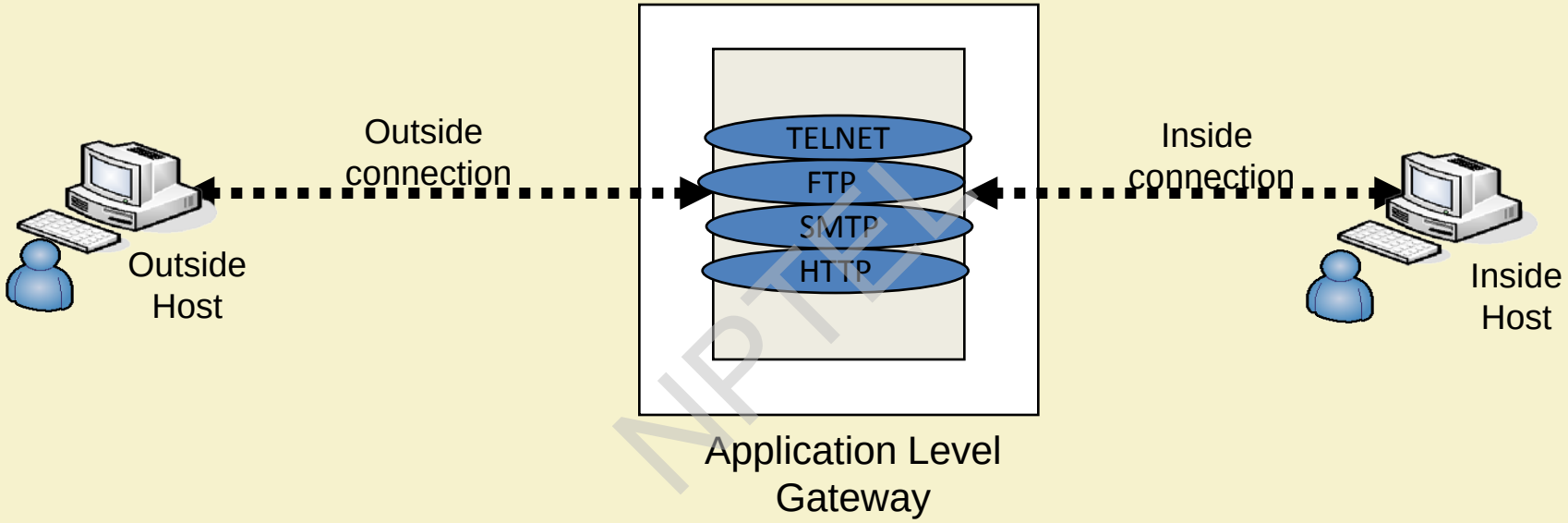
# Packet Filtering Router (contd.)

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
  - Typically based on IP addresses and port numbers.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- Two default policies (discard or forward).

