NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE
(NAAC Accredited)
(Approved by AICTE, Affiliated to KTU University, Kerala)

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

Course Material

S7 - EC407: Computer Communication

2015 Regulations

About the Department:

Department of ECE established in 2002 with an intake of 60 students to undergraduate (B.Tech) programme and enhanced to an intake of 120 students from 2006. The department offers two Postgraduates(M.Tech) programmes in “Electronics”. “Applied Electronics & Communication System” from 2011 with an intake of 18 students and “ VLSI Design” from 2012 with an intake of 18.Highly qualified, experienced and dedicated staff members are the backbone of the Department. The Department always strive hard to satisfy the knowledge thirst of both students and faculties by organizing workshops / technical talks / conferences etc. The faculty members are actively involved in research work and regularly present/ publish their work in various national and international conferences / journals. The ECE Department is proud to host state-of- the art Laboratories in the area of VLSI, Embedded Systems, Microprocessor and Microcontrollers, Circuits, Analog and Digital Communication and Microwave and Optical communication.The ECE department formally inaugurated the ECHOS (The ECE Association) in 2009 and under this banner many extra-academic activities have been conducted such as paper presentation, quiz competition, workshops and seminars. Also the department has two magazines that have been developed on the basis of the creative skills of our imaginative students. There is an Embedded Club that meets on monthly basis to discuss innovative projects and publication based activities. Department is closely associated with INSTITUTE OF ELECTRONICS & TELECOMMUNICATION ENGINEERS (IETE) Palakkad Centre to organize technical events like guest lecture, seminars and conferences.

Vision of the institute:

To mould true citizens who are millennium leaders and catalysts of change through excellence in education.

Mission of the institute:

NCERC is committed to transform itself into a center of excellence in Learning and Research in Engineering and Frontier Technology and to impart quality education to mould technically competent citizens with moral integrity, social commitment and ethical values. We intend to facilitate our students to assimilate the latest technological know-how and to imbibe discipline, culture and spiritually, and to mould them in to technological giants, dedicated research scientists and intellectual leaders of the country who can spread the beams of light and happiness among the poor and the underprivileged.

Vision of the department:

Providing Universal Communicative Electronics Engineers with corporate and social relevance towards sustainable developments through quality education.

Mission of the department:

1) Imparting Quality education by providing excellent teaching, learning environment.

2) Transforming and adopting students in this knowledgeable era, where the electronic gadgets (things) are getting obsolete in short span.

3) To initiate multi-disciplinary activities to students at earliest and apply in their respective fields of interest later.

4) Promoting leading edge Research & Development through collaboration with academia & industry.

Program Educational Objectives (PEOs)

I. To prepare students to excel in postgraduate programmes or to succeed in industry / technical profession through global, rigorous education and prepare the students to practice and innovate recent fields in the specified program/ industry environment.

II. To provide students with a solid foundation in mathematical, Scientific and engineering fundamentals required to solve engineering problems and to have strong practical knowledge required to design and test the system.

III. To train students with good scientific and engineering breadth so as to comprehend, analyze, design, and create novel products and solutions for the real life problems.

IV. To provide student with an academic environment aware of excellence, effective communication skills, leadership, multidisciplinary approach, written ethical codes and the life-long learning needed for a successful professional career.

Program Outcomes (Pos):

1. **Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem Analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of Solutions**: Design solutions for complex engineering problems and design system components or processes that meet t h e specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct Investigations of Complex Problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern Tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The Engineer and Society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and Sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and Team Work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project Management and Finance**: Demonstrate knowledge and understanding of t h e engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long Learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes (PSO):

1. Facility to apply the concepts of Electronics, Communications, Signal processing, VLSI, Control systems etc., in the design and implementation of engineering systems.

2. Facility to solve complex Electronics and communication Engineering problems, using latest hardware and software tools, either independently or in team.

Mapping of PEOs with the Program Outcomes (POs):

The Electronics and Communication Engineering Program outcomes leading to the achievement of the objectives can be summarized in the following Table.

		Program Outcomes										
		a	b	c	d	e	f	g	h	i	j	k
PEOs	1	X	X	X								X
	2	X	X	X	X		X					X
	3		X	X	X	X					X	
	4				X	X	X	X	X	X	X	X

Course Outcome:

After completion of this course the students will be able to

01. Different types of network topologies and protocols
02. The layers of the OSI model and TCP/IP with their functions.
03. The concept of subnetting and routing mechanisms
04. The basic protocols of computer networks, and how they can be used to assist in network design and implementation.
05. Security aspects in designing a trusted computer communication system.
06. Knowing the Security System, Common Attacks, Defence and Counter Measures in different layers in OSI Model.

CO-PO Mapping

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1							1	2	
CO2	2	3			2					1	2	
CO3	2	3	2		1					1	2	
CO4	2	3								1	2	
CO5		3			2					1	2	
CO6		2	2		3					1	2	

LESSON PLAN:

1. Introduction to computer communication: Transmission modes - serial and parallel transmission

2. Asynchronous, synchronous, simplex, half duplex, full duplex communication.

3. Switching: circuit switching and packet switching.

4. Networks: Network criteria, physical structures, network models, categories of networks

5. Interconnection of Networks: Internetwork

6. Network models: Layered tasks, OSI model, Layers in OSI model, TCP/IP protocol suite

7. Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP, STP, Fiber optic cable)

8. Data Link Layer: Framing, Flow control (stop and wait, sliding window flow control)

9. Error control, Error detection (check sum, CRC)

10. Bit stuffing, HDLC

11. Media access control: Ethernet (802.3), CSMA/CD

12. Logical link control, Wireless LAN (802.11)

13. CSMA/CA

14. Network Layer Logical addressing: IPv4 & IPV6

15. Address Resolution protocols (ARP, RARP)

16. Subnetting, Classless Routing (CIDR)

17. ICMP, IGMP

18. DHCP Virtual

19. LANNetworking devices (Hubs, Bridges & Switches)

20. Routing: Routing and Forwarding

21. Static routing and Dynamic routing

22. Routing Algorithms: Distance vector routing algorithm,

23. Link state routing (Dijkstra's algorithm)
24. Routing Protocols: Routing Information protocol (RIP),
25. Open Shortest Path First (OSPF),
26. Border Gateway Protocol (BGP)
27. MPL
28. Transport Layer –UDP, TCP
29. Congestion Control & Quality of Service
30. Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics
31. Application Layer – DNS, Remote Logging (Telnet), HTTP, POP3,
32. MIME, SNMP
33. SMTP, FTP, WWW,
34. Introduction to information system security
35. common attacks Security at Application Layer (E-MAIL, PGP and S/MIME).
36. Security at Transport Layer (SSL and TLS).
37. Security at Network Layer (IPSec).
38. Defence and counter measures: Firewalls and their types.
39. DMZ, Limitations of firewalls,
40. Intrusion Detection Systems -Host based,
41. Network based, and Hybrid IDSs
42. Applications of information security system

Assignment Questions:

1. Explain the Transmission modes

2. Describe the different Network models

3. Explain transport layer in the Internet model?

4. Explain spanning tree algorithm. Why is it used?

5. Define random access and explain pure ALOHA & Slotted ALOHA protocols in this category.

6. Explain network layer in the Internet model?

7. Create a system of three LANs with four bridges. The bridges (B 1 to B4) connect the LANs as follows:

a. B1 connects LAN 1 and LAN 2. b. B2 connects LAN 1 and LAN 3.

c. B3 connects LAN 2 and LAN 3. d. B4 connects LAN 1, LAN 2, and LAN 3.

8. Choose B1 as the root bridge. Show the forwarding and blocking ports, after applying the spanning tree procedure.

9. 3. Define controlled access and explain polling and reservation protocol in this category.

10. Explain window adjustment in TCP.

11. Explain how TCP flow control works

12. What is IP Security? Give the overview and explain the fields of IPV6 header with neat diag.

13. Mention the functions of MAC and LLC layers.

14. Explain the functions of UDP & TCP.

15.Write short notes on E-Mail, SSL, IPsec.

Question Bank

Module 1

1. Explain the Transmission modes.
2. Differentiate serial and parallel communication.
3. Which are the different types of serial communication?
4. What are the important criterion for networking?

Module 2

1. Explain the different layers in the networking
2. What is Guided and unguided transmission media?
3. What is bit stuffing?
4. Explain HDLC
5. Write short note on

a. Ethernet (802.3)

b. CSMA/CD

c. Logical link control

d. Wireless LAN (802.11)

e. CSMA/CA

Module 3

1. Explain IPv4 & IPV6
2. Give short note on Address Resolution protocols (ARP, RARP)
3. What is Subnetting?
4. Explain the different Classless Routing
5. Explain the various Networking devices

Module 4

1. What is Routing?
2. What is Forwarding?
3. Differentiate Static routing and Dynamic routing
4. Explain the various Routing Algorithms:
5. Explain the Routing Protocols:

a. Routing Information protocol (RIP),

b. Open Shortest Path First (OSPF),

c. Border Gateway Protocol (BGP),

d. MPLS

Module 5

1. Explain the Transport Layer.
2. Differentiate UDP and TCP
3. What is Congestion Control?
4. What are the characteristics of flow?
5. What is QoS?
6. Write short note on a. DNS b. Remote Logging (Telnet) c. SMTP,

   d. FTP e. WWW, f. HTTP, g. POP3 h. MIME & i. SNMP

Module 6

1. Explain the Security at Application Layer.
2. Explain the Security at Network Layer (IPSec).
3. What are the Defence and counter measures?
4. What are Firewalls and which are their types?
5. Explain the Intrusion Detection Systems.

COURSE CODE	COURSE NAME	L-T-P-C	YEAR OF INTRODUCTION
EC407	COMPUTER COMMUNICATION	3-0-0-3	2016

Prerequisite: NIL

Course objectives:

- To give the basic concepts of computer network and working of layers, protocols and interfaces in a computer network.
- To introduce the fundamental techniques used in implementing secure network communications and give them an understanding of common threats and its defences.

Syllabus: Introduction to computer communication, Transmission modes, Networks, Interconnection of Networks: Internetwork, Network models: OSI model, TCP/IP protocol suite. Physical Layer, Data Link Layer, Media access control, Ethernet(802.3), Logical link control, Logical addressing: IPV4, IPV6, Subnetting, CIDR, ICMP, IGMP, DHCP, Routing, Transport Layer, Congestion Control & Quality of Service, Application Layer, Introduction to system and network security, security attacks, Firewalls, Intrusion detection systems.

Expected outcome:

The students will have a thorough understanding of:

i. Different types of network topologies and protocols.
ii. The layers of the OSI model and TCP/IP with their functions.
iii. The concept of subnetting and routing mechanisms.
iv. The basic protocols of computer networks, and how they can be used to assist in network design and implementation.
v. Security aspects in designing a trusted computer communication system.

Text Books:

1. Behrouz A. Forouzan, Cryptography & Network Security , , IV Edition, Tata McGraw-Hill, 2008
2. J F Kurose and K W Ross, Computer Network A Top-down Approach Featuring the Internet, 3/e, Pearson Education, 2010

References:

1. Behrouz A Forouzan, Data Communications and Networking, 4/e, Tata McGraw-Hill, 2006.
2. Larry Peterson and Bruce S Davie: Computer Network- A System Approach, 4/e, Elsevier India, 2011.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson Education, 2005.
4. Achyut S.Godbole, Data Communication and Networking, 2e, McGraw Hill Education New Delhi, 2011

Course Plan

Module	Course content (42 hrs)	Hours	End Sem. Exam Marks
I	Introduction to computer communication: Transmission modes - serial and parallel transmission, asynchronous, synchronous, simplex, half duplex, full duplex communication. Switching: circuit switching and packet switching	2	15%

	Networks: Network criteria, physical structures, network models, categories of networks, Interconnection of Networks: Internetwork	2	
	Network models: Layered tasks, OSI model, Layers in OSI model, TCP/IP protocol suite.	2	
II	Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable)	2	15%
	Data Link Layer: Framing, Flow control (stop and wait , sliding window flow control)	2	
	Error control, Error detection(check sum, CRC), Bit stuffing, HDLC	2	
	Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA	2	
FIRST INTERNAL EXAM			
III	Network Layer Logical addressing : IPv4 & IPV6	2	15%
	Address Resolution protocols (ARP, RARP)	2	
	Subnetting, Classless Routing(CIDR), ICMP, IGMP, DHCP	3	
	Virtual LAN, Networking devices (Hubs, Bridges & Switches)	1	
IV	Routing: Routing and Forwarding, Static routing and Dynamic routing	1	15%
	Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm)	2	
	Routing Protocols: Routing Information protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS	3	
SECOND INTERNAL EXAM			
V	Transport Layer –UDP, TCP	1	20%
	Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics	4	
	Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP	3	
VI	Introduction to information system security, common attacks	1	20%
	Security at Application Layer (E-MAIL, PGP and S/MIME). Security at Transport Layer (SSL and TLS). Security at Network Layer (IPSec).	3	
	Defence and counter measures: Firewalls and their types. DMZ, Limitations of firewalls, Intrusion Detection Systems -Host based, Network based, and Hybrid IDSs	2	
END SEMESTER EXAM			

Question Paper Pattern

The question paper shall consist of three parts. Part A covers modules I and II, Part B covers modules III and IV, and Part C covers modules V and VI. Each part has three questions uniformly covering the two modules and each question can have maximum four subdivisions. In each part, any two questions are to be answered. Mark patterns are as per the syllabus with 90% for theory and 10% for logical/numerical problems, derivation and proof.

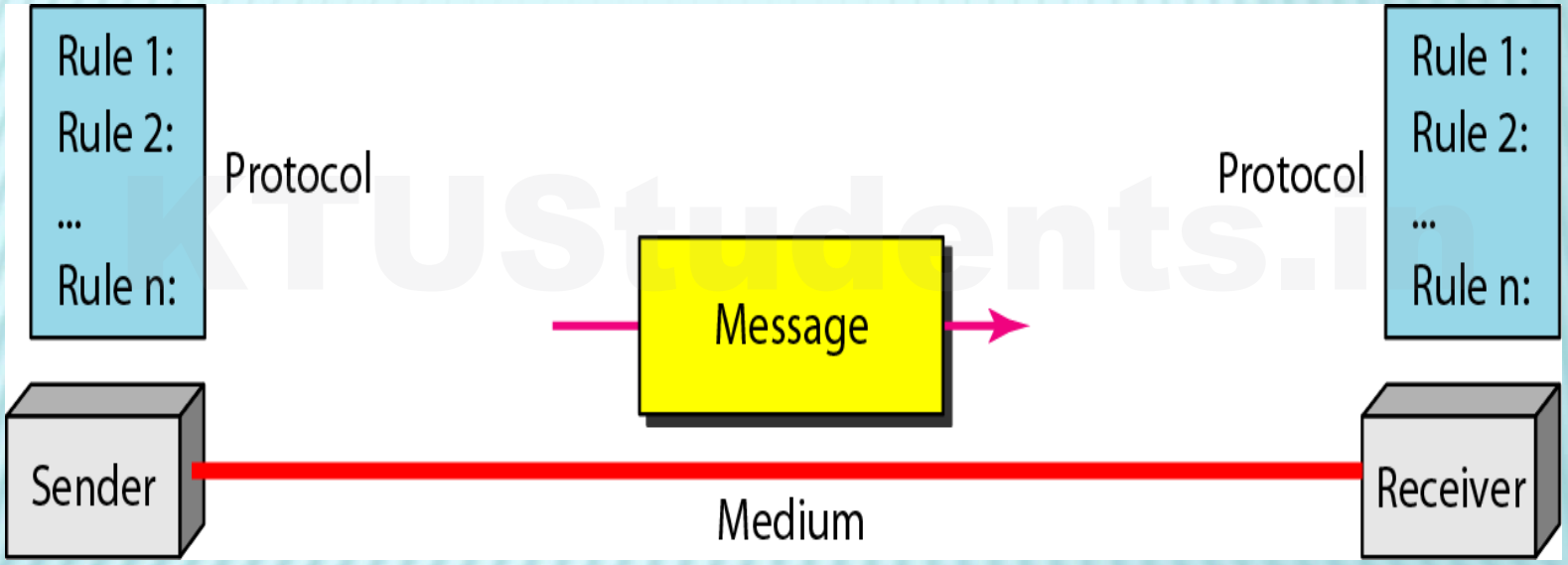
KTUStudents.in

INTRODUCTION TO COMPUTER COMMUNICATION

MOD 1

- Data communications is the exchange of data between two devices via some form of transmission medium.
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

SYSTEM


Rule 1:
Rule 2:
...
Rule n:
Protocol
Message
Protocol
Rule 1:
Rule 2:
...
Rule n:
Sender
Medium
Receiver

1. Message. The message is the information (data) to be communicated.
2. Sender. The sender is the device that sends the data message.
3. Receiver. The receiver is the device that receives the message.
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver.

5. Protocol - A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

KTUStudents.in

MODES OF TRANSMISSION

1. serial and parallel
2. Synchronous and asynchronous
3. Simplex , half duplex and full duplex

KTUStudents.in

NETWORK

- A network is a set of devices (*nodes) connected by communication* links.
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- Most networks use distributed processing, in which a task is divided among multiple computers.

NETWORK CRITERIA

1. *Performance*

- Performance can be measured in transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another.
- Response time is the elapsed time between an inquiry and a response.

2. Reliability

- network reliability is measured by the frequency of failure,OR the time it takes a link to recover from a failure

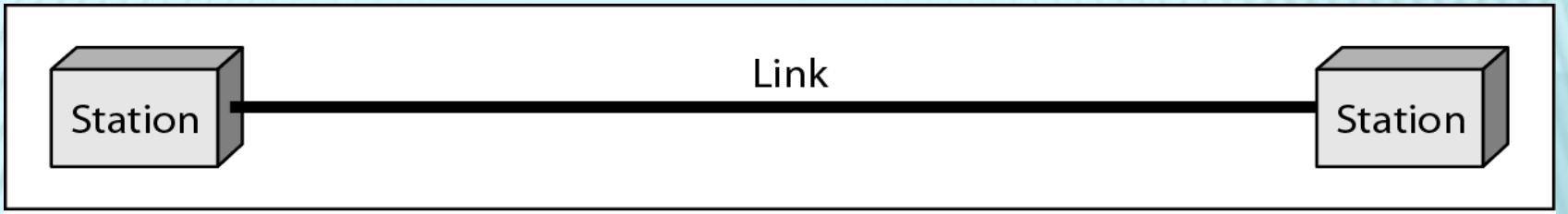
3. Security

- Network security issues :
- include protecting data from unauthorized access,
- protecting data from damage and development,
- implementing policies and procedures for recovery from breaches and data losses.

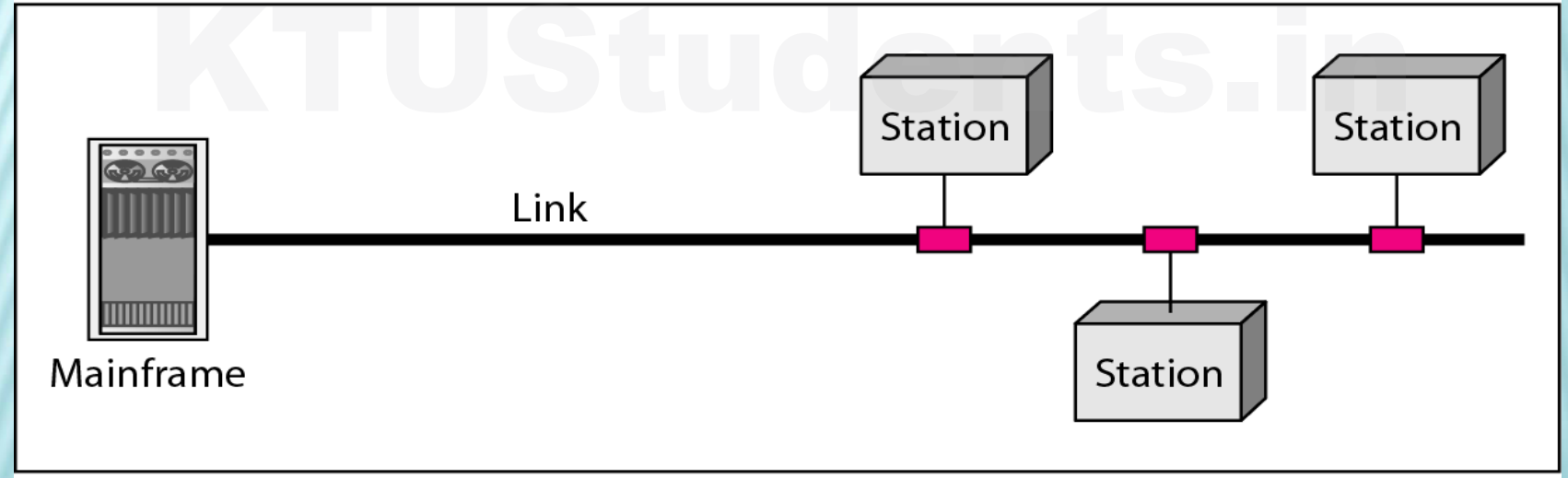
PHYSICAL STRUCTURE

- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.

1. Point-to-Point - A point-to-point connection provides a dedicated link between two devices.
2. Multipoint - A multipoint connection is one in which more than two specific devices share a single link. Types: spatial ,time shared



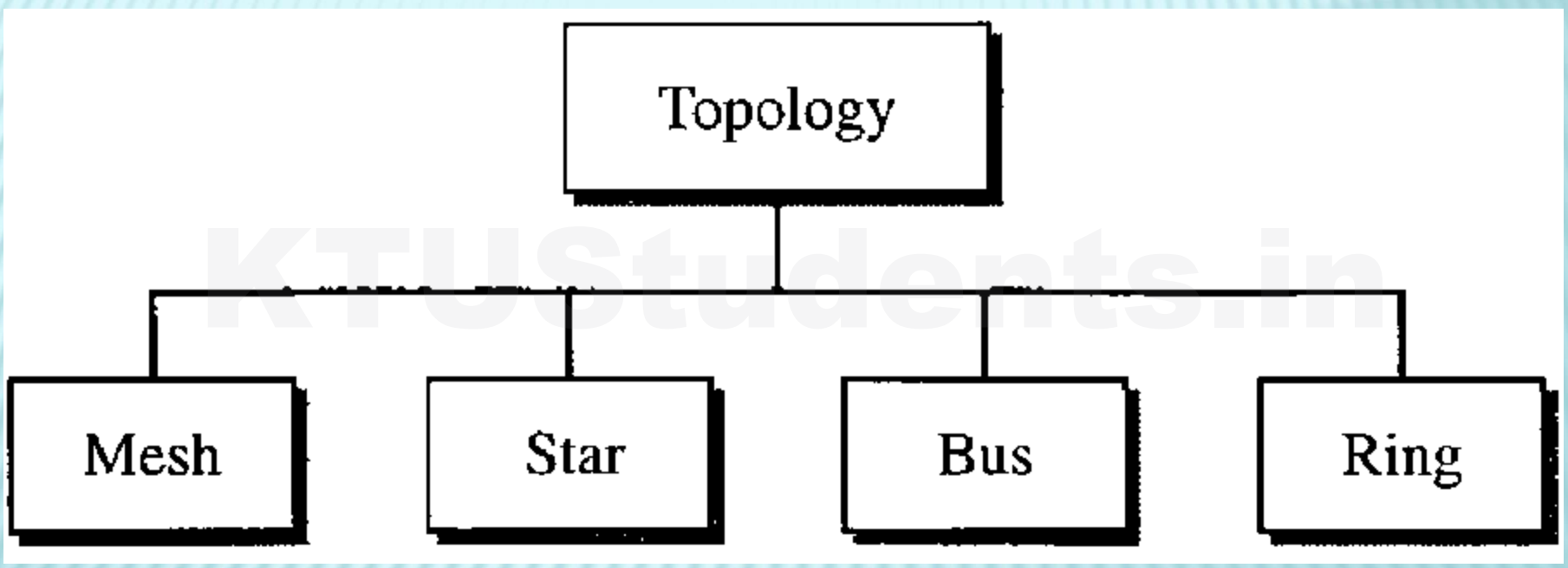
a. Point-to-point



b. Multipoint

KTUStudents.in

NETWORK TOPOLOGIES

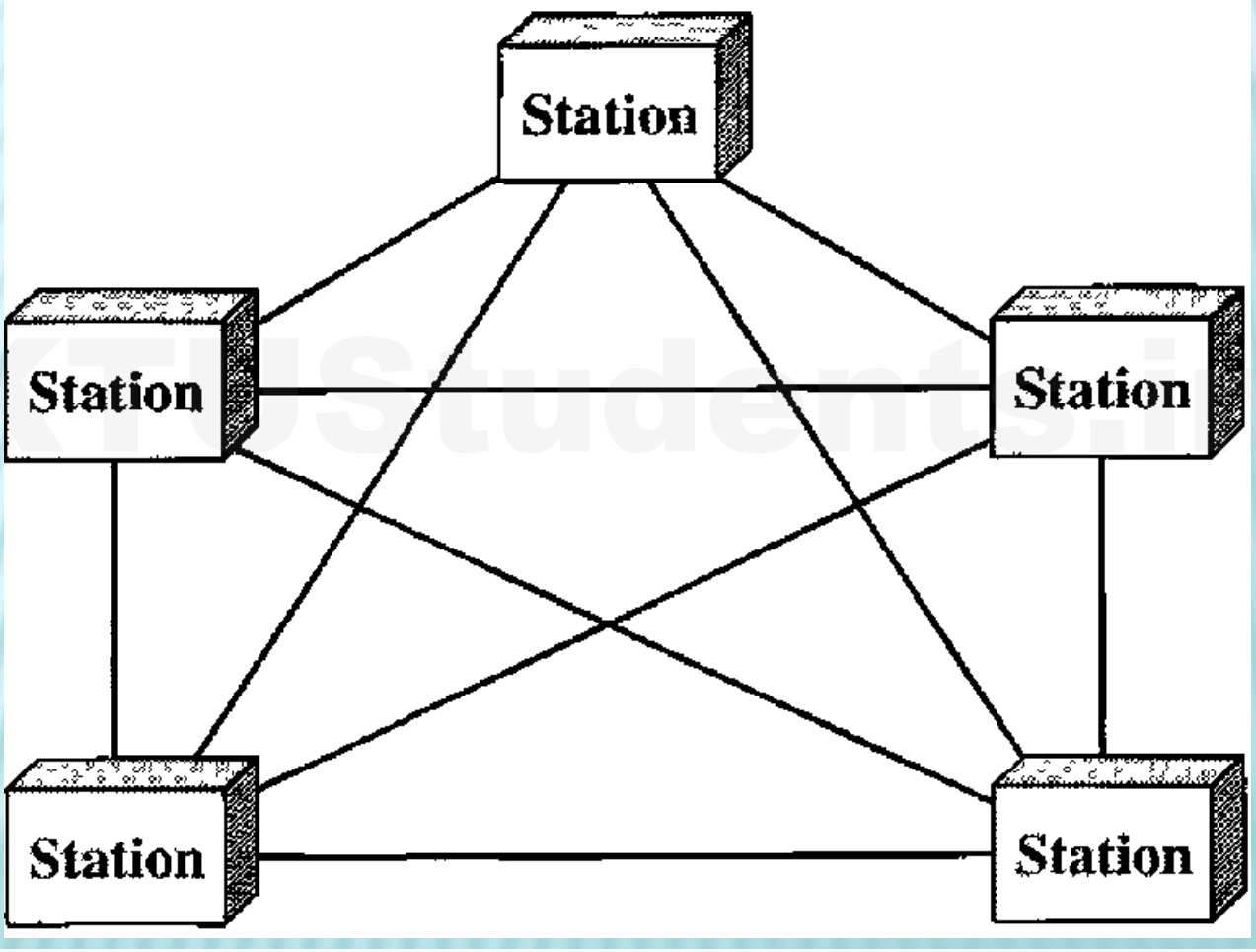


KTUStudents.in

MESH TOPOLOGY

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term *dedicated means that the link carries traffic only between the* two devices it connects.

MESH TOPOLOGY



4. Assume six devices are arranged in a mesh topology. How many cables are needed ? How many ports are needed for each device ?

KTUStudents.in

ADVANTAGES AND DISADVANTAGES

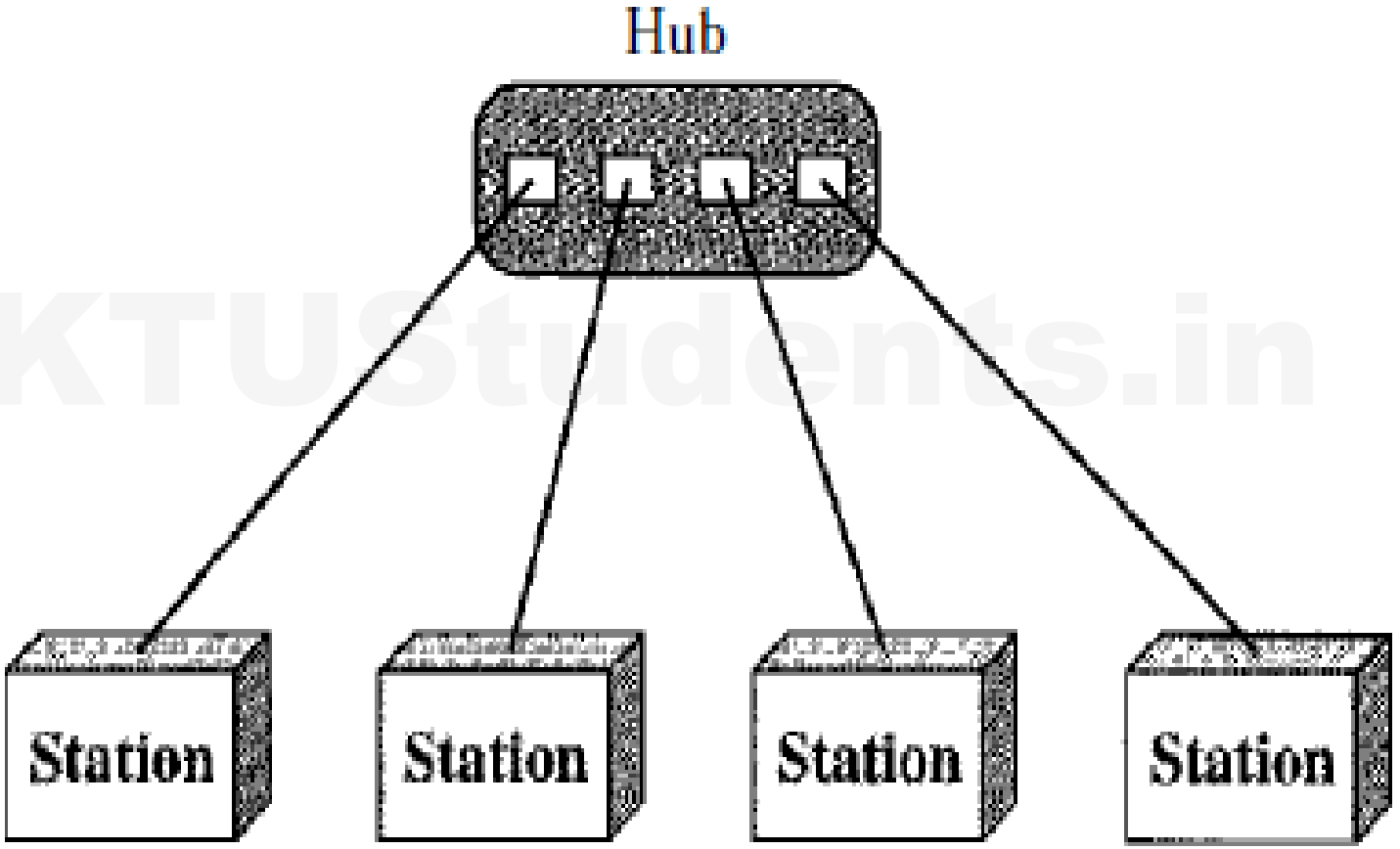
1. the use of dedicated links guarantees that each connection can carry its own data load.
2. robust.
3. privacy or security
4. point-to-point links make fault identification and fault

1. installation and reconnection are difficult
2. sheer bulk of the wiring can be greater than the available space
3. the hardware required to connect each link can be prohibitively

STAR TOPOLOGY

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- each device needs only one link and one I/O port to connect it to any number of others.
- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub.

EEUStudents.in

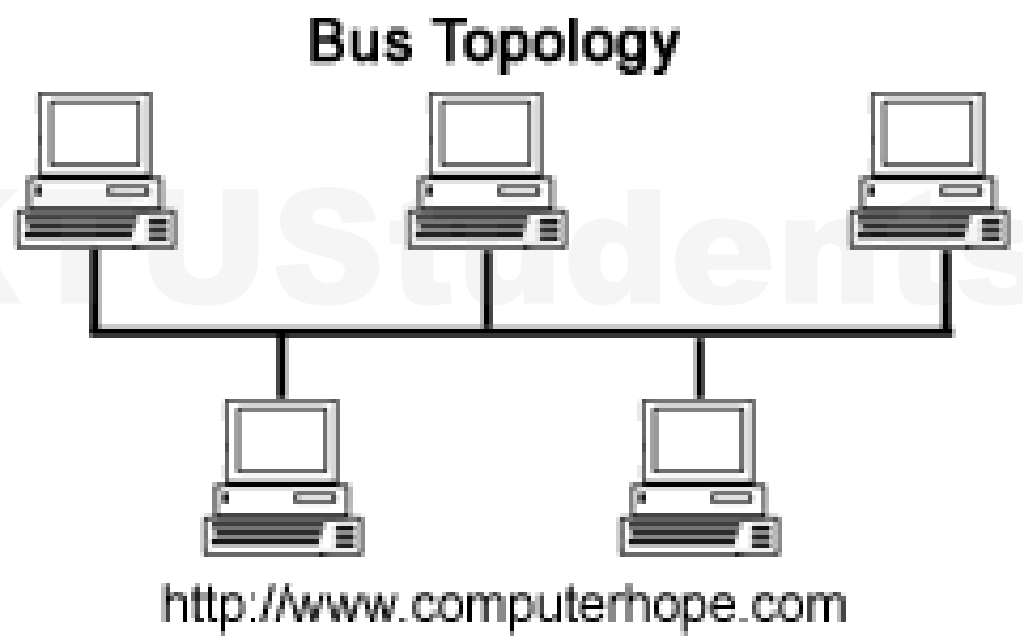


KTUStudents.in

BUS TOPOLOGY

- A **bus Topology is multipoint.**
- **One long cable acts as a backbone to link all** the devices in a network
- Nodes are connected to the bus cable by drop lines and taps.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther.
- For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

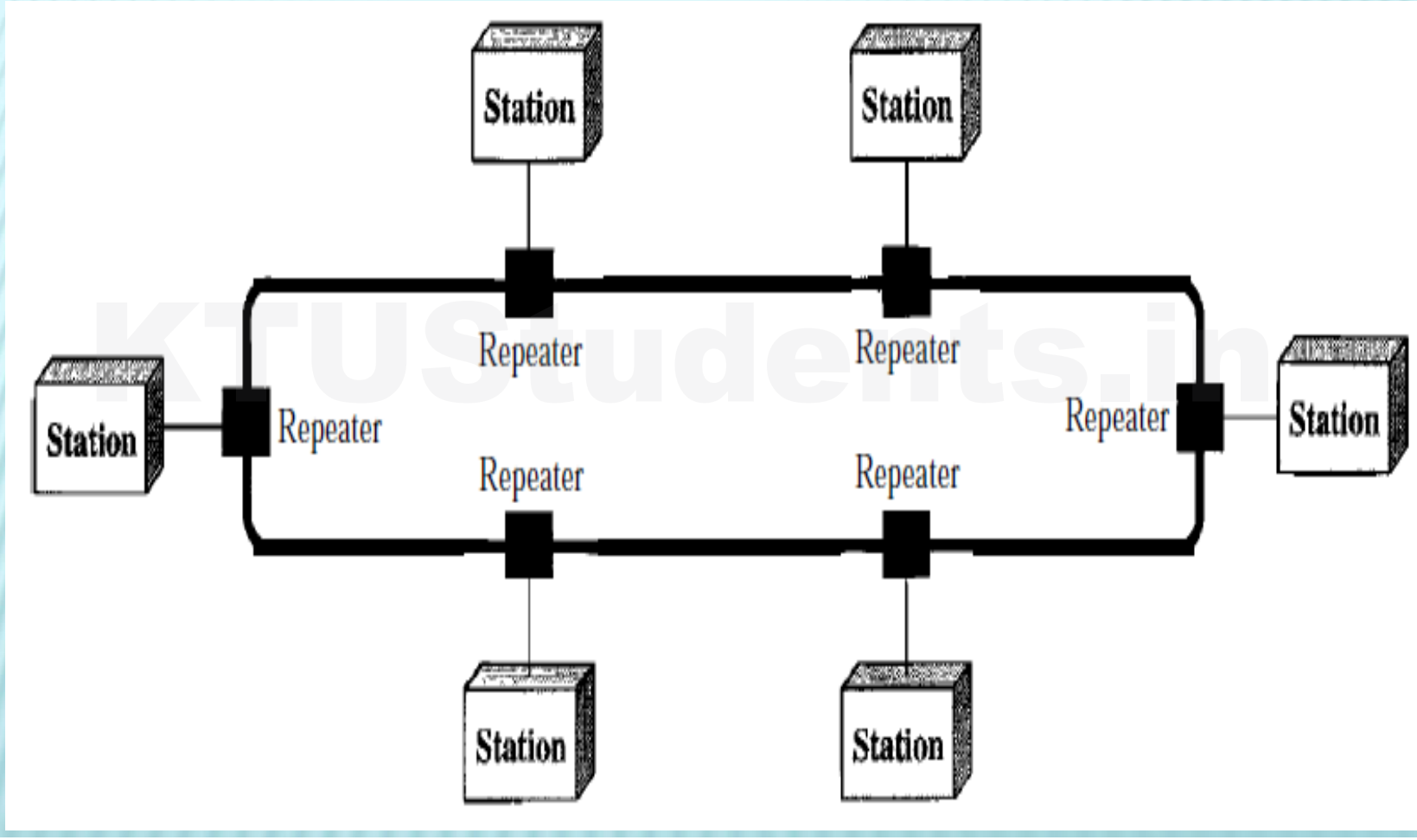
BUS TOPOLOGY



RING TOPOLOGY

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

RING TOPOLOGY



NETWORK MODELS

- Computer networks are created by different entities.
- Standards are needed so that these heterogeneous networks can communicate with one another.
- The two best-known standards are the
- OSI model and the Internet model.

CATEGORIES OF NETWORK

- Local area network(LAN)
- Wide area network(WAN)
- Metropolitan area network(MAN)

KTUStudents.in

LAN

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- LAN size is limited to a few kilometers.
- LANs are distinguished from other types of networks by their transmission media and topology.
- The most common LAN topologies are bus, ring, and star.

WAN

- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

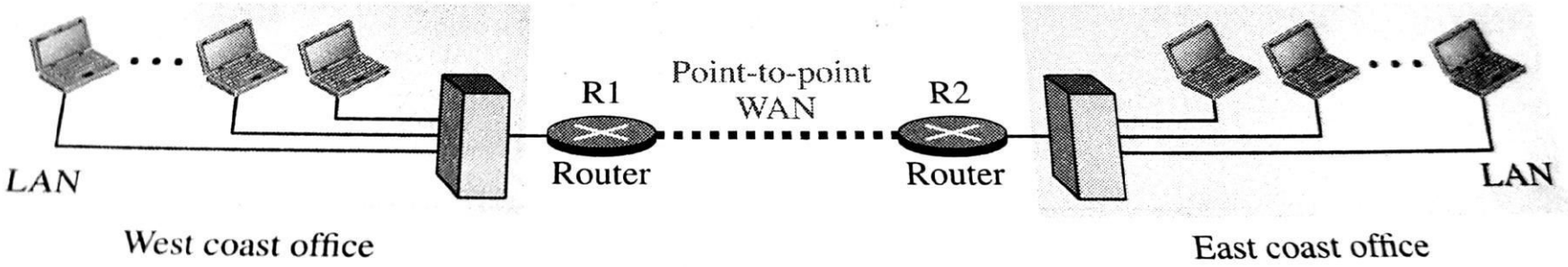
MAN

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city.
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

INTERNETWORK

- When two or more networks are connected, they become an internetwork, or internet.

KTUStudents.in



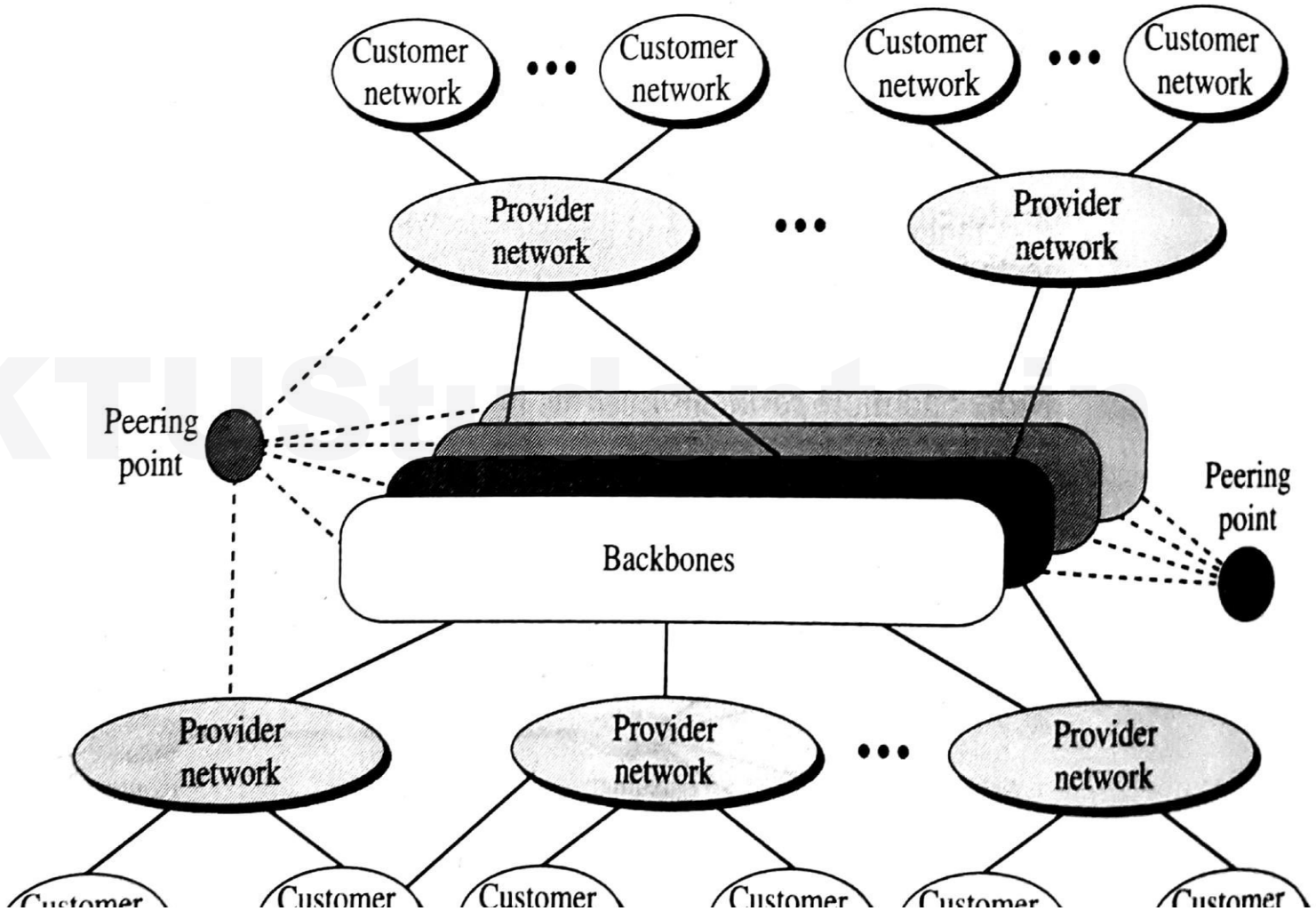
SWITCHING

- An internet is a switched network in which a switch connects at least two links together.
- A switch needs forward data from a network to another network.
- 2 common methods are :
- Circuit switched
- Packet switched

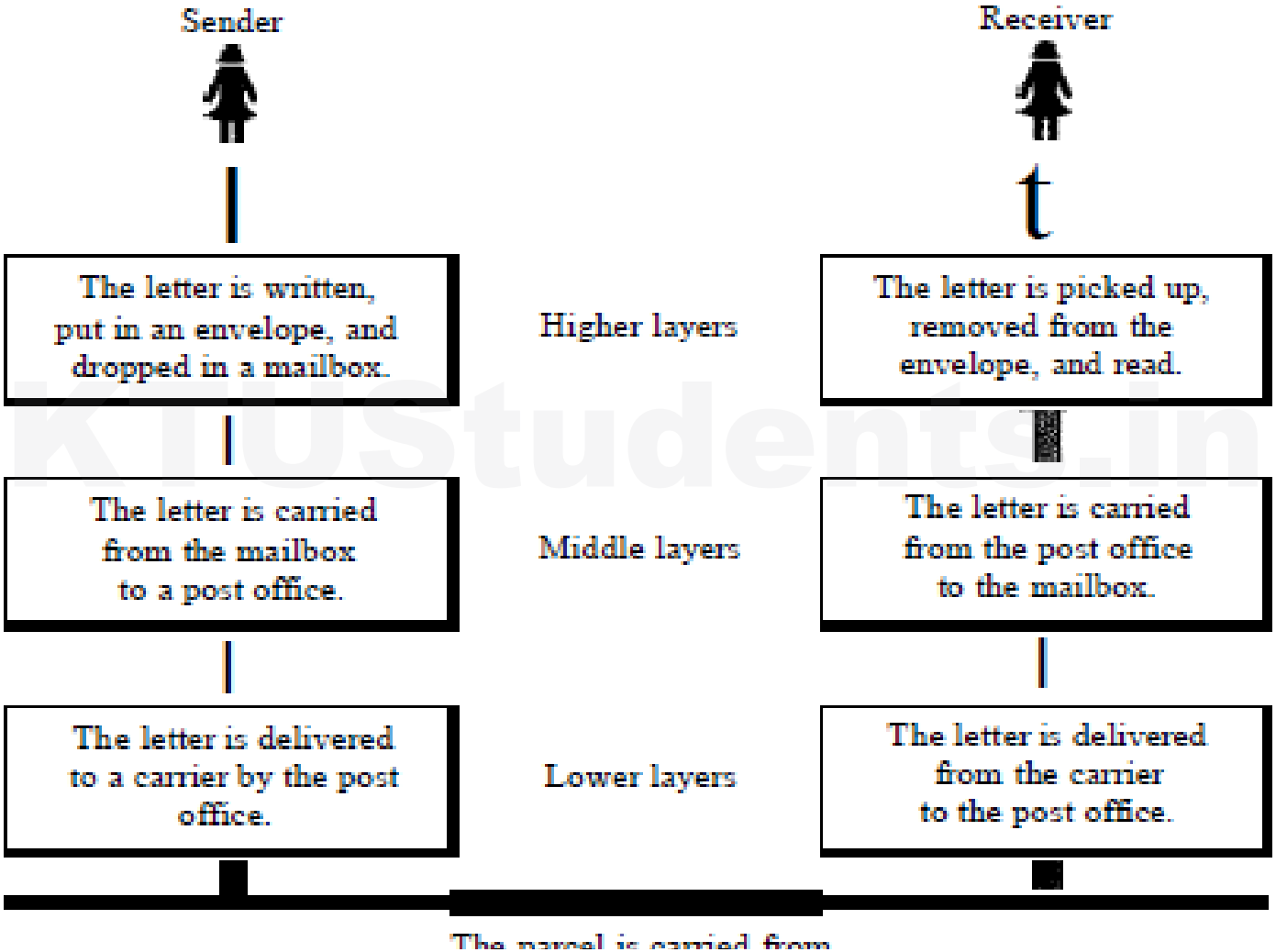
CIRCUIT SWITCHING

- In a circuit switched network a dedicated connection called a circuit is always available between the two ends .
- Switch can only make it active or inactive.