# Packet Filtering Router (contd.)

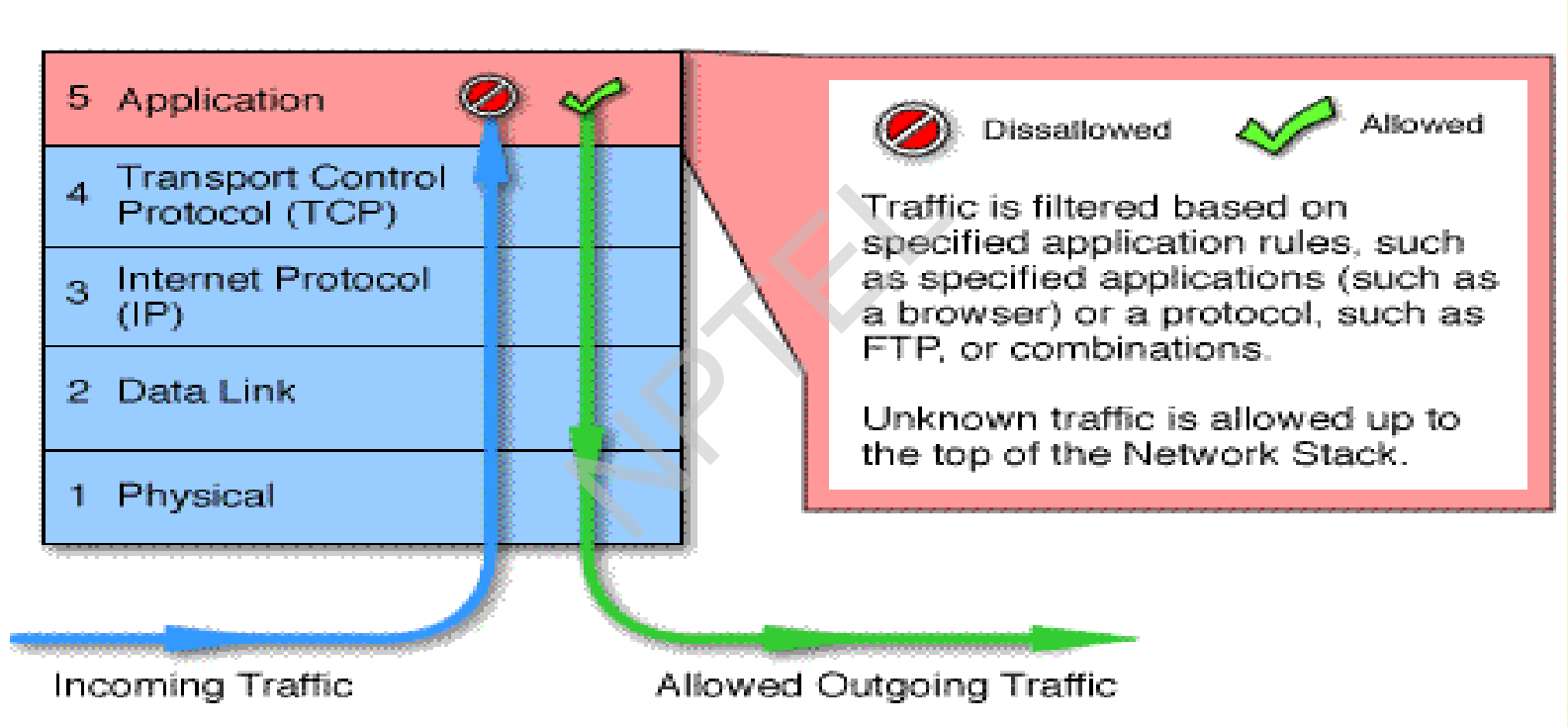
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of authentication