INTERNET


Customer network
Customer network
Customer network
Customer network
Provider network
Provider network
Peering point
Peering point
Backbones
Provider network
Provider network
Provider network

LAYERED TASKS

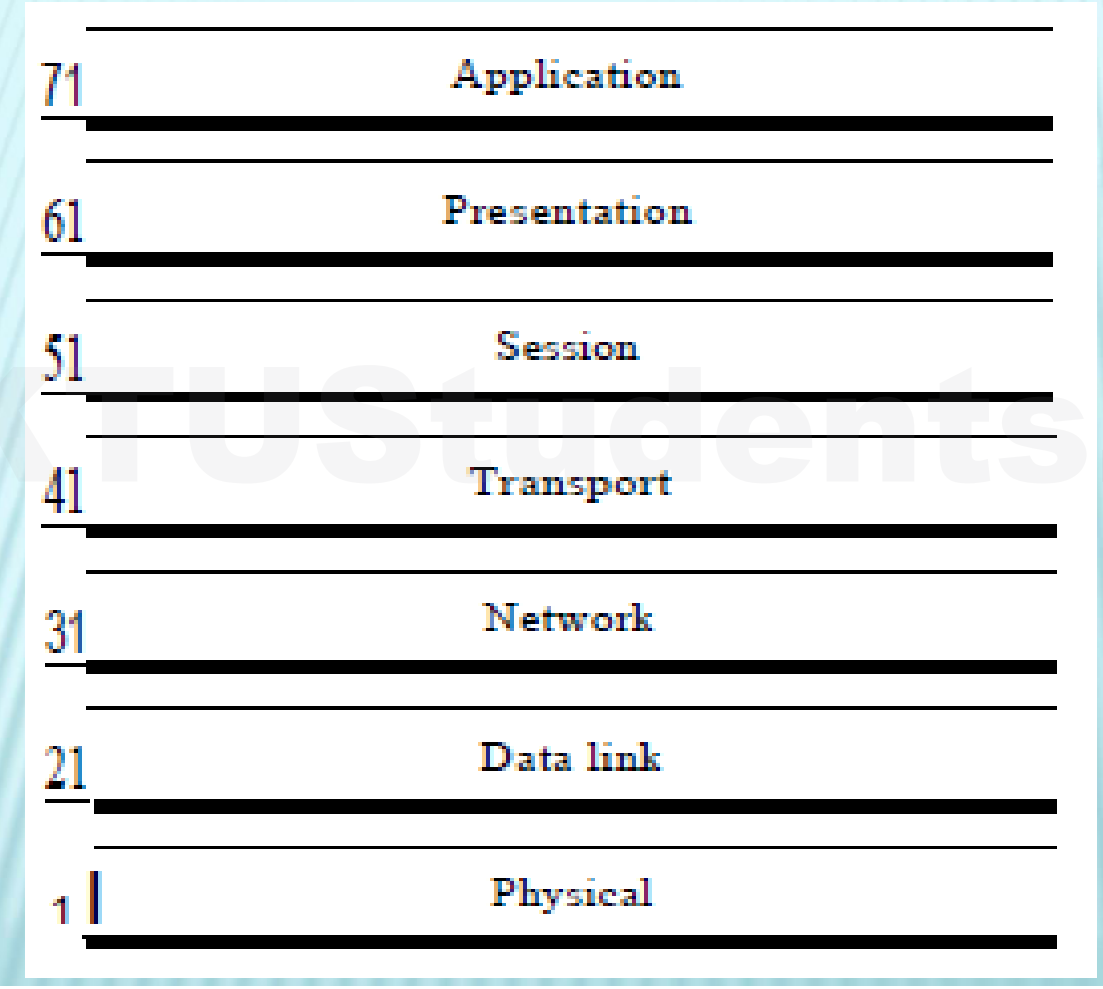


KTUStudents.in

OSI MODEL

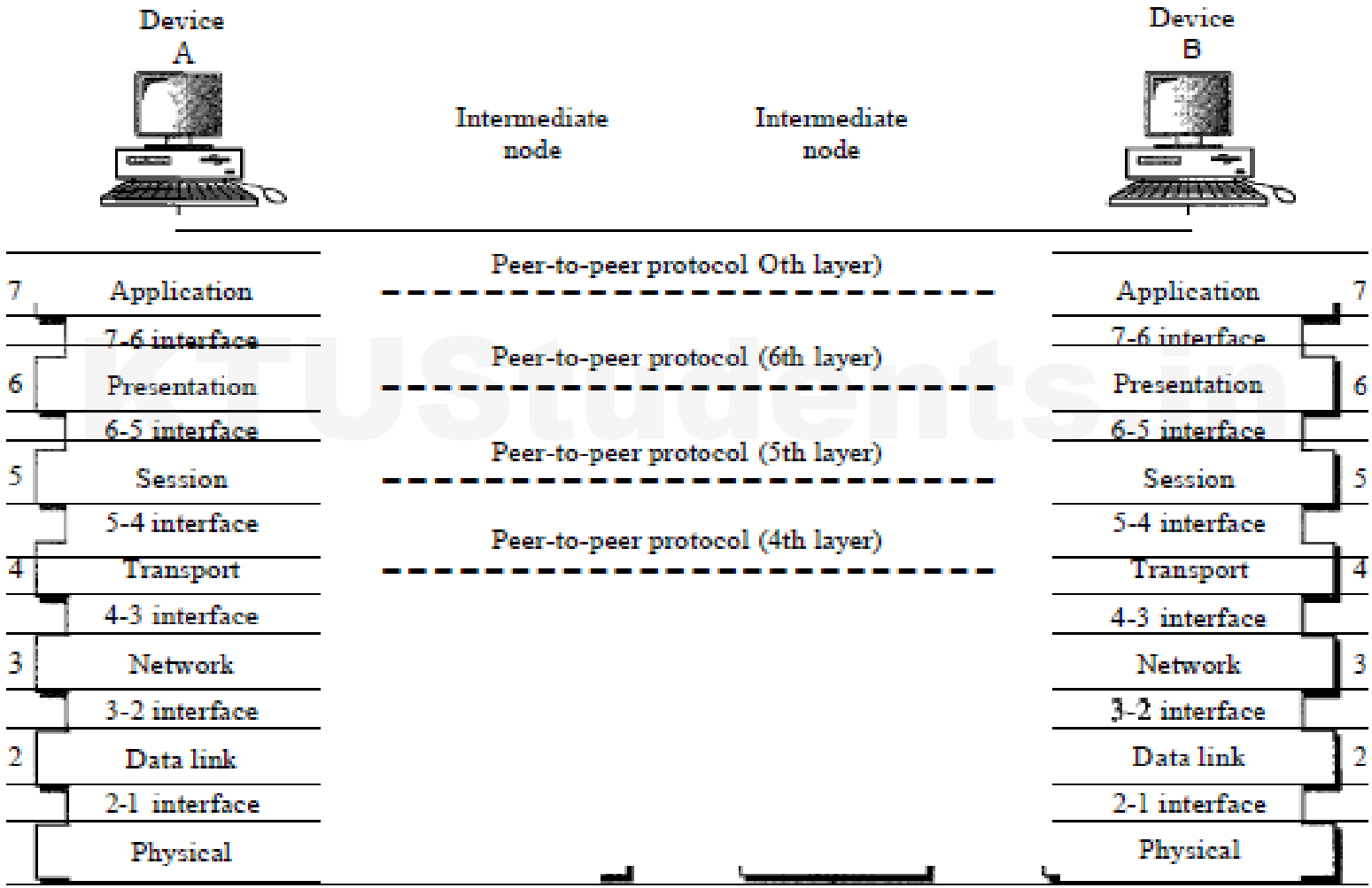
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network


7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical

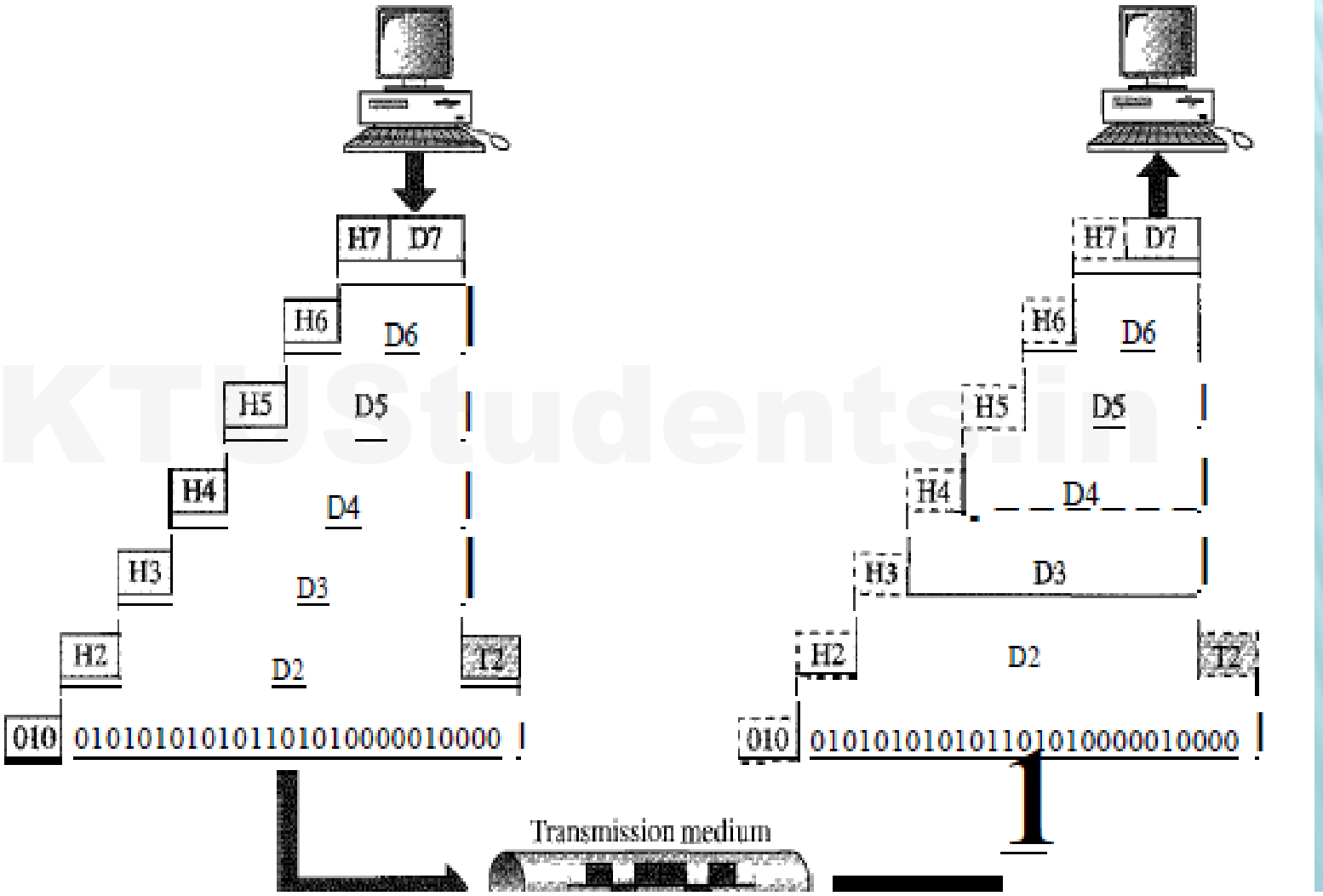
- Within a single machine, each layer calls upon the services of the layer just below it.
- Between machines, layer *x on one machine communicates with layer x on* another machine.
- This communication is governed by an agreed-upon series of rules and conventions called protocols.
- The processes on each machine that communicate at a given layer are called peer-to-peer processes.

PEER TO PEER COMMUNICATION



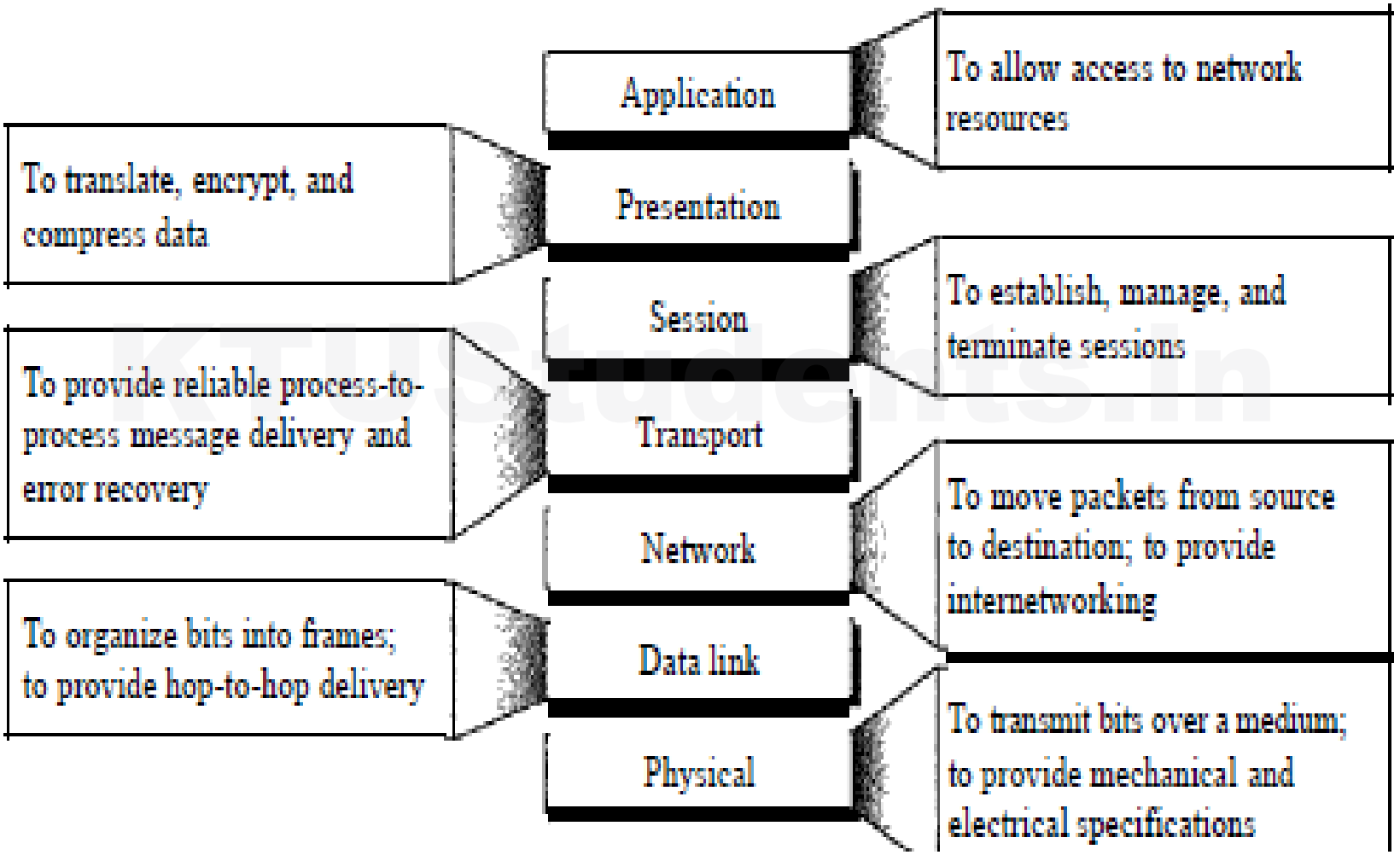
INTERFACES BETWEEN LAYERS

- Each interface defines the information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.


H7
D7
H6
D6
H5
D5
H4
D4
H3
D3
H2
D2
T2
010
0101010101011010100000 10000
Transmission medium
1

ENCAPSULATION

- the data portion of a packet at level *N - 1 carries the whole packet* (data and header and maybe trailer) from level *N.*
- *The concept is called encapsulation;*
- level *N - 1 is not aware of which part of the encapsulated packet is data and which part* is the header or trailer.
- For level *N - 1, the whole packet coming from level N is treated* as one integral unit.


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP PROTOCOL SUITE

- TCP/IP protocol suite is having 5 layers:
- physical,
- Data link
- internet,
- transport,
- application

VTUStudents.in

- The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, are represented in TCP/IP by a single layer called the *application layer*

PHYSICAL AND DATA LINK LAYER

- At the physical and data link layers, *TCP/IP does not define any specific protocol.*
- *It* supports all the standard and proprietary protocols.
- A network in a *TCP/IP internetwork* can be a local-area network or a wide-area network.

NETWORK LAYER

- At the network layer (or, more accurately, the internetwork layer), *TCP/IP supports* the Internetworking Protocol.
- IP, in turn, uses four supporting protocols: ARP,

RARP, ICMP, and IGMP.

TRANSPORT LAYER

- the transport layer was represented in *TCP/IP by two protocols: TCP and* UDP.
- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

APPLICATION LAYER

- The *application layer in TCP/IP is equivalent to the combined session, presentation,* and application layers in the OSI model
- Many protocols are defined at this layer

EC407 M4-Computer Communication

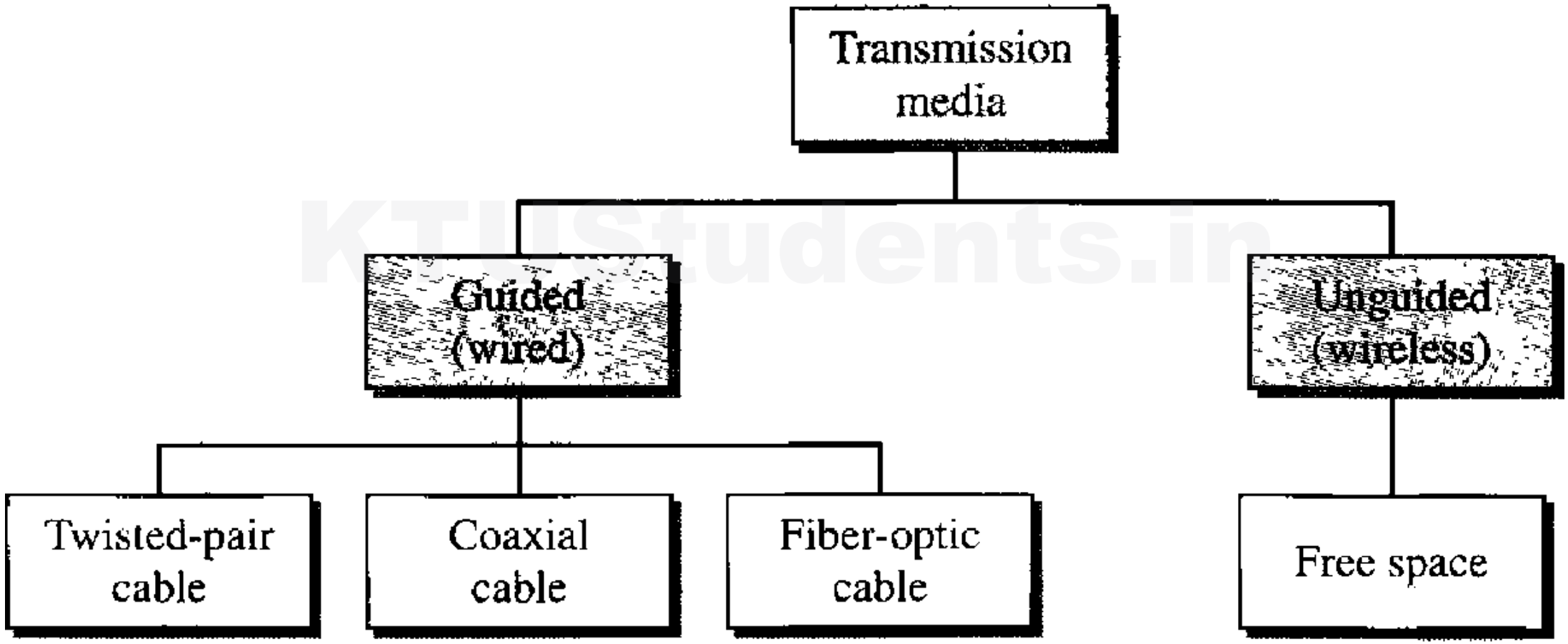
Mod 2

KTUStudents.in

Physical layer

- Transmission medium - A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination.
- Two types : guided and unguided media

KTUStudents.in


Transmission media
Guided (wired)
Unguided (wireless)
Twisted-pair cable
Coaxial cable
Fiber-optic cable
Free space

Guided media

- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
- Optical fiber is a cable that accepts and transports signals in the form of light.

KTUStudents.in

Twisted-Pair Cable

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

KTUStudents.in

- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
- The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- Because of twisting the cables the unwanted signals are mostly cancelled out.

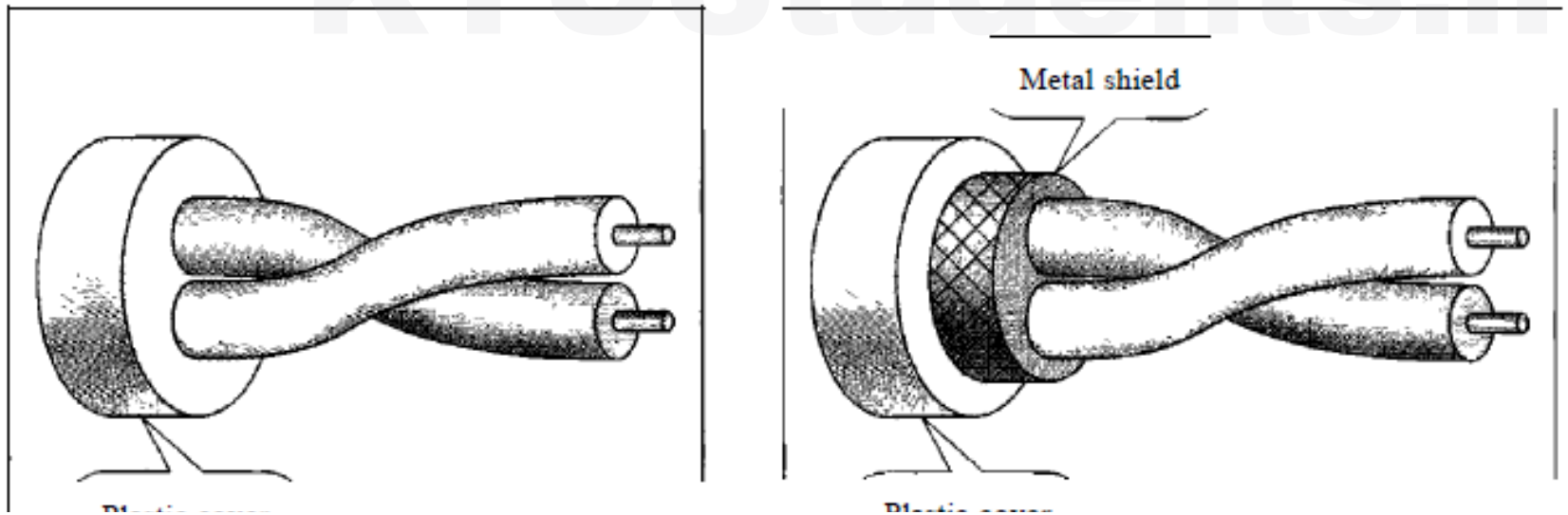
KTUStudents.in

STP and UTP

- Two types of twisted pair cables are there:

1. Shielded twisted pair cable (STP)
2. Unshielded twisted pair cable(UTP)

KTUStudents.in



STP

- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

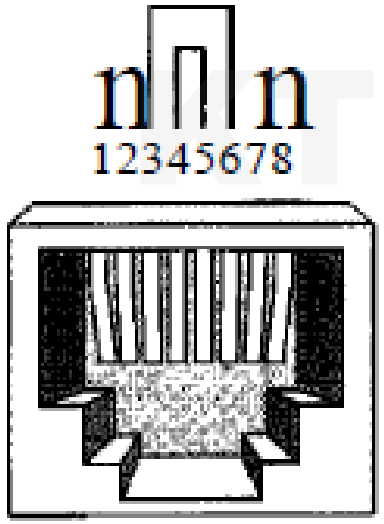
KTUStudents.in

UTP categories

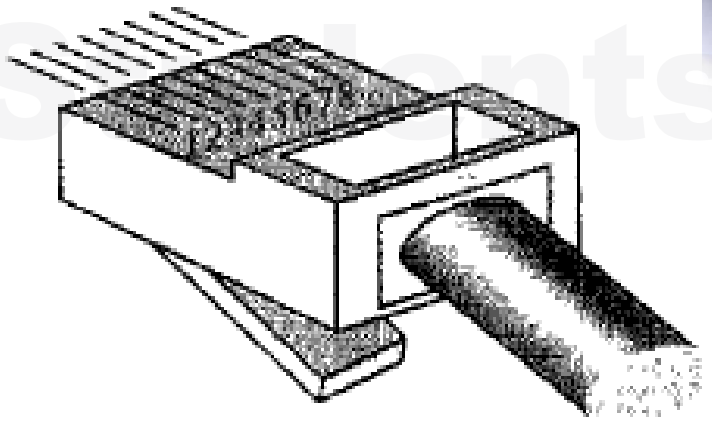
Table 7.1 *Categories of unshielded twisted-pair cables*

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside	600	LANs

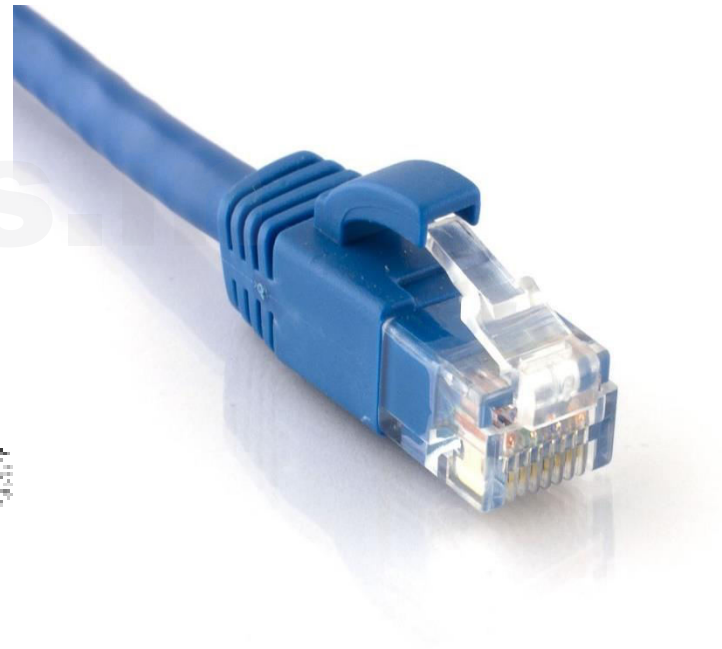
- Connector- most commonly used is RJ 45.



RJ-45 Female



RJ-45 Male



- Performance : One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance.
- Application : telephone networks, DSL lines etc

KTUStudents.in

Data link layer - framing

- In data link layer bits are packed in to frames to distinguish from one another.
- Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

KTUStudents.in

- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.

KTUStudents.in

Fixed-Size Framing

- In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

KTUStudents.in

Variable-Size Framing

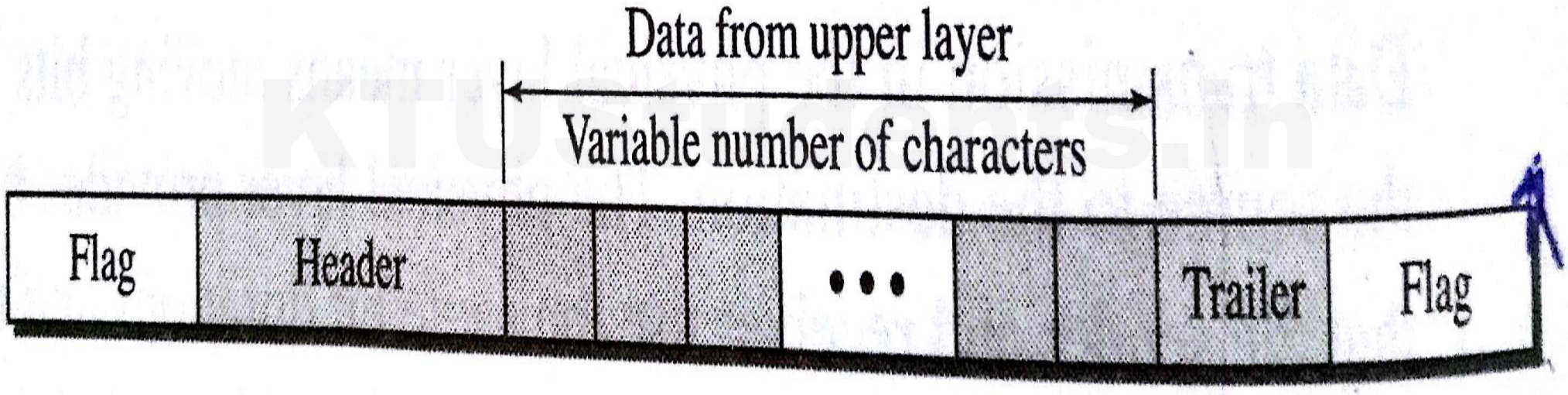
- In variable-size framing, we need a way to define the end of the frame and the beginning of the next.
- two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

KTUStudents.in

Character-Oriented Protocols

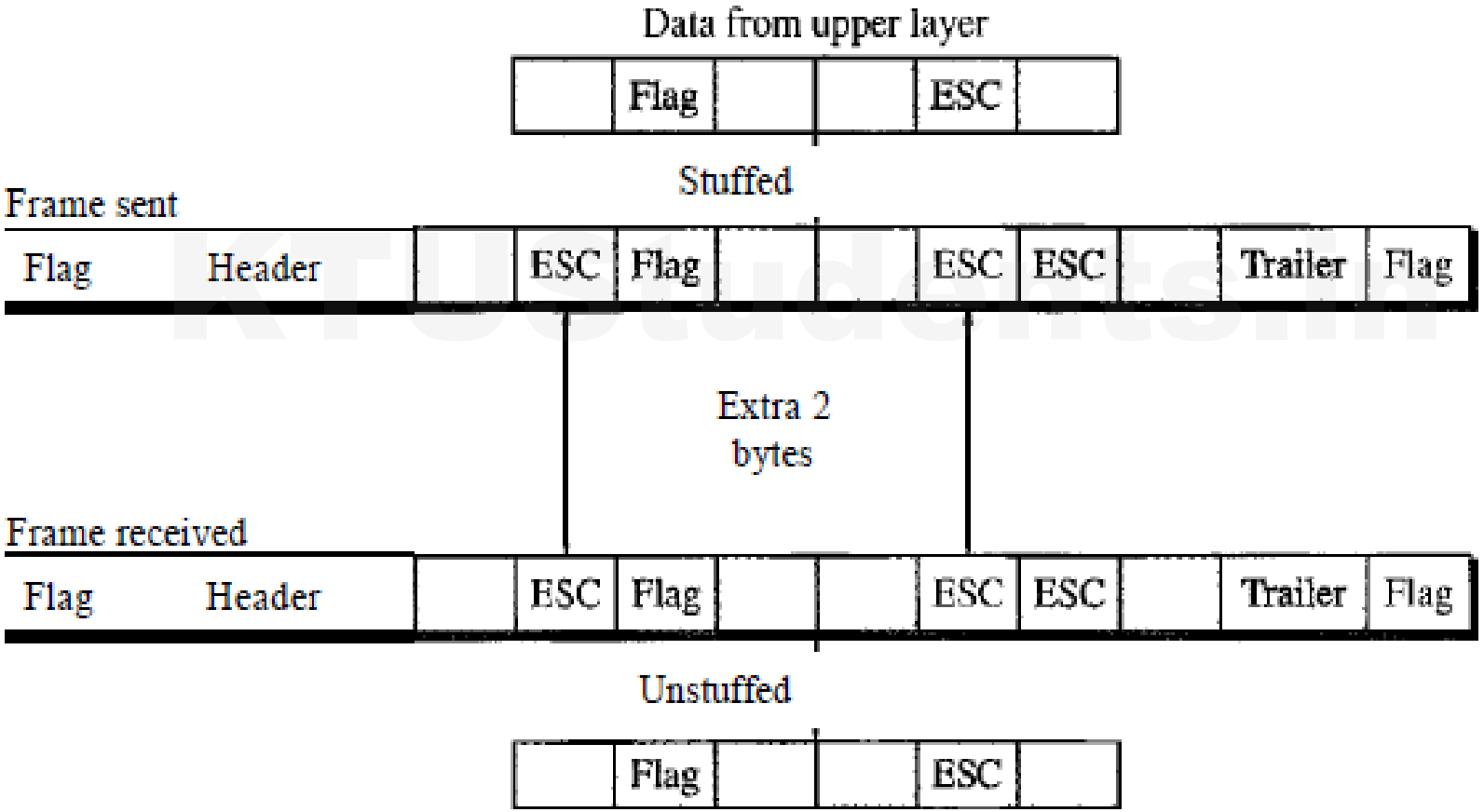
- In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII .
- the header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

KTUStudents.in


Data from upper layer
Variable number of characters
Flag
Header
Trailer
Flag

- The flag could be selected to be any character not used for text communication.
- In byte stuffing a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

KTUStudents.in


Data from upper layer
Flag
ESC
Stuffed
Frame sent
Flag
Header
ESC
Flag
ESC
ESC
Trailer
Flag
Extra 2
bytes
Frame received
Flag
Header
ESC
Flag
ESC
ESC
Trailer
Flag
Unstuffed
Flag
ESC

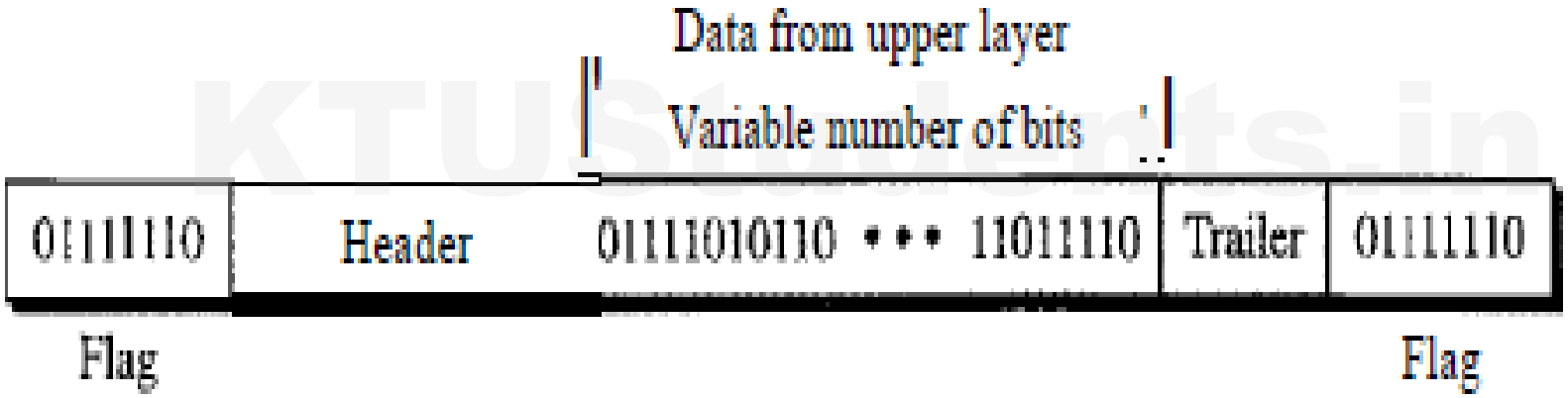
- Character-oriented protocols present another problem in data communications.
- The universal coding systems in use today, such as Unicode, have 16-bit and 32-bit characters that conflict with 8-bit characters.

KTUStudents.in

Bit oriented protocol

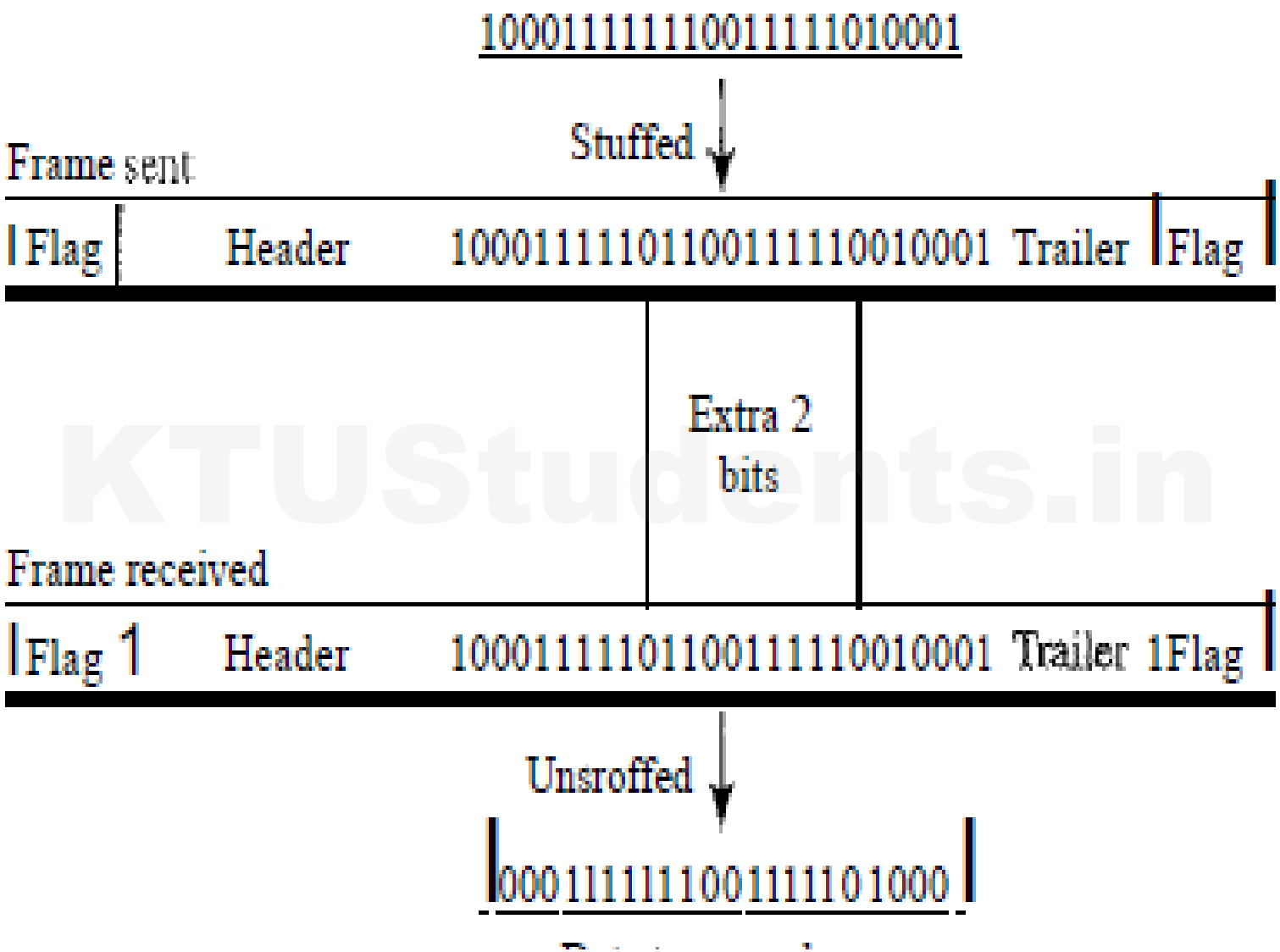
- In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame.

KTUStudents.in


Data from upper layer
Variable number of bits
01111110
Header
01111010110 • • • 11011110
Trailer
01111110
Flag
Flag

- This flag can create the same type of problem we saw in the byte-oriented protocols. That is, if the flag pattern appears in the data, it should be distinguished.
- This is done by stuffing 1 single bit to prevent the pattern from looking like a flag.
- The strategy is called bit stuffing. In bit stuffing, if a 0 and five consecutive I bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.

KTUStudents.in

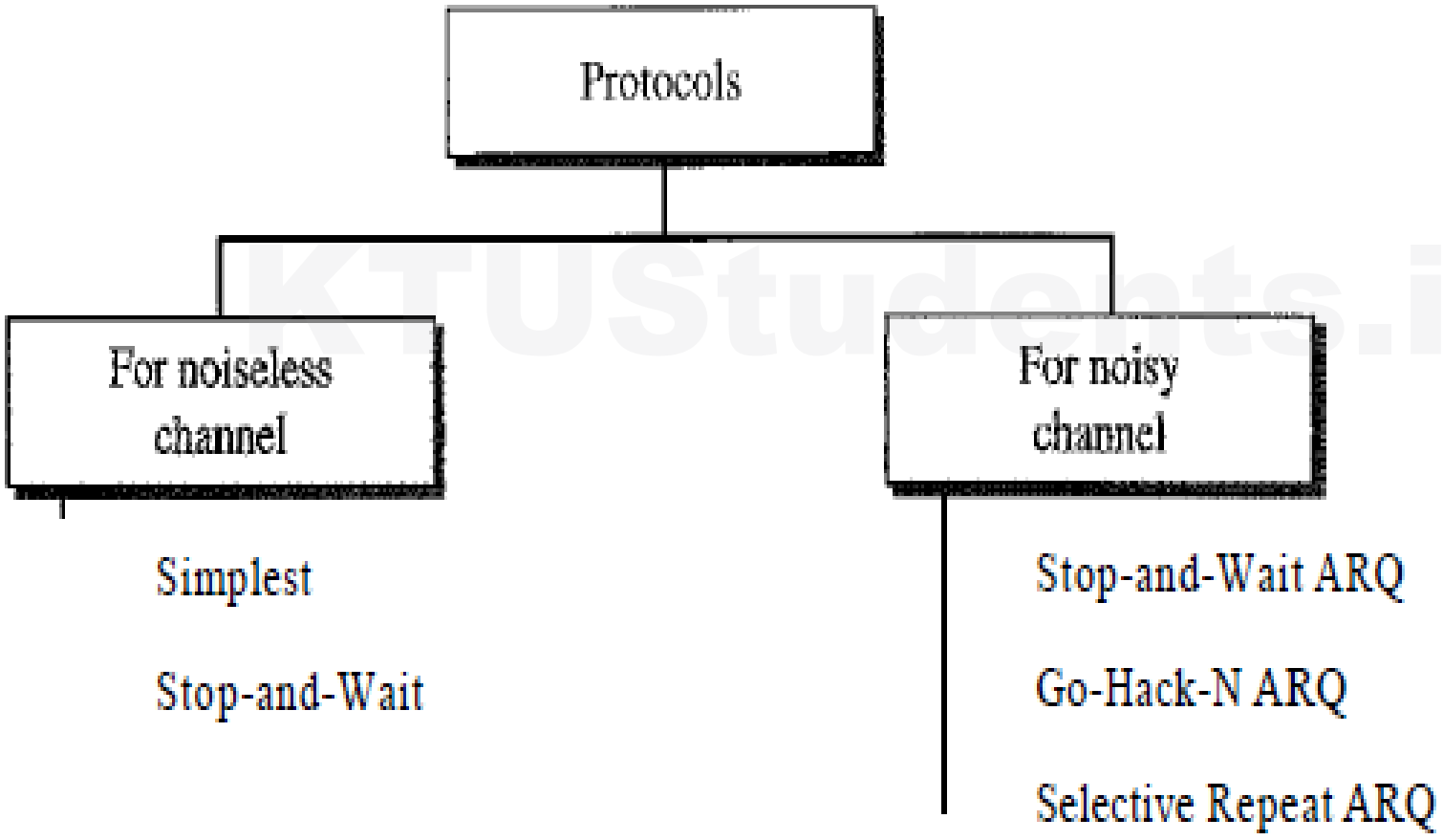


KTUStudents.in

Flow control

- It coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer.
- flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.
- The rate of data processing is often slower than the rate of transmission.
- So each receiving device has a block of memory, called a *buffer,* reserved for storing incoming data until they are processed.
- If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

KTUStudents.in



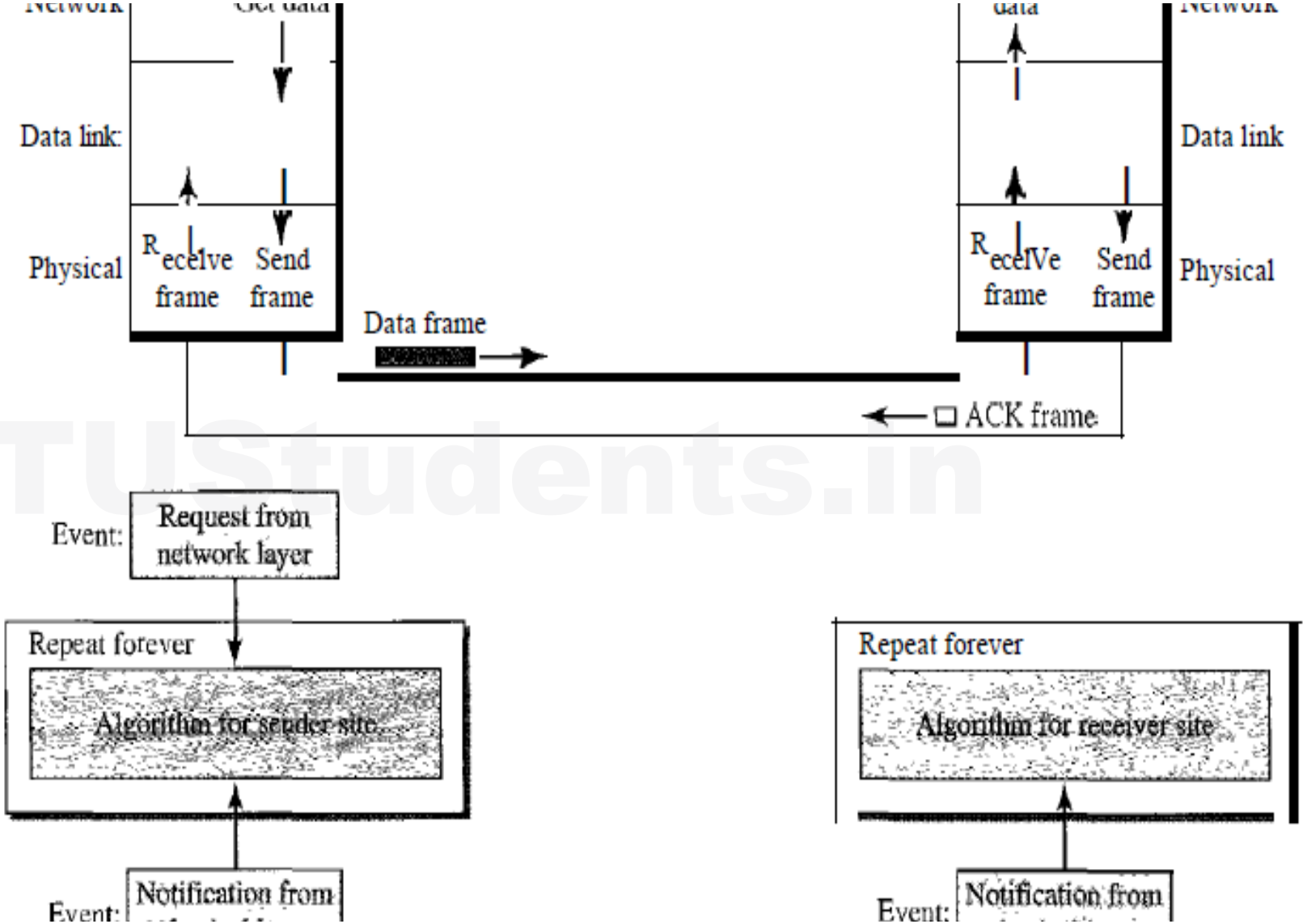
KTUStudents.in

Stop and wait protocol

- sender sends one frame, stops until it receives confirmation from the receiver , and then sends the next frame.
- unidirectional communication for data frames, but auxiliary ACK frames travel from the other direction.