# Application-Level Gateway

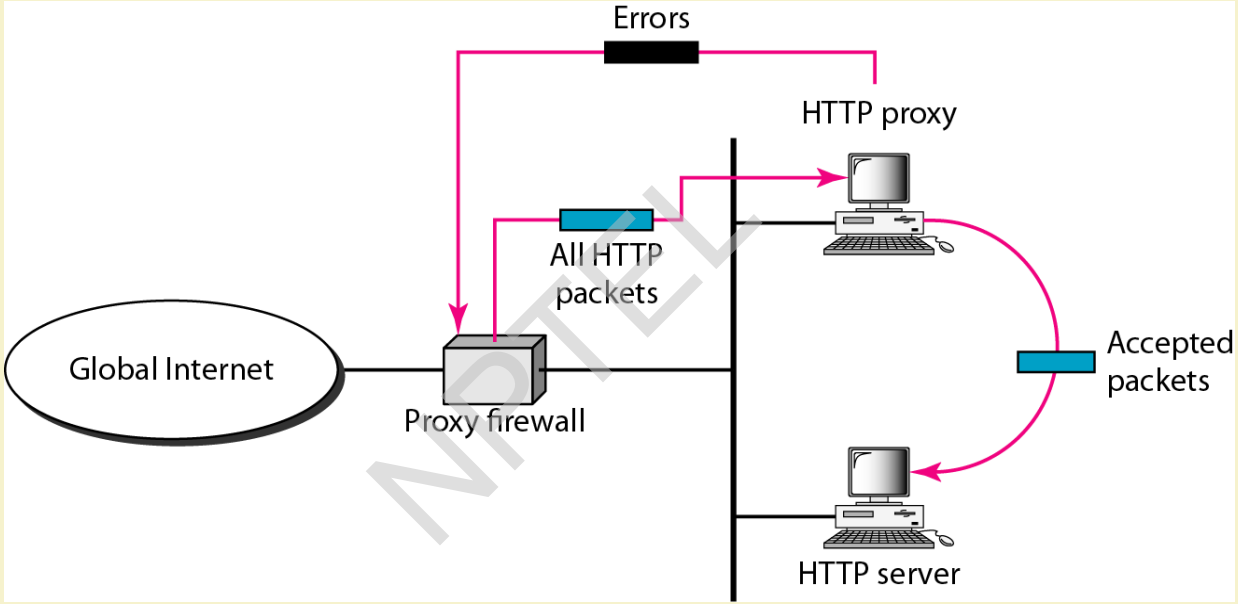



- Also called a Proxy Server; acts as relay of application level traffic.
- It is service specific.

# Application Level Gateway



# Proxy firewall

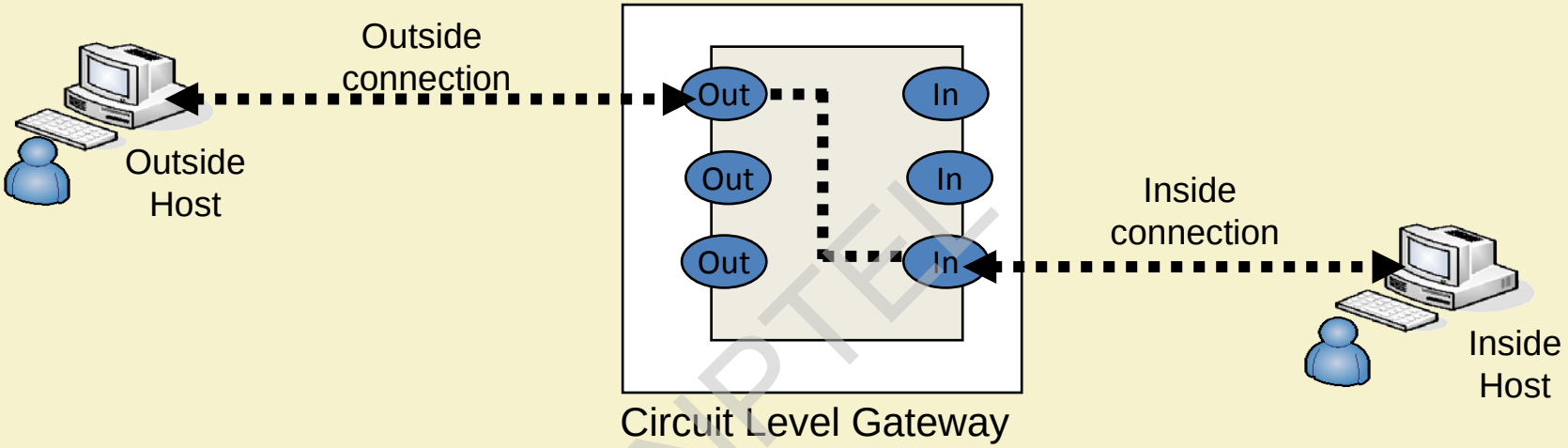



A proxy firewall filters at the application layer.