KTUStudents.in

design


Data link:
Physical
Receive frame
Send frame
Data frame
ACK frame
Data link
Physical
Receive frame
Send frame
Event:
Request from network layer
Repeat forever
Algorithm for sender site
Notification from
Repeat forever
Algorithm for receiver site
Notification from

- At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel.
- We therefore need a half-duplex link.

KTUStudents.in

Sender side algorithm

```
1  while(true)                          IIRepeat forever
2  canSend =true                        IIAllow the first frame to go
3  {
4    WaitForEvent()i                    II Sleep until an event occurs
5    if(Event(RequestToSend) AND canSend}
6    {
7       GetData()i
8       MakeFrame();
9       SendFrame()i                    I/Send the data frame
10      canSend =false;                 I/cannot send until ACK arrives
11   }
12   WaitForEvent()i                    II Sleep until an event occurs
13   if(Event(ArrivalNotification)      /l An ACK has arrived
14    {
15      ReceiveFrame();                 I/Receive the ACK frame
16      canSend = true;
```

KTUStudents.in

Analysis

- Here two events can occur: a request from the network layer or an arrival notification from the physical layer.
- The responses to these events must alternate.
- In this algorithm ,a ***canSend*** *variable that can either be true or false is used.*
- *When a frame is sent, the variable* is set to false to indicate that a new network request cannot be sent until *canSend is true.*
- *When an* ACK is received, canSend is set to true to allow the sending of the next frame.

KTUStudents.in

Receiver side algorithm

```
1  while (true)                              IIRepeat  forever
2  {
3    WaitForEvent();                         II Sleep until an event occurs
4    if(Event(ArrivalNotification)}          IIData frame arrives
5    {
6        ReceiveFrame(};
7        ExtractData(}i
8        Deliver(data};                      /IDeliver data to network layex
9        SendFrame();                        IISend an ACK frame
10   }
11 }
```

KTUStudents.in

Flow diagram

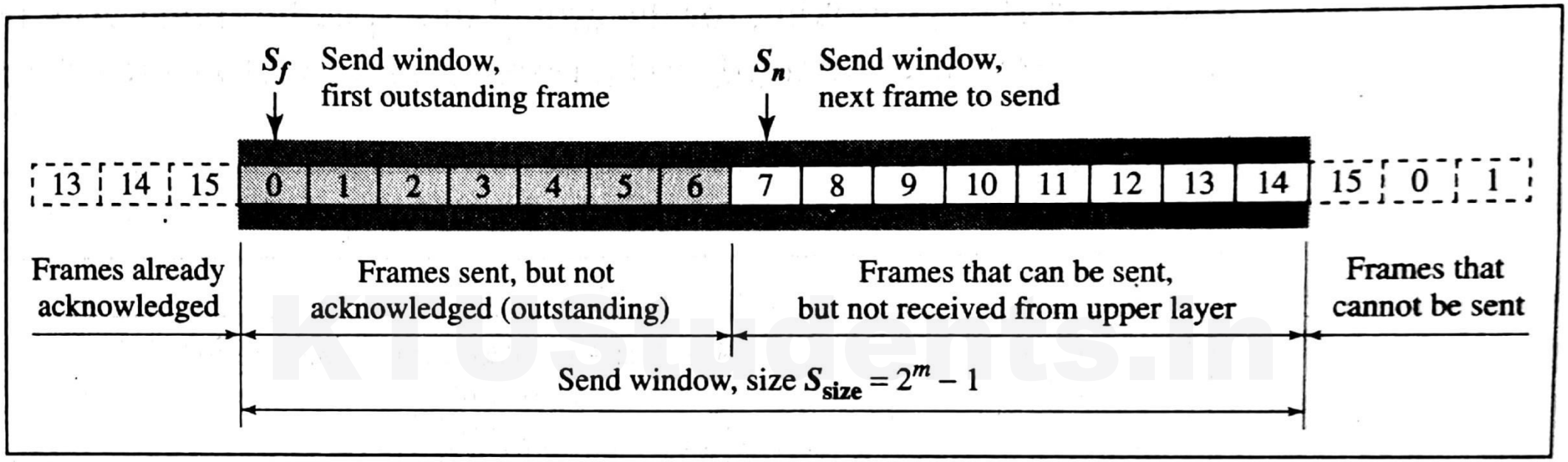
KTUStudents.in

Sliding window protocol

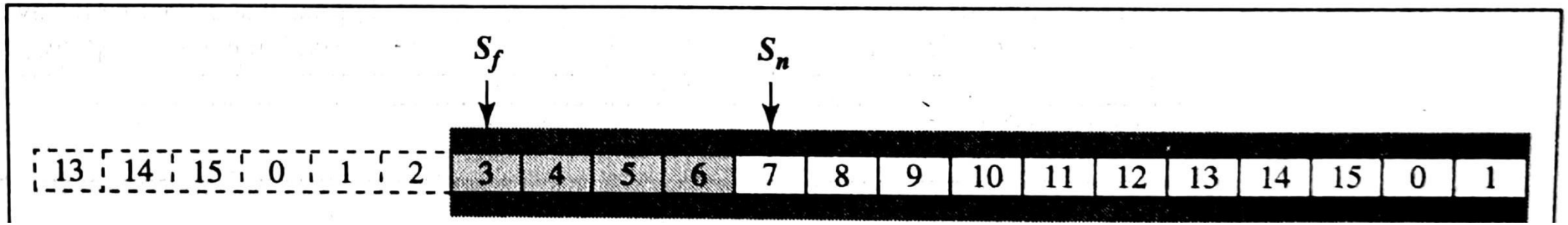
- To improve the efficiency of transmission , multiple frames must be in transition while waiting for acknowledgment.
- Frames from a sending station are numbered sequentially.
- If the header of the frame allows *m bits for the sequence number, the sequence numbers* range from 0 to *2m - 1.*
- the sender and receiver need to deal with only part of the possible sequence numbers.
- The range which is the concern of the sender is called the send sliding window;
- the range that is the concern of the receiver is called the receive sliding window.

ktustudents.in

Figure 11.12 *Send window for Go-Back-N ARQ*



a. Send window before sliding



- The send window is an imaginary box covering the sequence numbers of the data frames which can be in transit.
- In each window position, some of these sequence numbers define the frames that have been sent; others define those that can be sent.
- The window at any time divides the possible sequence numbers into four regions.
- The first region, from the far left to the left wall of the window, defines the sequence numbers belonging to frames that are already acknowledged.

KTUStudents.in

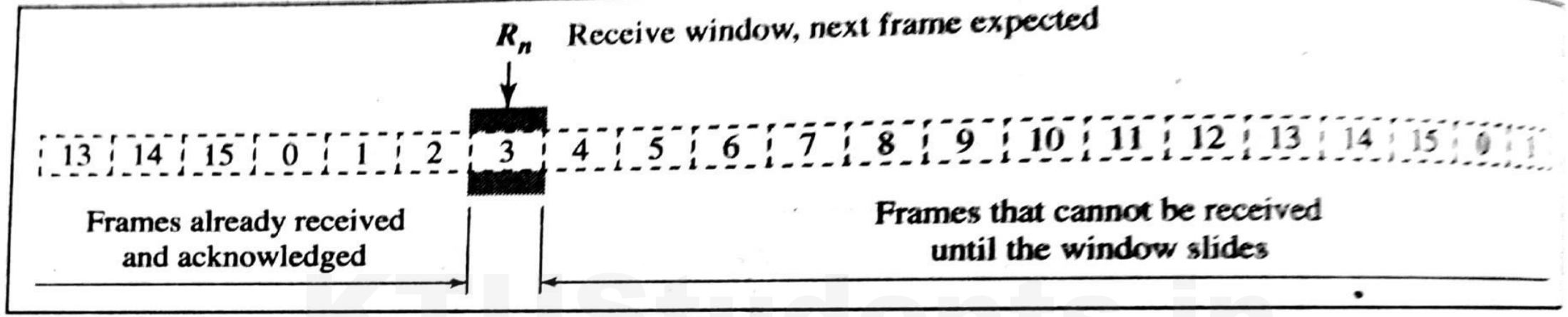
- The second region, defines the range of sequence numbers belonging to the frames that are sent and have an unknown status. The sender needs to wait to find out if these frames have been received or were lost - outstanding frames.
- The third range, defines the range of sequence numbers for frames that can be sent;
- Finally, the fourth region defines sequence numbers that cannot be used until the window slides.

KTUStudents.in

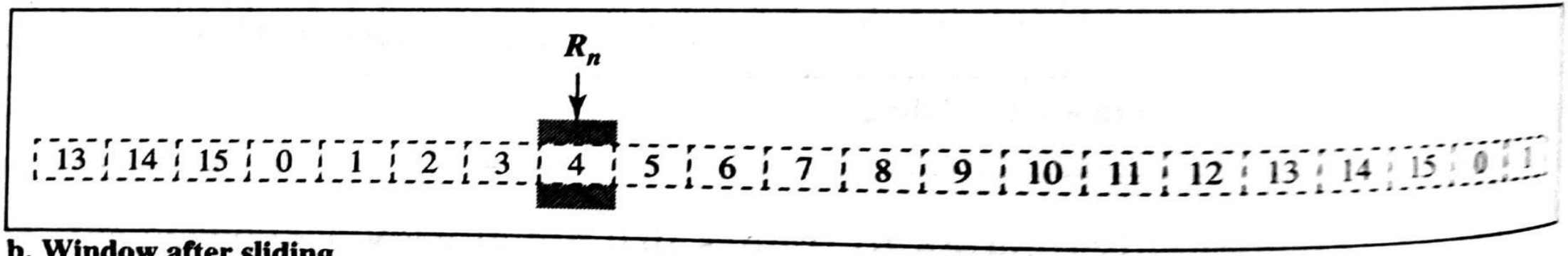
- three variables define its size and location at any time.
- *Sf(send window, the first outstanding frame), Sn (send* window, the next frame to be sent), and Ssize (send window, size).
- the acknowledgments in this protocol are cumulative, meaning that more than one frame can be acknowledged by an ACK frame.

KTUStudents.in

Figure 11.13 *Receive window for Go Back*



a. Receive window



b. Window after sliding

KTUStudents.in

- The receive window makes sure that the correct data frames are received and that the correct acknowledgments are sent.
- The size of the receive window is always 1.
- The receiver is always looking for the arrival of a specific frame.
- Any frame arriving out of order is discarded and needs to be resent.

KTUStudents.in

- The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order.
- If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting.
- The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire.
- This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer.
- The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgment for several frames.

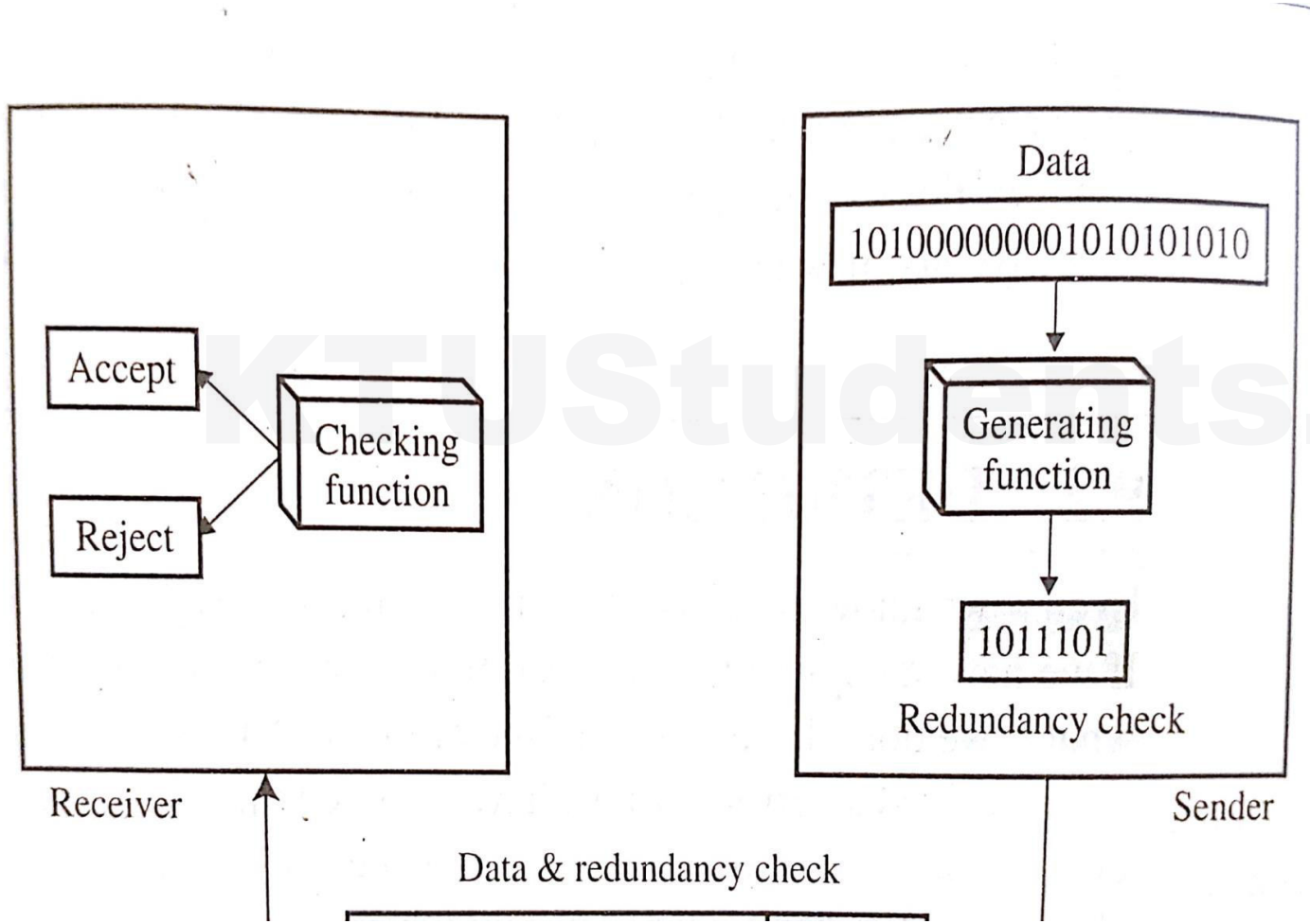
KTUStudents.in

Error control

- Error control is both error detection and error correction.
- It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender.
- In the data link layer, the term *error control* refers primarily to methods of error detection and retransmission.

KTUStudents.in

Error detection



KTUStudents.in

Error detection – check sum

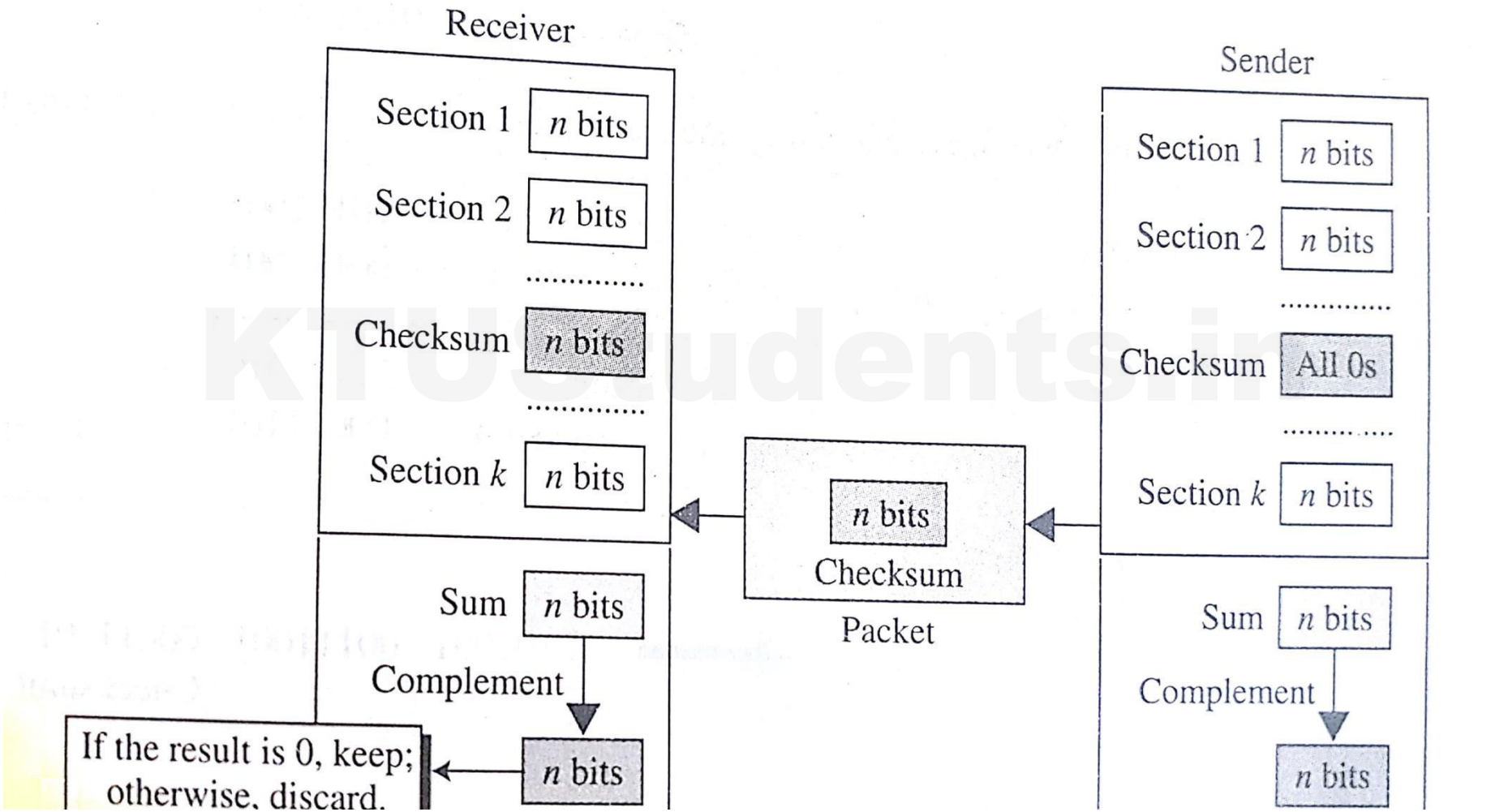
- the checksum is based on the concept of redundancy.
- The sender creates code words out of data words by using a generator that applies the rules and procedures of encoding
- Each codeword sent to the receiver may change during transmission.
- If the received codeword is the same as one of the valid code words, the word is accepted; the corresponding data word is extracted for use.
- If the received codeword is not valid, it is discarded.

KTUStudents.in

Check sum method

- At the sender :
- The unit is divided in to *k* sections, each of n bits
- All sections are added together using ones complement to get sum
- The sum is complemented and becomes the checksum
- Checksum is sent with data.
- At receiver :
- The unit is divided in to *k* sections, each of n bits
- All sections are added together using ones complement to get sum.
- Sum is complemented
- If the result is zero, data are accepted otherwise rejected.

KTUStudents.in

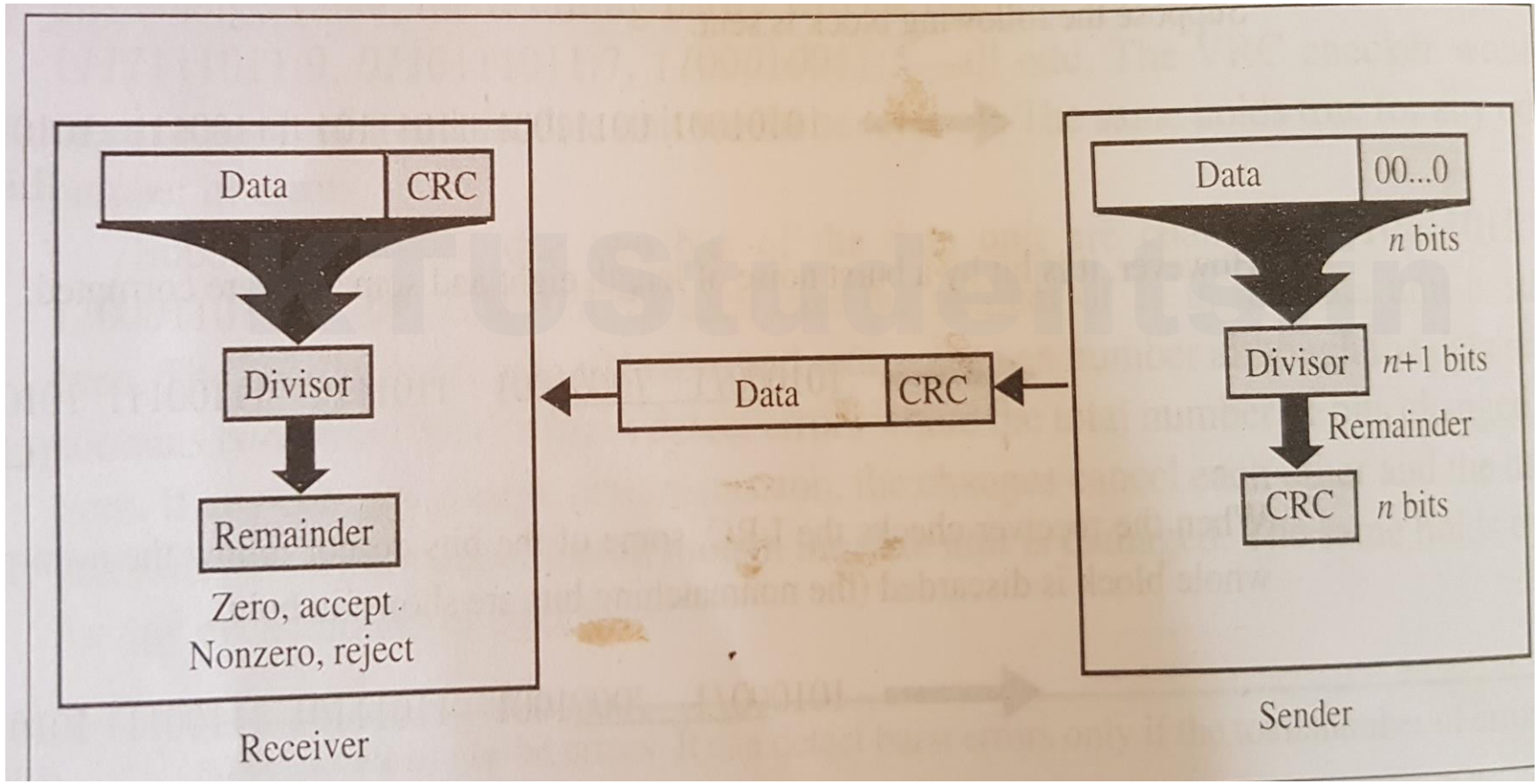

Receiver
Section 1
n bits
Section 2
n bits
Checksum
n bits
Section k
n bits
Sum
n bits
Complement
n bits
If the result is 0, keep;
otherwise, discard.
n bits
Checksum
Packet
Sender
Section 1
n bits
Section 2
n bits
Checksum
All 0s
Section k
n bits
Sum
n bits
Complement
n bits

Cyclic redundancy check (CRC)

- In CRC, a sequence of redundant bits called CRC remainder is appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second predetermined binary number.
- At the receiver ,incoming data unit is divided by the same number, if there is no remainder, the data is accepted, else discarded.
- Redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor.
- The remainder is the CRC
- To be a valid CRC ,it must have exactly one less bit than the divisor and appending it to the end of the data string must make the resulting data string exactly divisible by the divisor.

KTUStudents.in

CRC


Data
CRC
Divisor
Remainder
Zero, accept
Nonzero, reject
Receiver
Data
CRC
Data
00...0
n bits
Divisor
n+1 bits
Remainder
CRC
n bits
Sender

III	Network Layer Logical addressing : IPv4 & IPV6	2	15%
	Address Resolution protocols (ARP, RARP)	2	
	Subnetting, Classless Routing(CIDR), ICMP, IGMP, DHCP	3	
	Virtual LAN, Networking devices (Hubs, Bridges & Switches)	1	

KTUStudents.in

CONTENTS

- INTRODUCTION
- CLASSFUL ADDRESSING
  - Different Network Classes
  - Subnetting
- Classless Addressing
  - CIDR (classless Inter domain Routing)

KTUStudents.in

OBJECTIVES:

- To introduce the concept of an address space in general and the address space of IPv4 in particular.
- To discuss the classful architecture and the blocks of addresses available in each class.
- To discuss the idea of hierarchical addressing and how it has been implemented in classful addressing.
- To explain subnetting and supernetting for classful architecture.
- To discuss classless addressing, that has been devised to solve the problems in classful addressing.

KTUStudents.in

IP Addresses: Classful Addressing

KTUStudents.in

INTRODUCTION

The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected to the Internet is called the Internet address or IP address.

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet; an IP address is the address of the interface.

KTUStudents.in

IP Versions

- **IPv4: IP version 4**.
  - Current, predominant version.
  - **32-bit** long addresses.
  - IPv4 was **initially deployed on 1 January 1983** and is still the most commonly used version.
- IPv6: IP version 6 (aka, IPng).
  - Evolution of IPv4.
  - Longer addresses (**128-bit**).
  - Deployment of the IPv6 protocol began in 1999.

KTUStudents.in

What is an IP Address?

- Currently there are two types of Internet Protocol (IP) addresses in active use:

  IP version 4 (IPv4) and IP version 6 (IPv6).

- **IPv4 addresses are 32-bit** numbers often expressed as 4 octets in **"dotted decimal"** notation (for example, *192.0.2.53*).

- **IPv6 addresses are 128-bit numbers** and are conventionally expressed using **hexadecimal strings** (for example, *2001:0db8:582:ae33::29*).

KTUStudents.in

What is an IP Address?

Note

An IPv4 address is 32 bits long.

KTUStudents.in

Note

The IPv4 addresses are unique and universal.

- An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

- An IP address serves two principal functions: host or network interface identification and location addressing.

KTUStudents.in

- The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries(Internet service providers) and other entities.

- IANA is responsible for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic.

- Both IPv4 and IPv6 addresses are generally assigned in a hierarchical manner.

KTUStudents.in

- ***Users are assigned IP addresses by Internet service providers (ISPs).***
- ***ISPs obtain allocations of IP addresses from a local Internet registry (LIR) or National Internet Registry (NIR), or from their appropriate Regional Internet Registry (RIR).***

Address space rule

The address space in a protocol
That uses N-bits to define an
Address is:

$$2^N$$

KTUStudents.in

IPv4 address space

The address space of IPv4 is

2^{32}

or

4,294,967,296.

Binary Notation

01110101 10010101 00011101 11101010

KTUStudents.in

Introduction

- You can probably work with decimal numbers much easier than with the binary numbers needed by the computer.
- Working with binary numbers is time-consuming & error-prone.

KTUStudents.in

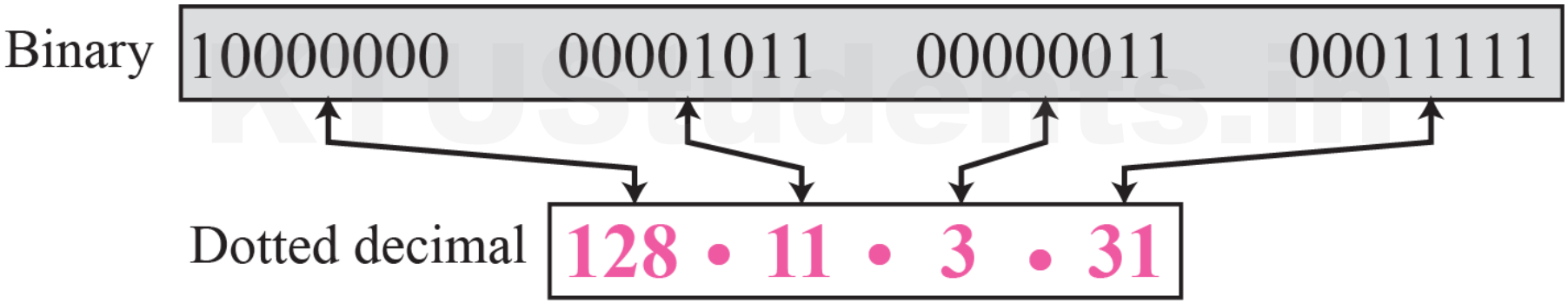
Octets

- The 32-bit IP address is broken up into 4 octets, which are arranged into a dotted-decimal notation scheme.
- Example of an IP version 4:

172.64.126.52

KTUstudents.in

Dotted-decimal notation



Hexadecimal Notation

0111 0101 1001 0101 0001 1101 1110 1010

75 95 1D EA

0x75951DEA

KTUStudents.in

Converting to Decimal

- What is its equivalent decimal value?

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

KTUStudents.in

The binary number 1111 1111 converts into the decimal number:

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

- Therefore, the largest decimal number that can be stored in an IP address octet is ***255***.

Example 1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

KTUStudents.in

c. 11100111 11011011 10001011 01101111

d. 11111001 10011011 11111011 00001111

Example 1: *Solution*

a. 10000001 00001011 00001011 11101111
b. 11000001 10000011 00011011 11111111
c. 11100111 11011011 10001011 01101111
d. 11111001 10011011 11111011 00001111

We replace each group of 8 bits with its equivalent decimal number and add dots for separation:

KTUStudents.in

a. 129.11.11.239
b. 193.131.27.255
c. 231.219.139.111
d. 249.155.251.15

Example 2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

c. *241.8.56.12*

d. *75.45.34.78*

KTUStudents.in

Example 2: *Solution*

a. 111.56.45.78
b. 221.34.7.82
c. *241.8.56.12*
d. *75.45.34.78*

We replace each decimal number with its binary equivalent:

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

c. 11110001 00001000 00111000 00001100

d. 01001011 00101101 00100010 01001110

KTUStudents.in

Example 3

Find the error, if any, in the following IPv4 addresses:

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

KTUStudents.in

Example 3: *Solution*

a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

a. There should be no leading zeroes (045).

b. We may not have more than 4 bytes in an IPv4 address.

c. Each byte should be less than or equal to 255.

d. A mixture of binary notation and dotted-decimal notation.

KTUStudents.in

Example 4

Change the following IPv4 addresses from binary notation to hexadecimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

KTUStudents.in

We replace each group of 4 bits with its hexadecimal equivalent. Note that 0X (or 0x) is added at the beginning or the subscript 16 at the end.

a. 0X810B0BEF or $810B0BEF_{16}$

b. 0XC1831BFF or $C1831BFF_{16}$

Example 4

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 4 bits with its hexadecimal equivalent. Note that 0X (or 0x) is added at the beginning or the subscript 16 at the end.

a. 0X810B0BEF or $810B0BEF_{16}$

b. 0XC1831BFF or $C1831BFF_{16}$

KTUStudents.in

Example 5

Find the number of addresses in a range if the first address is 146.102.29.0 and the last address is 146.102.32.255.

KTUStudents.in

Example 5

Find the number of addresses in a range if the first address is 146.102.29.0 and the last address is 146.102.32.255.

Solution

We can subtract the first address from the last address in base 256.

The result is 0.0.3.255 in this base.

To find the number of addresses in the range (in decimal), we convert this number to base 10 and add 1 to the result..

$$\text{Number of addresses} = (0 \times 256^3 + 0 \times 256^2 + 3 \times 256^1 + 255 \times 256^0) + 1 = 1024$$

KTUStudents.in

Example 6

The first address in a range of addresses is 14.11.45.96. If the number of addresses in the range is 32, what is the last address?

KTUStudents.in

Example 6

The first address in a range of addresses is 14.11.45.96. If the number of addresses in the range is 32, what is the last address?

Solution

We convert the number of addresses minus 1 to base 256, which is 0.0.0.31.

We then add it to the first address to get the last address. Addition is in base 256.

$$\text{Last address} = (14.11.45.96 + 0.0.0.31)_{256} = 14.11.45.127$$

KTUStudents.in

IP Address Scheme Categories

- Conventional (“Classful”) Addressing
  - Dividing line occurs only at octet boundaries
  - A, B, and C depending on how many octets for network ID and host ID
- Subnetted “Classful” Addressing
  - 3 tier system: network ID, subnet ID, host ID
  - Ex: Class C 24 (NID) + 8 (HID)

    24(NID) + 3(SID) + 5 (HID)

KTUStudents.in

CLASSFUL ADDRESSING

KTUStudents.in

CLASSFUL ADDRESSING

IP addresses, when started a few decades ago, used the ***concept of classes***. This architecture is called classful addressing.

In the **mid-1990s**, a new architecture, called classless addressing, was introduced that supersedes the original architecture.

KTUStudents.in

Topics Discussed in the Section

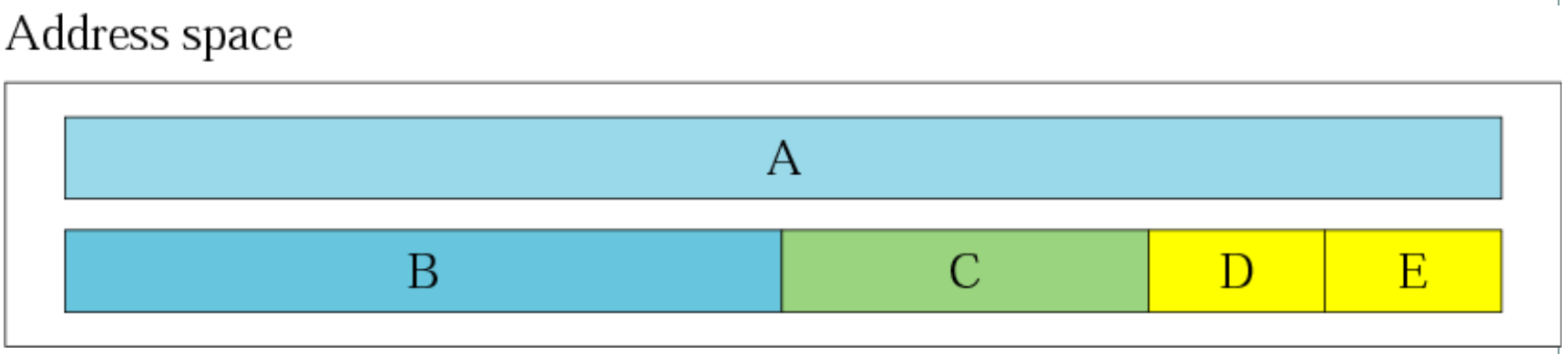
- ✓ Classes
- ✓ Classes and Blocks
- ✓ Two-Level Addressing
- ✓ Three-Level Addressing: Subnetting

Occupation of the address space

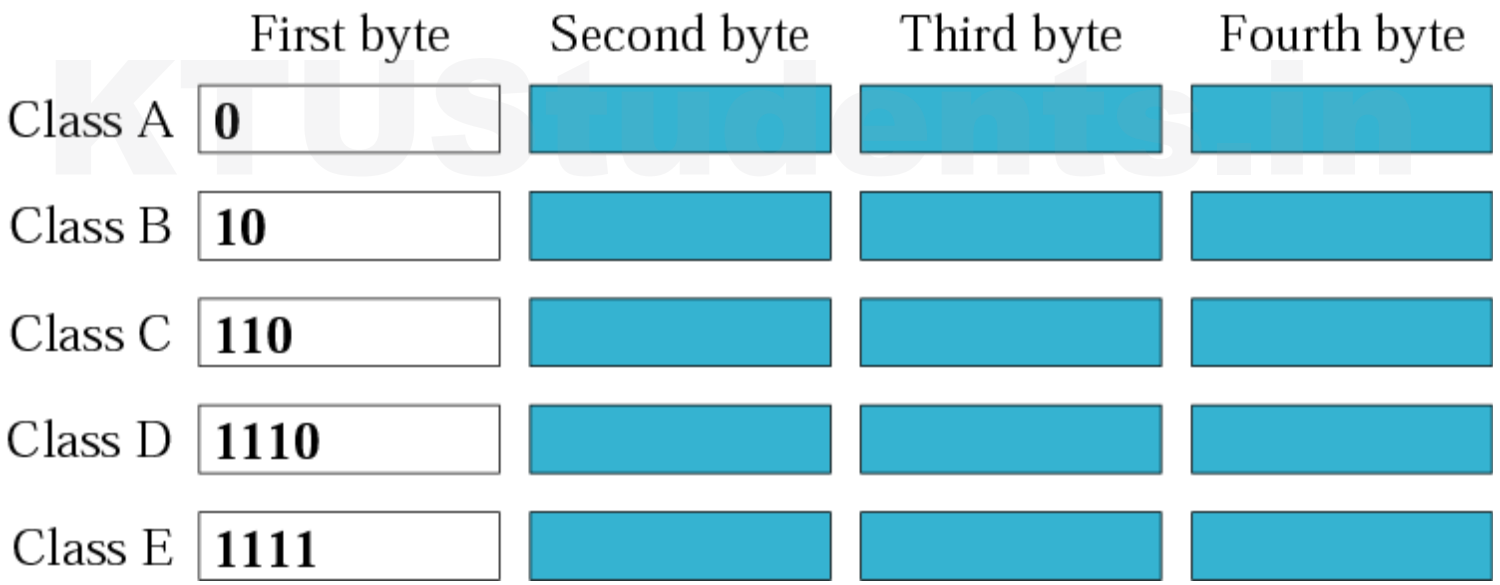
In classful addressing the address space is divided into 5 classes:

A, B, C, D, and E.

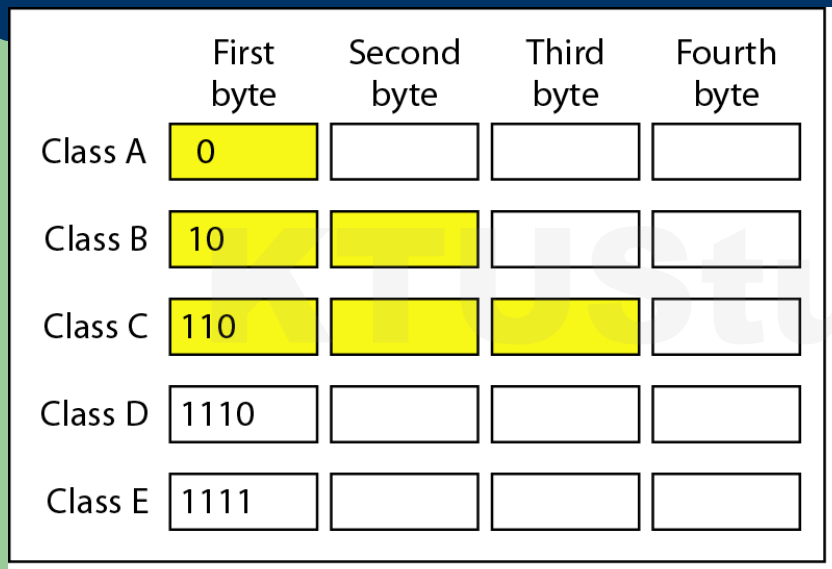
KTUStudents.in



Finding the class in binary notation

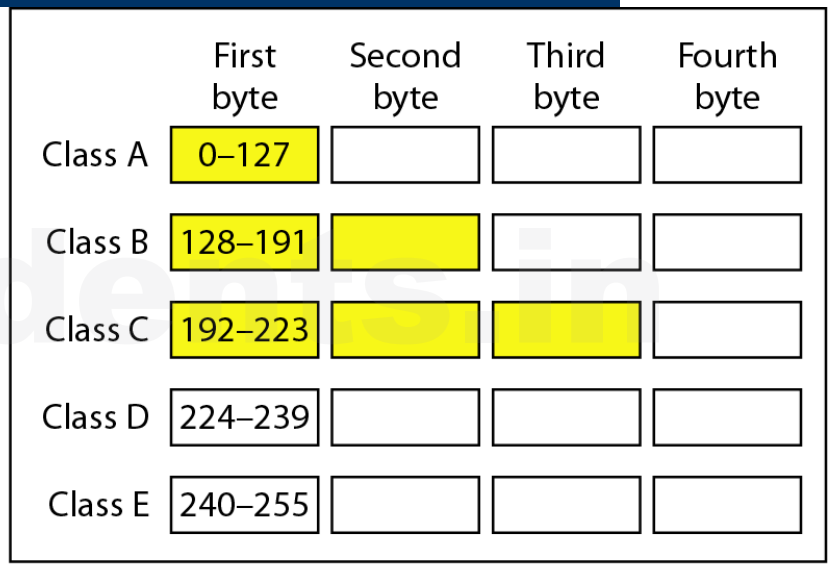


Finding the classes in binary and dotted-decimal notation



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

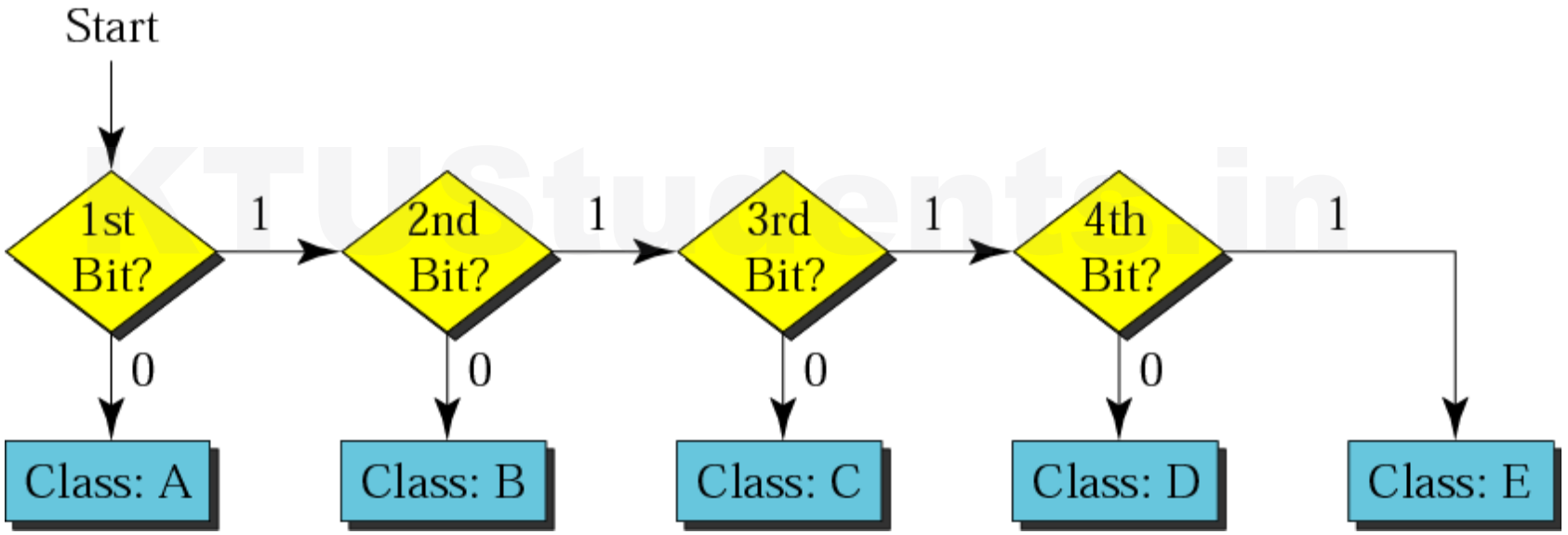


	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

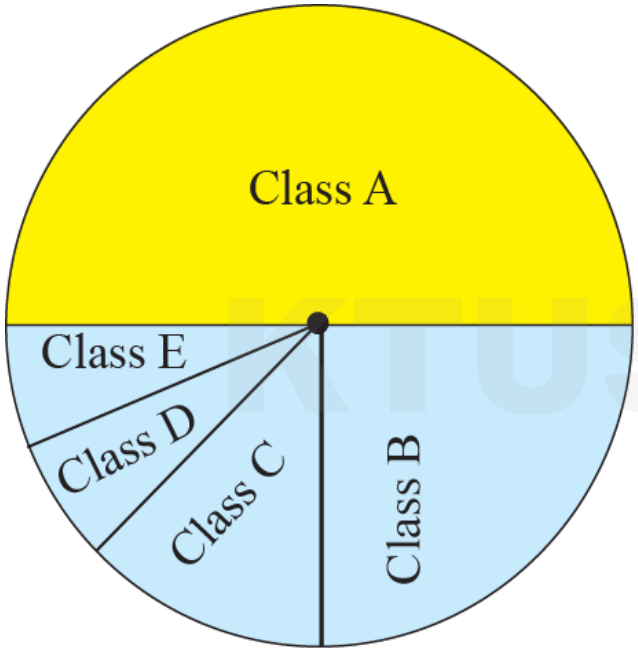
b. Dotted-decimal notation

Class D: multicast
Class E: reserved

Finding the address class



Occupation of address space



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

KTUstudents.in

Introduction *(Cont.)*

- There are only 3 usable IP address classes:
  - Class A
  - Class B
  - Class C
- Class A networks have the highest number of available hosts.
- Class C networks have the fewest number of hosts.

KTUStudents.in

Note

The range of addresses allocated to an organization in classful addressing was a block of addresses in Class A, B, or C.

KTUStudents.in

Note

Class D addresses are used for multicasting; there is only one block in this class.

KTUStudents.in

Note

Class E addresses are reserved for special purposes; most of the block is wasted.

Example 7

Find the class of each address:

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 10100111 11011011 10001011 01101111

d. 11110011 10011011 11111011 00001111

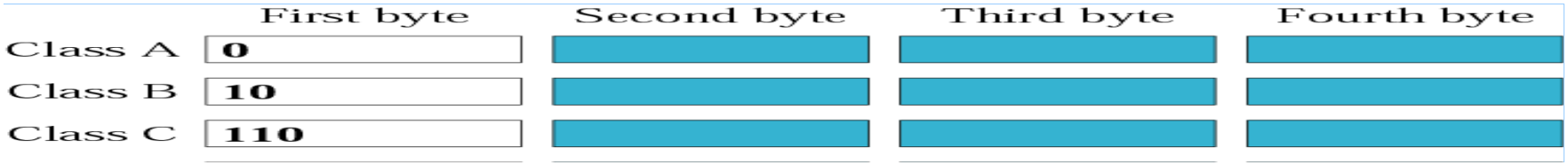
KTUStudents.in

Example 7

a. 00000001 00001011 00001011 11101111
b. 11000001 10000011 00011011 11111111
c. 10100111 11011011 10001011 01101111
d. 11110011 10011011 11111011 00001111

e. Solution

a. The first bit is 0. This is a class A address.
b. The first 2 bits are 1; the third bit is 0. This is a class C address.
c. The first bit is 1; the second bit is 0. This is a class B address.
d. The first 4 bits are 1s. This is a class E address.