# Application-level Gateway (contd.)

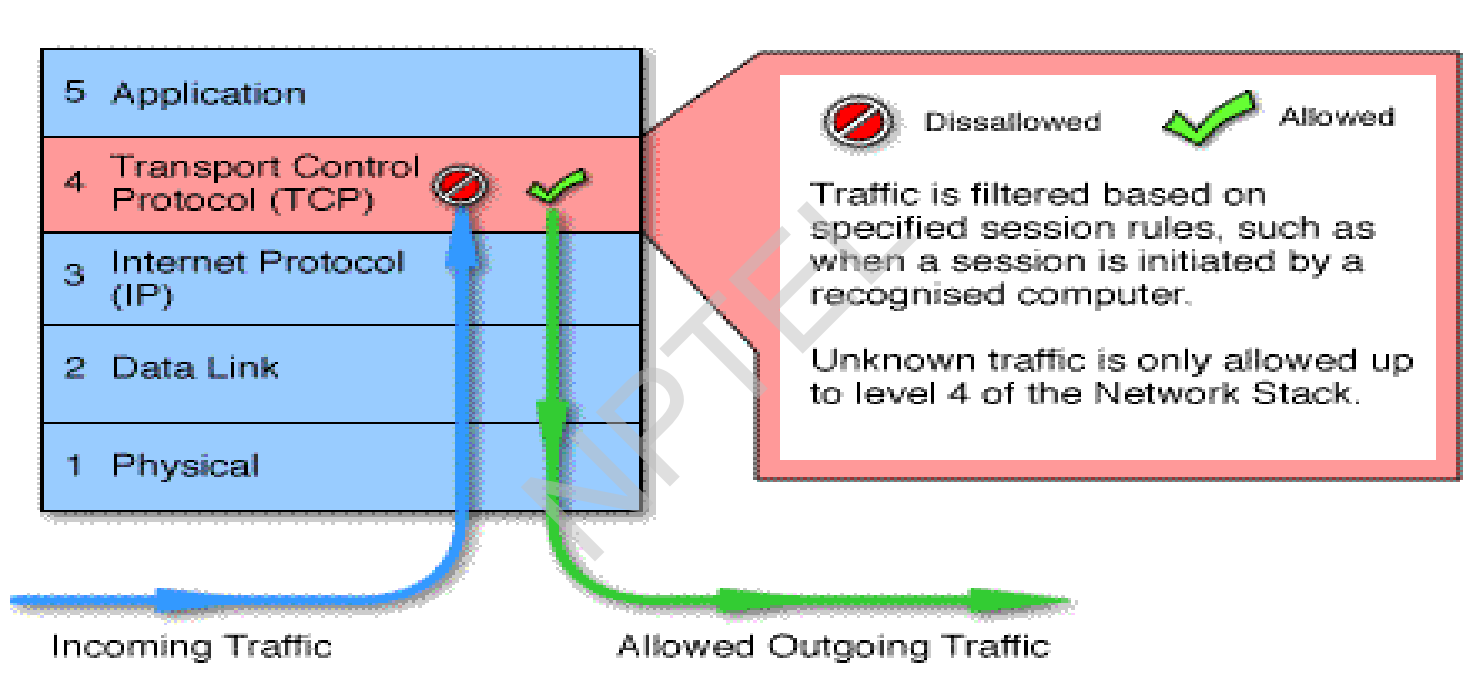
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

# Circuit-Level gateway




- This can be a standalone system / specialized system.
- It does not permit an end-to-end TCP connection; rather the gateway sets up two TCP connections.
- Once the TCP connections are established, the Gateway relays TCP segments from one connection to the other without examining the contents.