Example 8

Find the class of each address:

a. 227.12.14.87

b. 193.14.56.22

c. 14.23.120.8

d. 252.5.15.111

KTUStudents.in

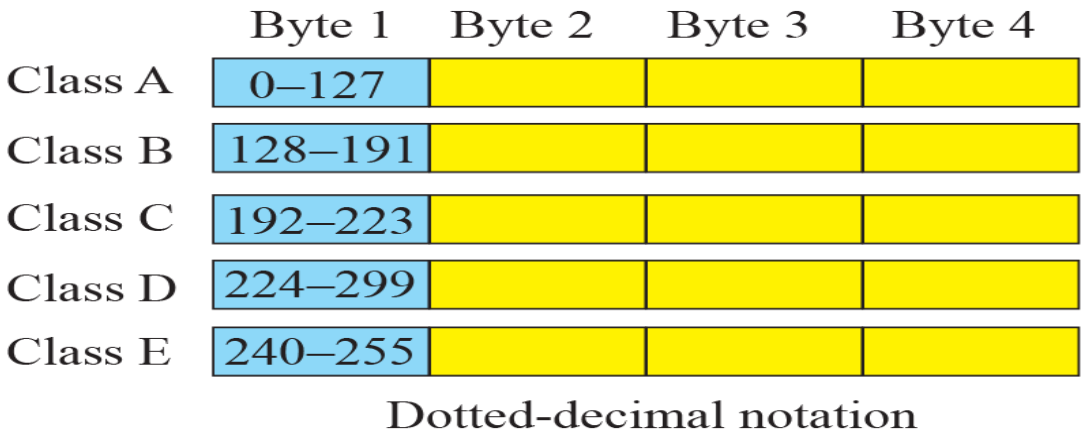
Example 8

a. 227.12.14.87

b. 193.14.56.22

c. 14.23.120.8

d. 252.5.15.111



Solution

a. The first byte is 227 (between 224 and 239); the class is D.

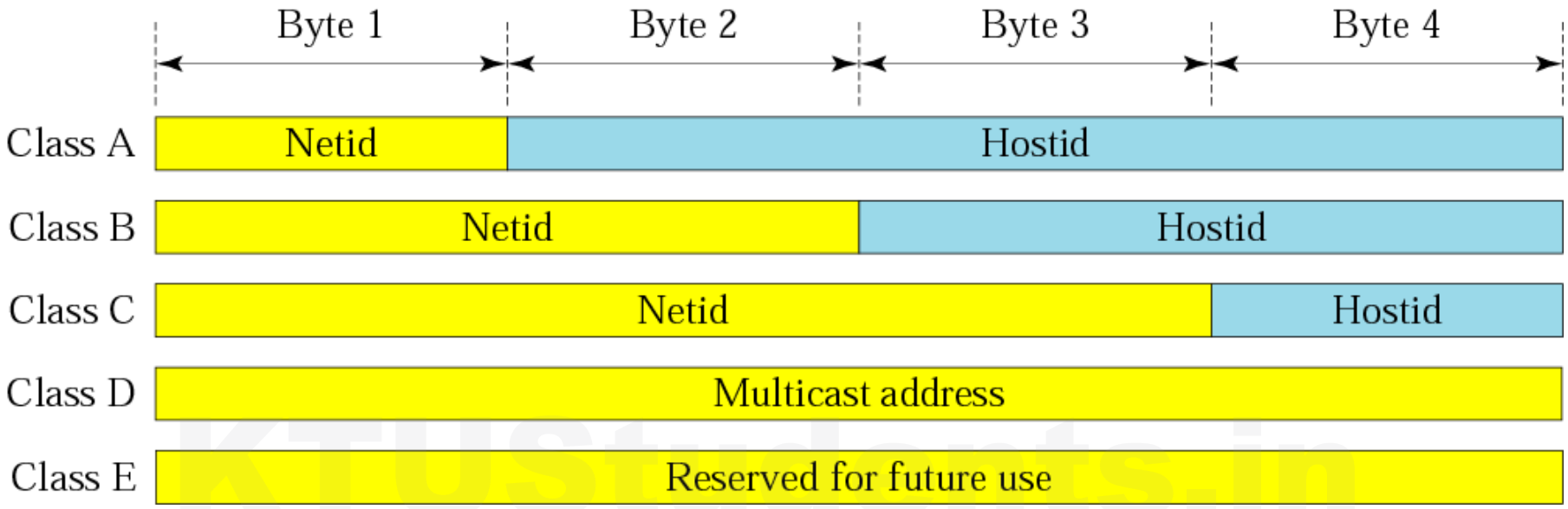
b. The first byte is 193 (between 192 and 223); the class is C.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

KTUStudents.in

Netid and hostid



KTUstudents.in

12.0.0.0/8	AT&T Services
16.0.0.0/8	Hewlett-Packard Company
17.0.0.0/8	Apple Inc.
19.0.0.0/8	Ford Motor Company

Netnumber	Organization
128.001.0.0	BBN Communications
128.002.0.0	Carnegie-Mellon University
128.003.0.0	Lawrence Berkeley National Laboratory
128.004.0.0	University of Delaware

Network Addresses

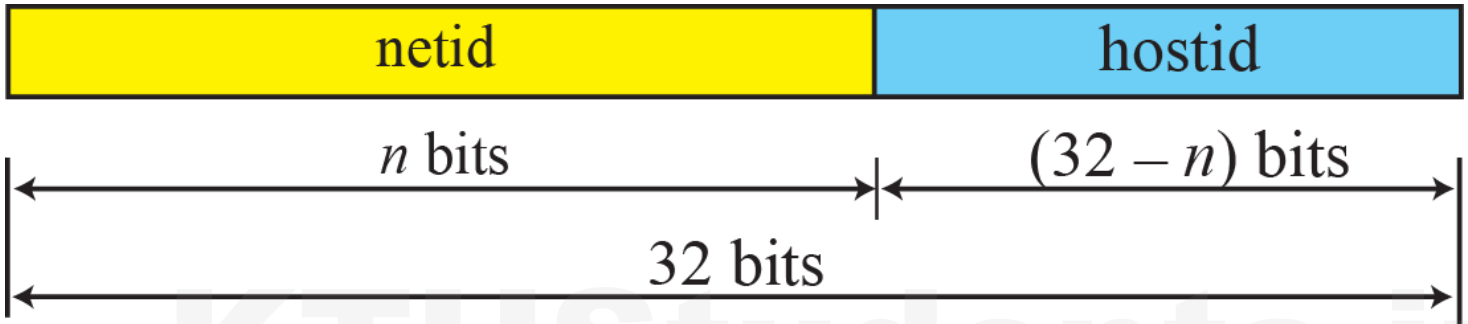
The network address is the first address.

The network address defines the network to the rest of the Internet.

Given the network address, we can find the class of the address, the block, and the range of the addresses in the block

KTUStudents.in

Two-level addressing in classful addressing



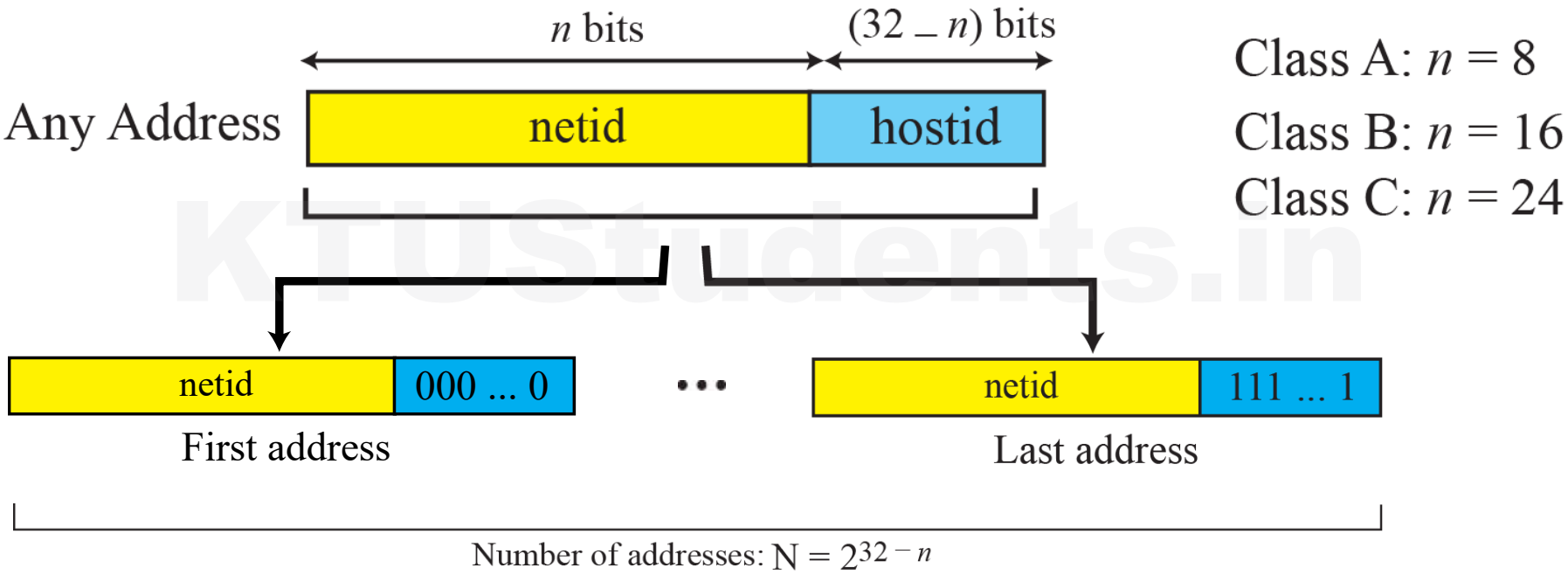
Class A: $n = 8$

Class B: $n = 16$

Class C: $n = 24$

KTUStudents.in

Information extraction in classful addressing



KTUStudents.in

Note

In classful addressing, the network address (the first address in the block) is the one that is assigned to the organization.

KTUstudents.in

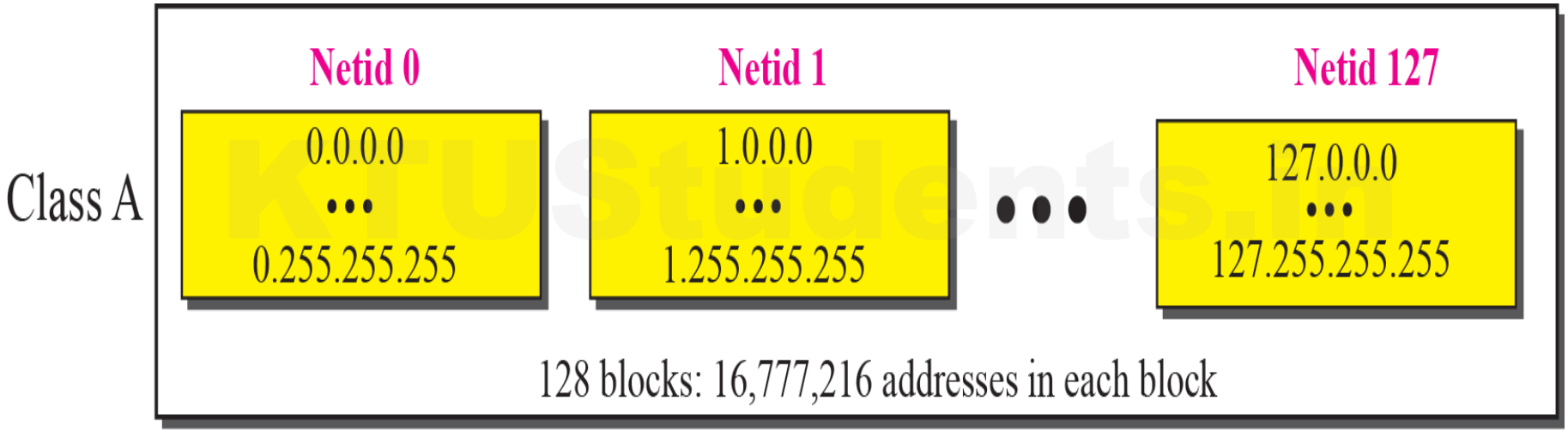
Note

The network address is the identifier of a network.

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

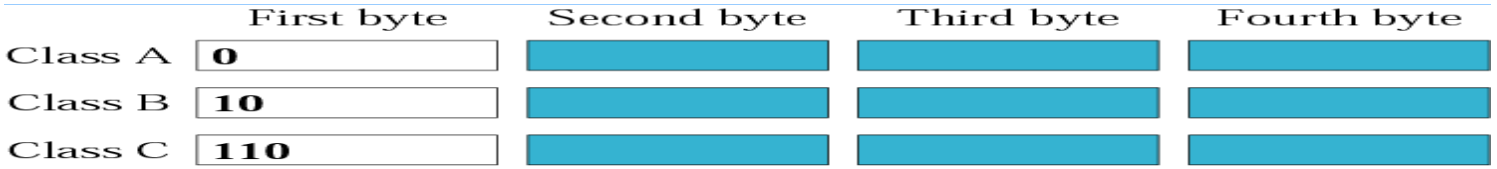
KTUStudents.in

Blocks in Class A



Class A Addresses

- Class A IP addresses use the 1st 8 bits (1st Octet) to designate the Network address.
- The 1st bit which is always a 0, is used to indicate the address as a Class A address & the remaining 7 bits are used to designate the Network.
- The other 3 octets contain the Host address.



KTUStudents.in

Class A Addresses *(Cont.)*

- There are 128(2^7) Class A Network Addresses, but because addresses with all zeros aren't used & address 127 is a special purpose address, 126 (128-2) or [(2^7 – 2)] Class A Networks are available.

KTUstudents.in

Class A Addresses *(Cont.)*

Note: A host address cannot be designated by all zeros or all ones.

➢These are special addresses that are reserved for special purposes.

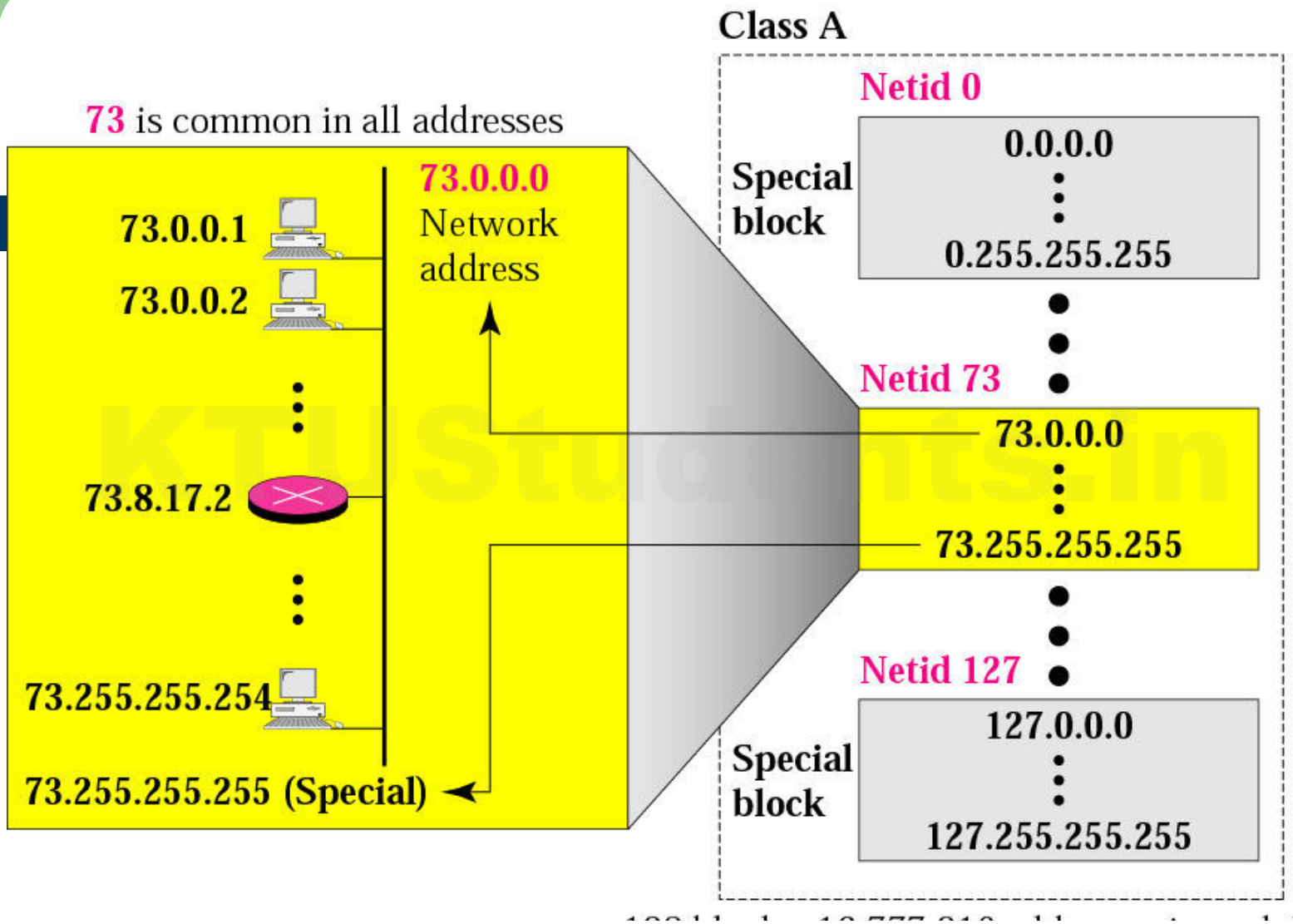
KTUStudents.in

- For **a** Class A network, there are:

  $2^{24} - 2$ or 16,777,214 hosts.

- Half of all IP addresses are Class A addresses.
- Class A address uses 7 bits to designate the network, so $(2^7 - 2) = 126$ or there can be 126 Class A Networks.

Blocks in class A



Note

Millions of class A addresses are wasted.

Class B IP Addresses

- Class B addresses use the 1st 16 bits (two octets) for the Network address.
- The last 2 octets are used for the Host address.
- The 1st 2 bit, which are always 10, designate the address as a Class B address & 14 bits are used to designate the Network. This leaves 16 bits (two octets) to designate the Hosts.

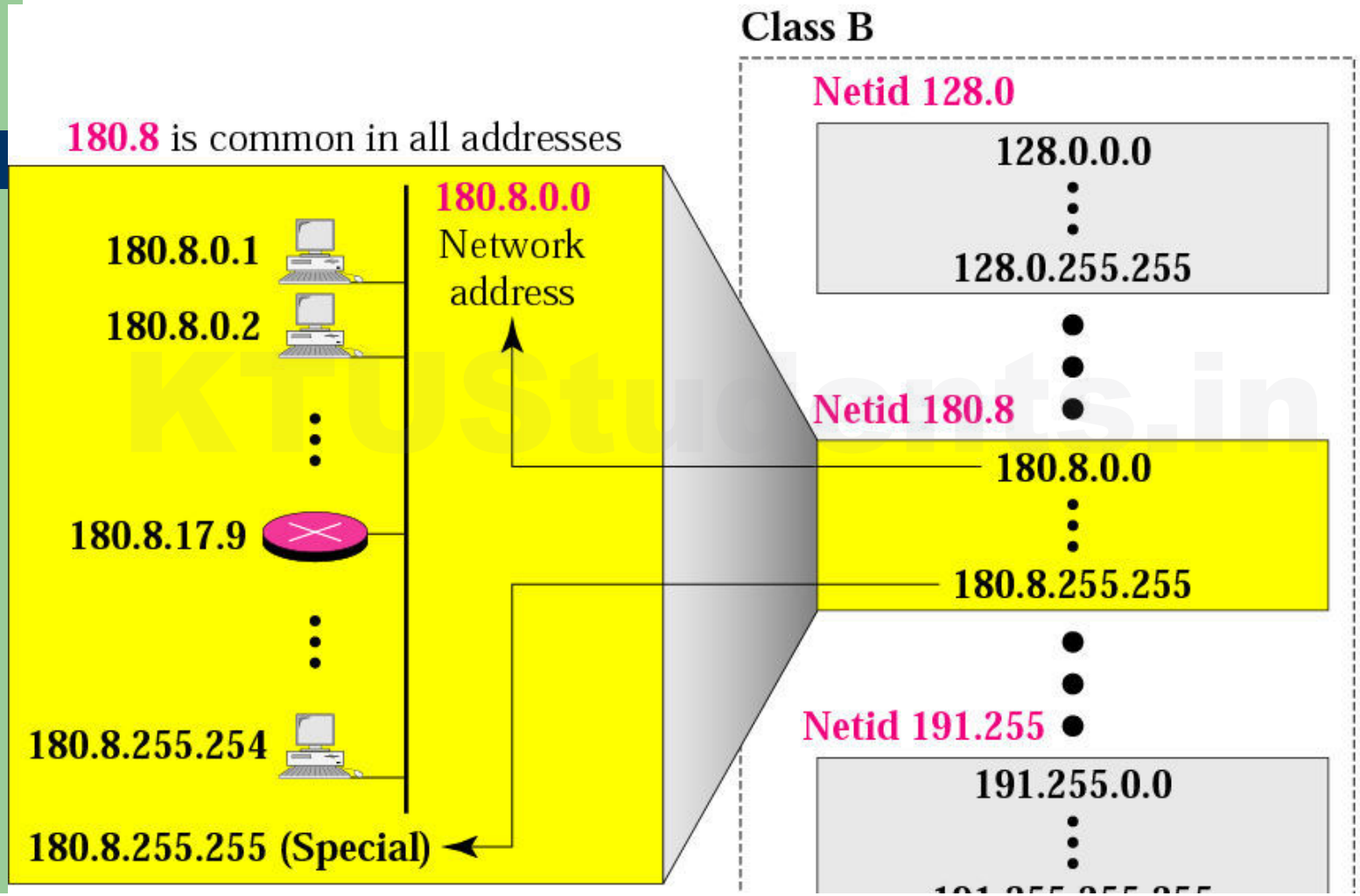
KTUStudents.in

Class B IP Addresses *(Cont.)*

- So how many Class B Networks can there be?
- Using our formula, $(2^{14} - 2)$, there can be 16,382 Class B Networks & each Network can have $(2^{16} - 2)$ Hosts, or 65,534 Hosts.

KTUStudents.in

Blocks in class B



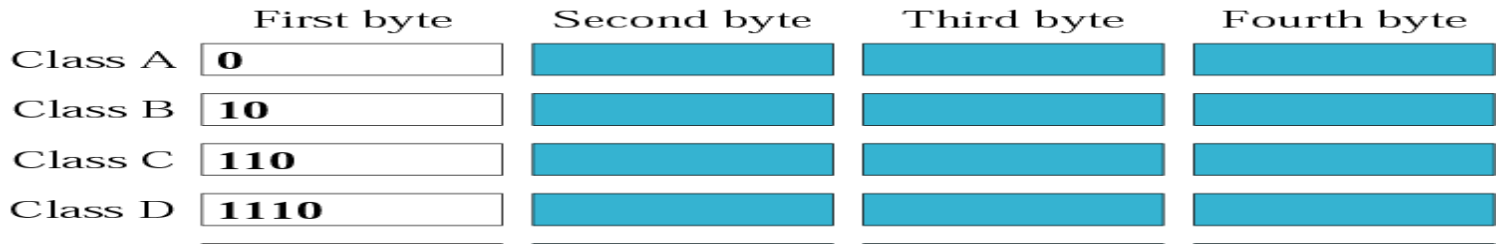
Note

Many class B addresses are wasted.