# Circuit Level Gateway



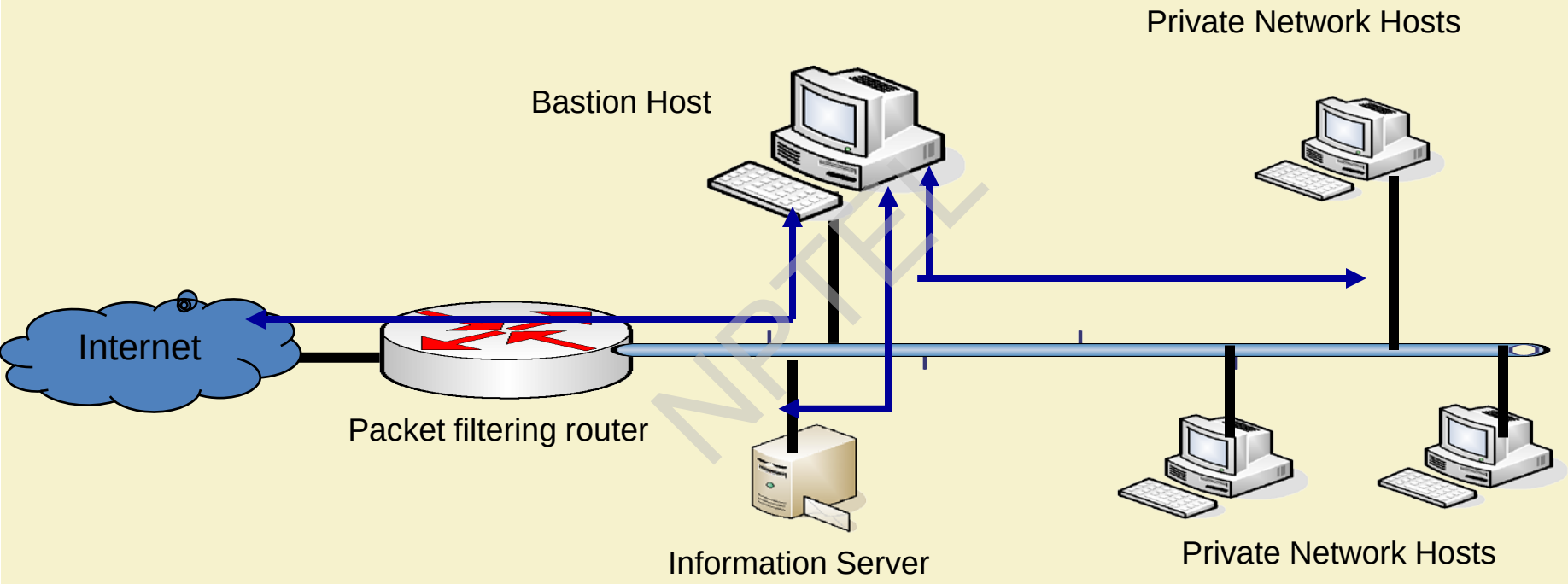
# Circuit-level Gateway (contd.)

- Stand-alone system, or specialized function performed by an Application-level Gateway.
- Sets up two TCP connections:
  - The gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- Typically use is a situation in which the system administrator trusts the internal users.
  - An example is the SOCKS package.

# Firewall Configurations

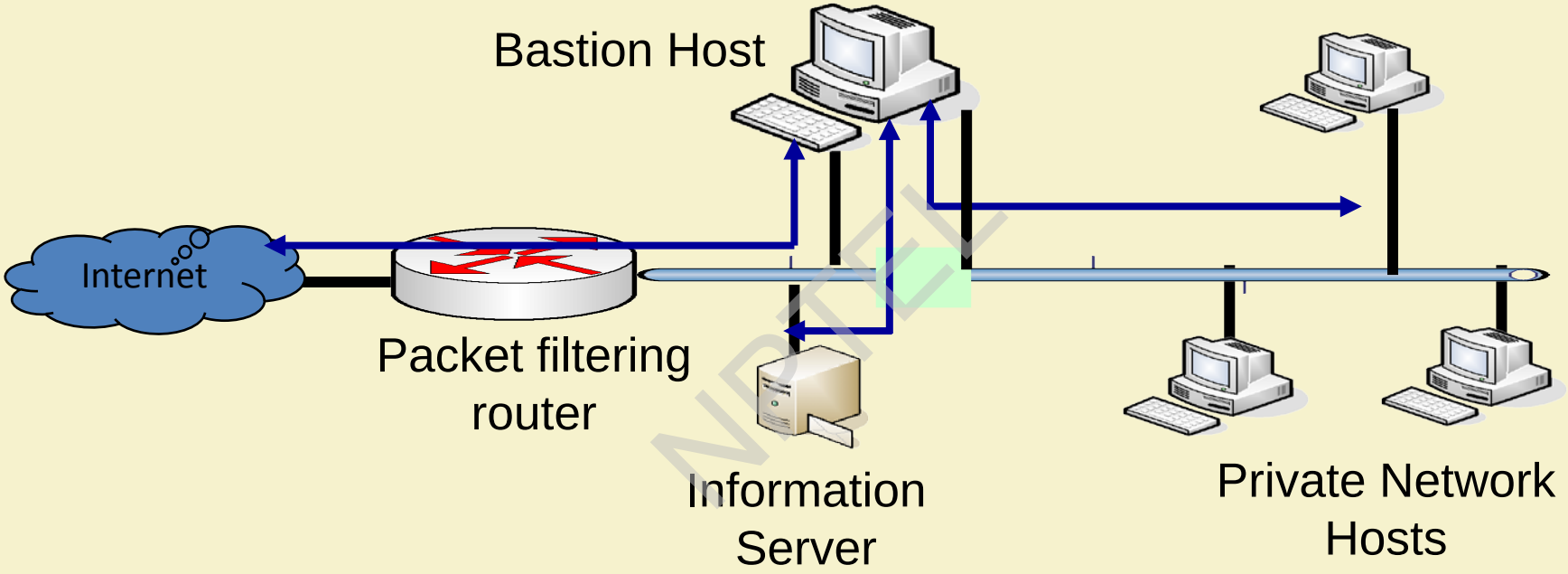
- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations are in popular use.

# Screened Host Firewall (Single-homed host)



- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host
- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router.
- The bastion host performs authentication and proxy functions.
- Greater security than single configurations because of two reasons:
  - Implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.

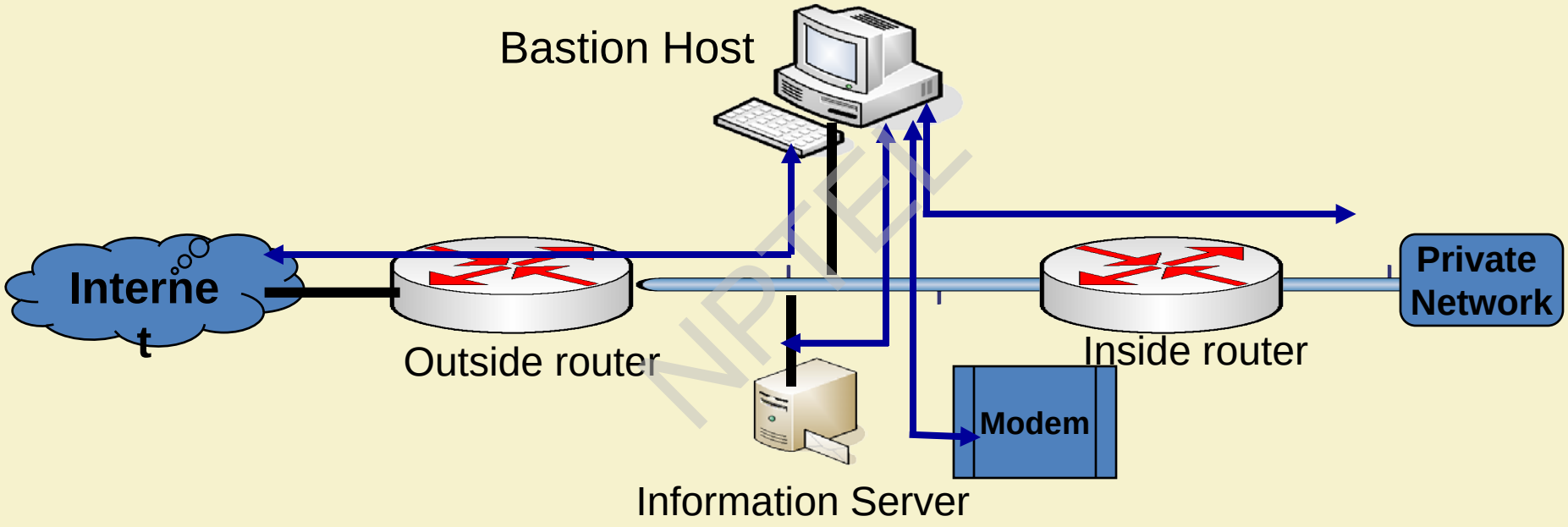
# Screened Host Firewall (dual-homed host)




This configuration physically prevents security breach.

- The packet-filtering router is not completely compromised.
- Traffic between the Internet and other hosts on the private network has to flow through the bastion host.

# Screened Subnet Firewall



# Perimeter Defense and Firewall – Typical Scenario