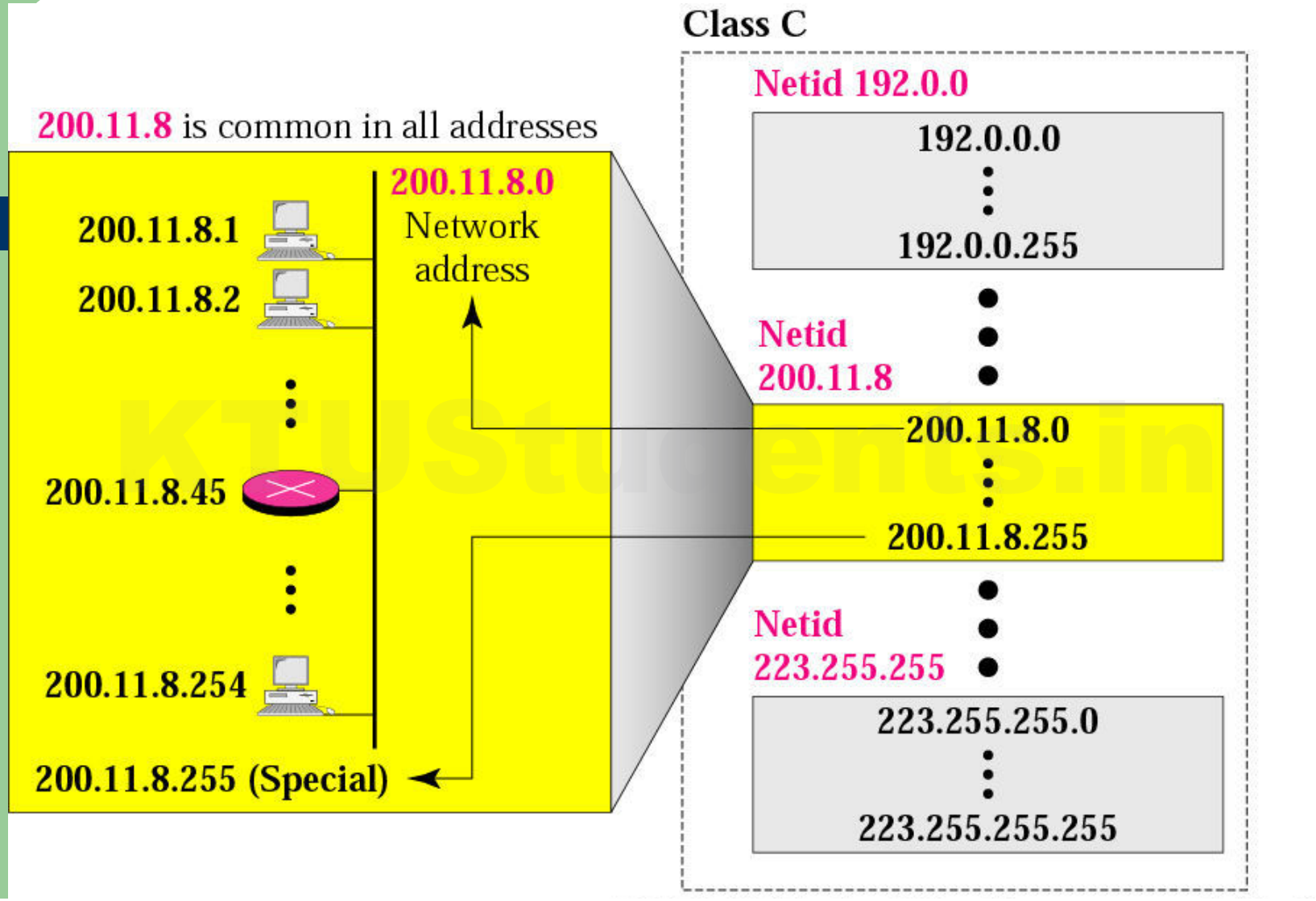
Class C IP Addresses

- Class C addresses use the 1st 24 bits (three octets) for the Network address & only the last octet for Host addresses.
- The 1st 3 bits of all class C addresses are set to 110, leaving 21 bits for the Network address, which means there can be 2,097,150 ($2^{21} - 2$) Class C Networks, but only 254 ($2^8 - 2$) Hosts per Network.

ktustudents.in



Blocks in class C



Note

The number of addresses in a class C block is smaller than the needs of most organizations.

KTUStudents.in

Class C IP Addresses *(Cont.)*

Characteristics of the IP Address Classes						
Class	Address Range	Identify Bits (binary value)	Bits in Network ID	Number of Networks	Bits in Host ID	Number of Hosts/ Network
A	0 ~ 127	1 (0)	7	126	24	16,777,214
B	128~191	2 (10)	14	16,382	16	5,534
C	192~223	3 (110)	21	2,097,150	8	254

Example 8

Given the network address 132. 21. 0. 0, find the class, the block, and the range of the addresses

KTUStudents.in

Example 8

Solution

132. 21. 0. 0

1. The 1st byte is between 128 and 191. Hence, Class B

2. The block has a ***netid of 132.21***.

3.The addresses range from

132.21.0.0 to 132.21.255.255

krishstudents.in

Example 9

An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address, and the last address.

KTUStudents.in

Example 9

An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address, and the last address.

Solution

Figure 9 shows a possible configuration of the network that uses this block (Class A).

1. The number of addresses in this block is $N = 2^{32-n} =$ 16,777,216.

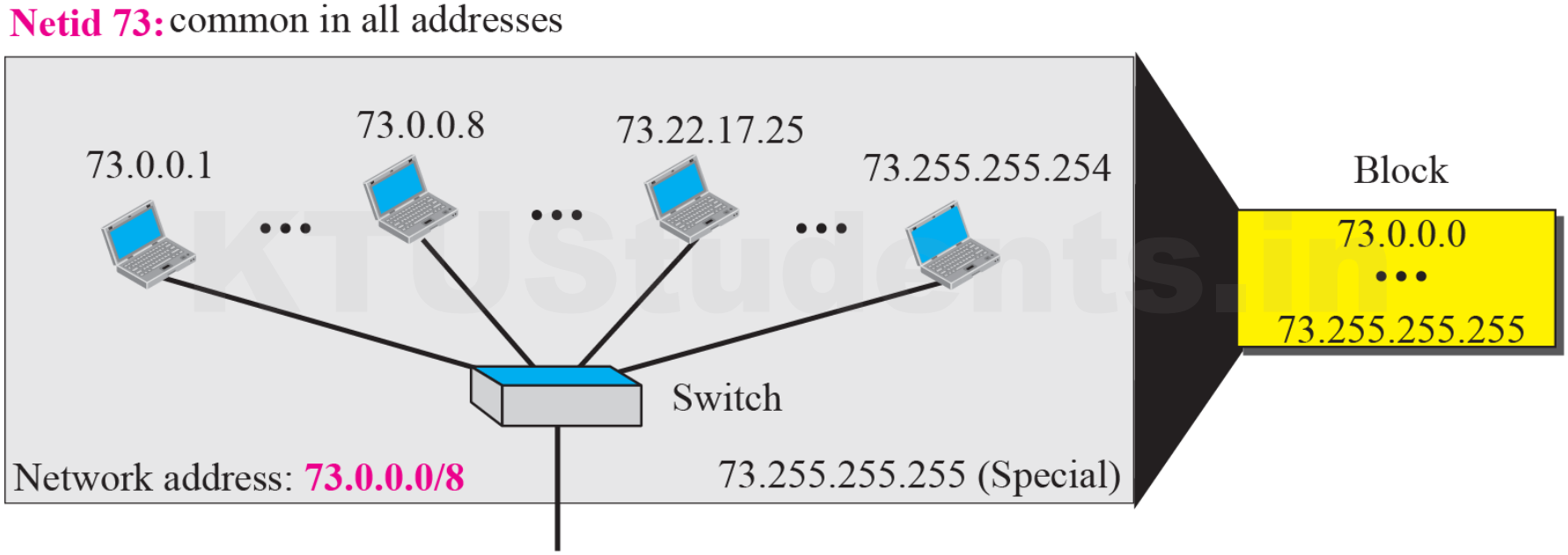
in which 8 is the value of *n*.

2. To find the first address, we keep the leftmost 8 bits and set the rightmost 24 bits all to 0s. The first address is 73.0.0.0,

3. To find the last address, we keep the leftmost 8 bits and set the rightmost 24 bits all to 1s. The last address is 73.255.255.255.

KTUStudents.in

Figure 9 *Solution to Example 9*



Example 10

An address in a block is given as 180.8.17.9. Find the number of addresses in the block, the first address, and the last address.

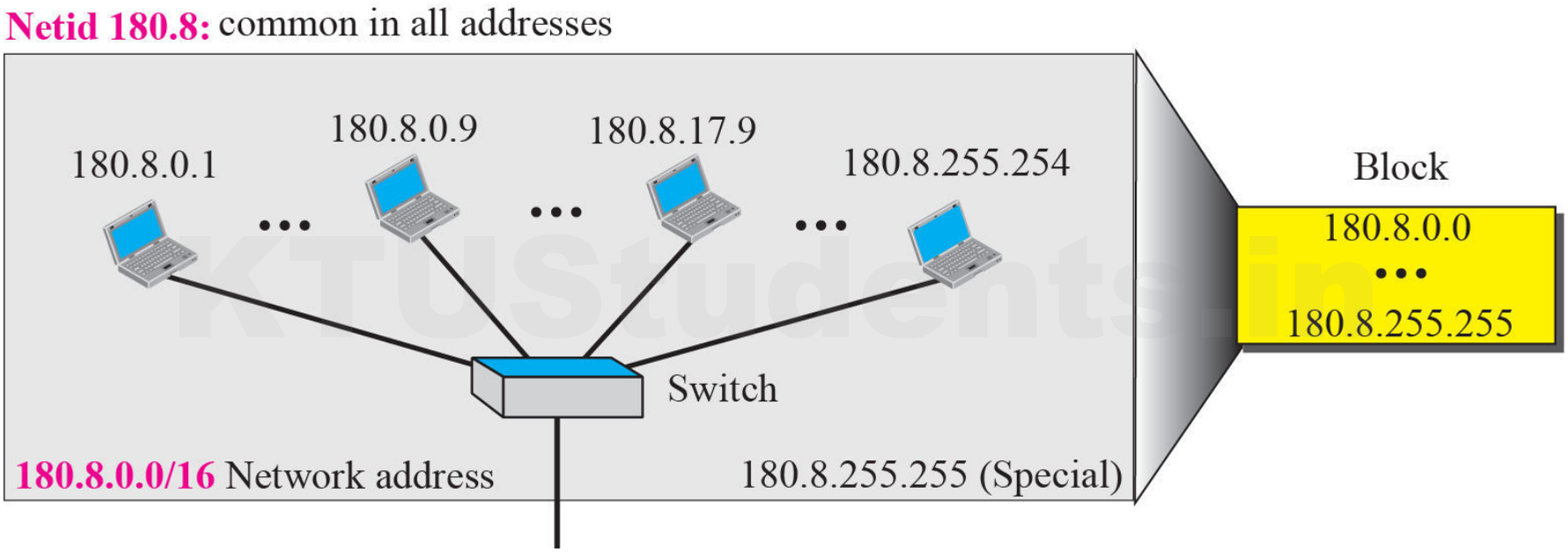
Solution

Figure 10 shows a possible configuration of the network that uses this block (Class B).

1. The number of addresses in this block is $N = 2^{32-n} = 65,536$.
2. To find the first address, we keep the leftmost 16 bits and set the rightmost 16 bits all to 0s. The first address is 180.8.0.0, in which 16 is the value of *n*.
3. To find the last address, we keep the leftmost 16 bits and set the rightmost 16 bits all to 1s. The last address is 180.8.255.255.

KTUStudents.in

Figure 10 *Solution to Example 10*



Example 11

An address in a block is given as 200.11.8.45. Find the number of addresses in the block, the first address, and the last address.

Solution

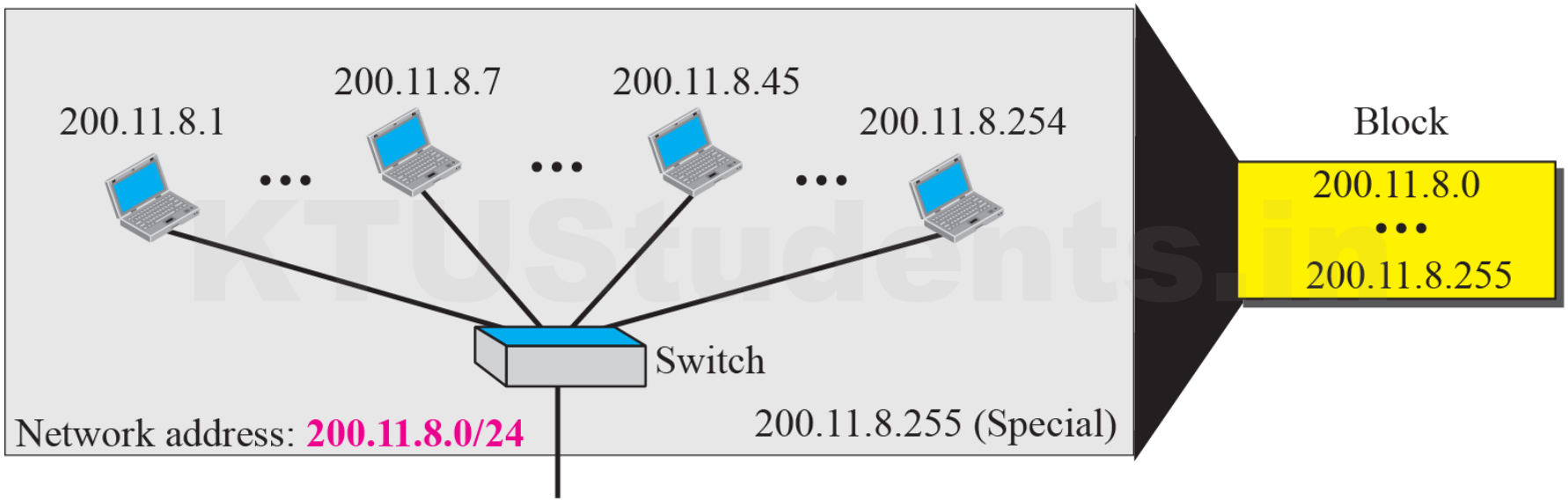
Figure 11 shows a possible configuration of the network that uses this block (Class C).

1. The number of addresses in this block is $N = 2^{32-n} = 256$.
2. To find the first address, we keep the leftmost 24 bits and set the rightmost 8 bits all to 0s. The first address is 200.11.8.0, in which 24 is the value of *n*.
3. To find the last address, we keep the leftmost 24 bits and set the rightmost 8 bits all to 1s. The last address is 200.11.8.255.

KTUStudents.in

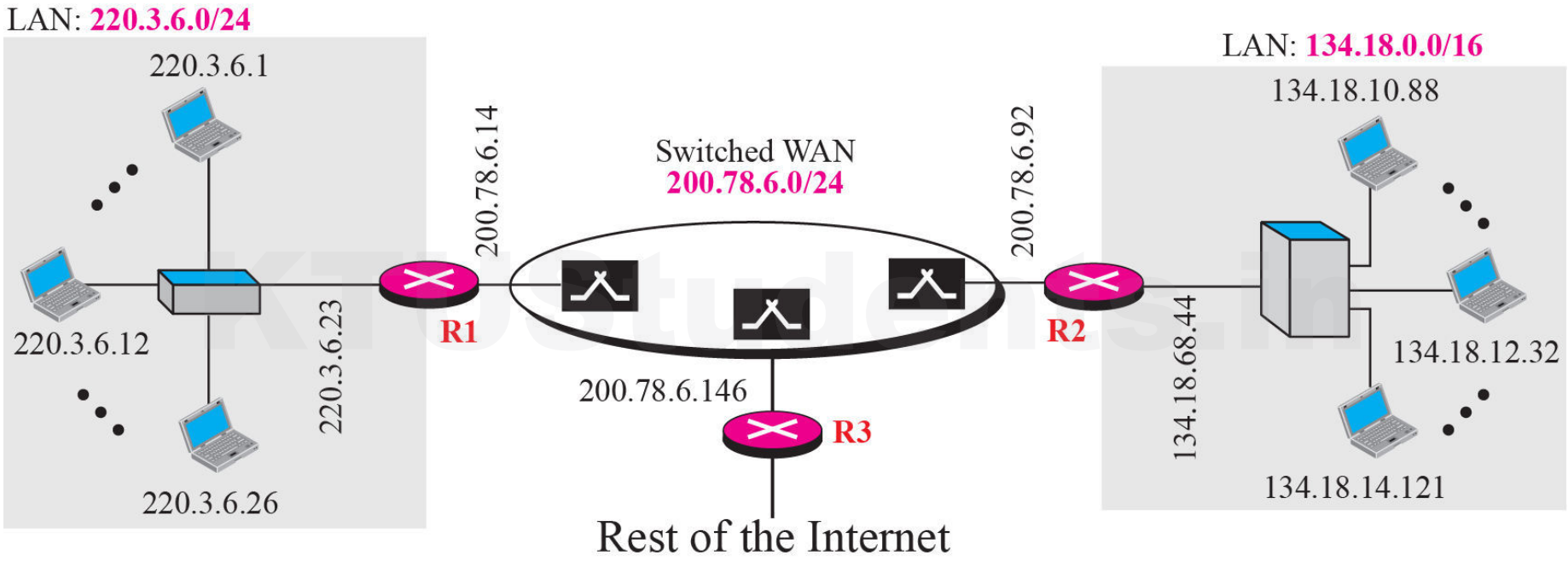
Solution to Example 11

Netid 200.11.8: common in all addresses

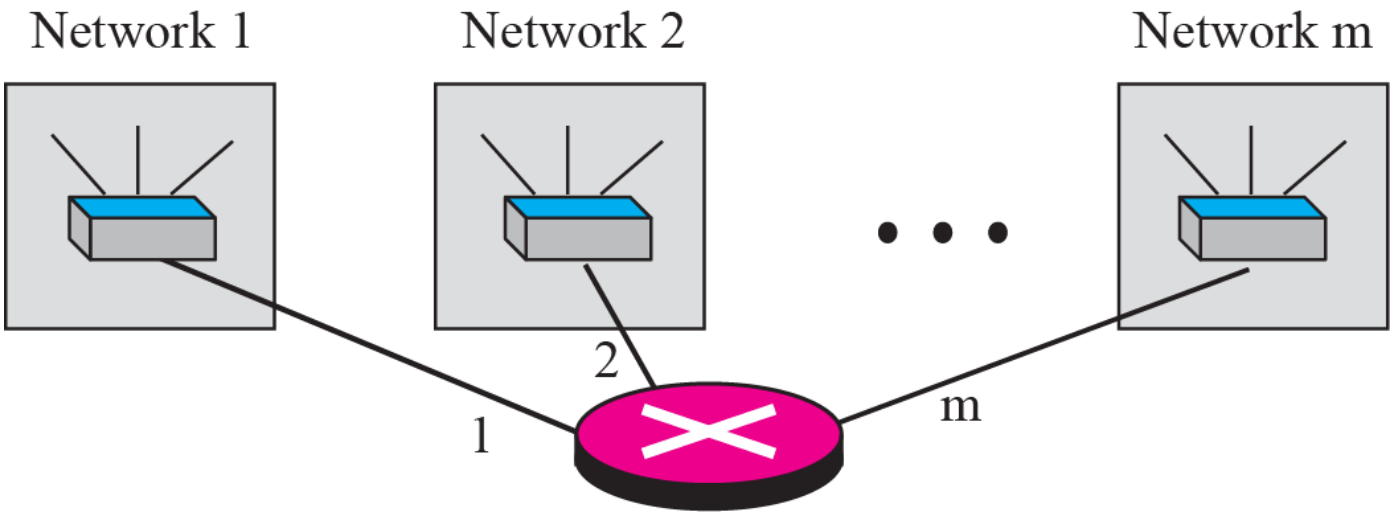


KTUStudents.in

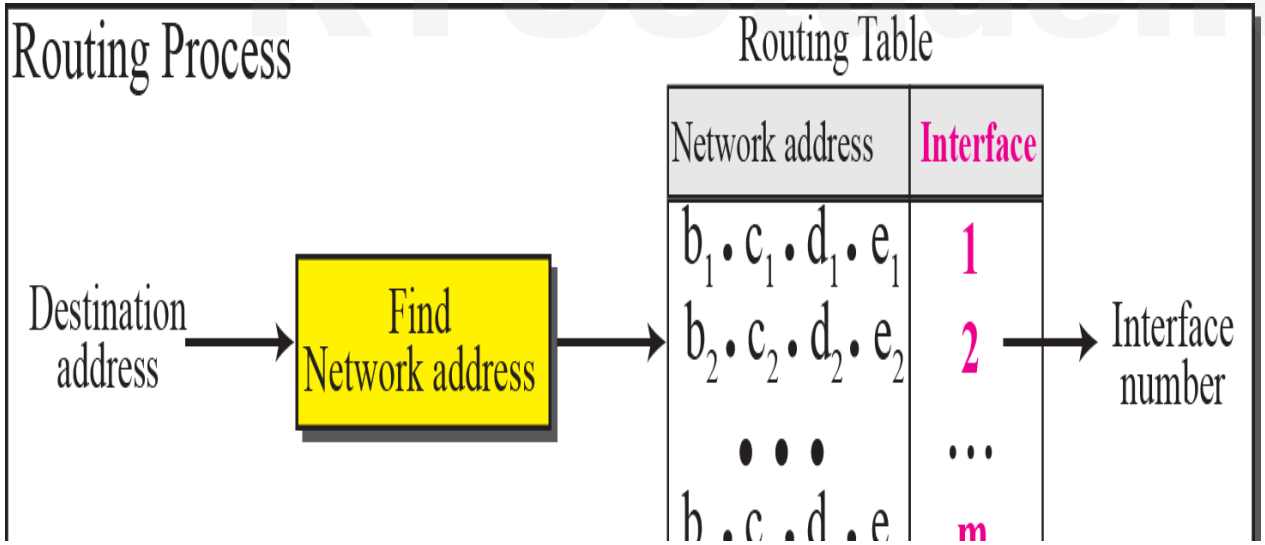
Sample Internet



Network addresses



KTUStudents.in

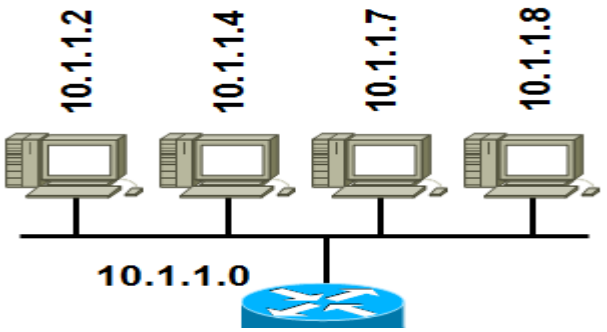


5.0.0.0/8	RIPE NCC
9.0.0.0/8	ARIN
13.0.0.0/8	ARIN
14.0.0.0/8	APNIC

Are You the Host or the Network?

(Cont.)

- Each Network is assigned a network address & every device or interface (such as a router port) on the network is assigned a host address.
- There are only 2 specific value of the address.



Subnet Mask

- An IP address has 2 parts:
  - The Network identification.
  - The Host identification.
- Frequently, the Network & Host portions of the address need to be separately extracted.
- In most cases, if you know the address class, it's easy to separate the 2 portions.

KTUStudents.in

Subnet Mask *(Cont.)*

- The subnet masking process was developed to identify & extract the Network part of the address.
- A subnet mask, which contains a binary bit pattern of ones & zeros, is applied to an address to determine whether the address is on the local Network.
- If it is not, the process of routing it to an outside network begins

KTUStudents.in

Subnet Mask *(Cont.)*

- The function of a subnet mask is to determine whether an IP address exists on the local network or whether it must be routed outside the local network.
- It is applied to a message's destination address to extract the network address.
- If the extracted network address matches the local network ID, the destination is located on the local network

Subnet Mask *(Cont.)*

- However, if they don't match, the message must be routed outside the local network.
- The process used to apply the subnet mask involves Boolean Algebra to filter out non-matching bits to identify the network address.

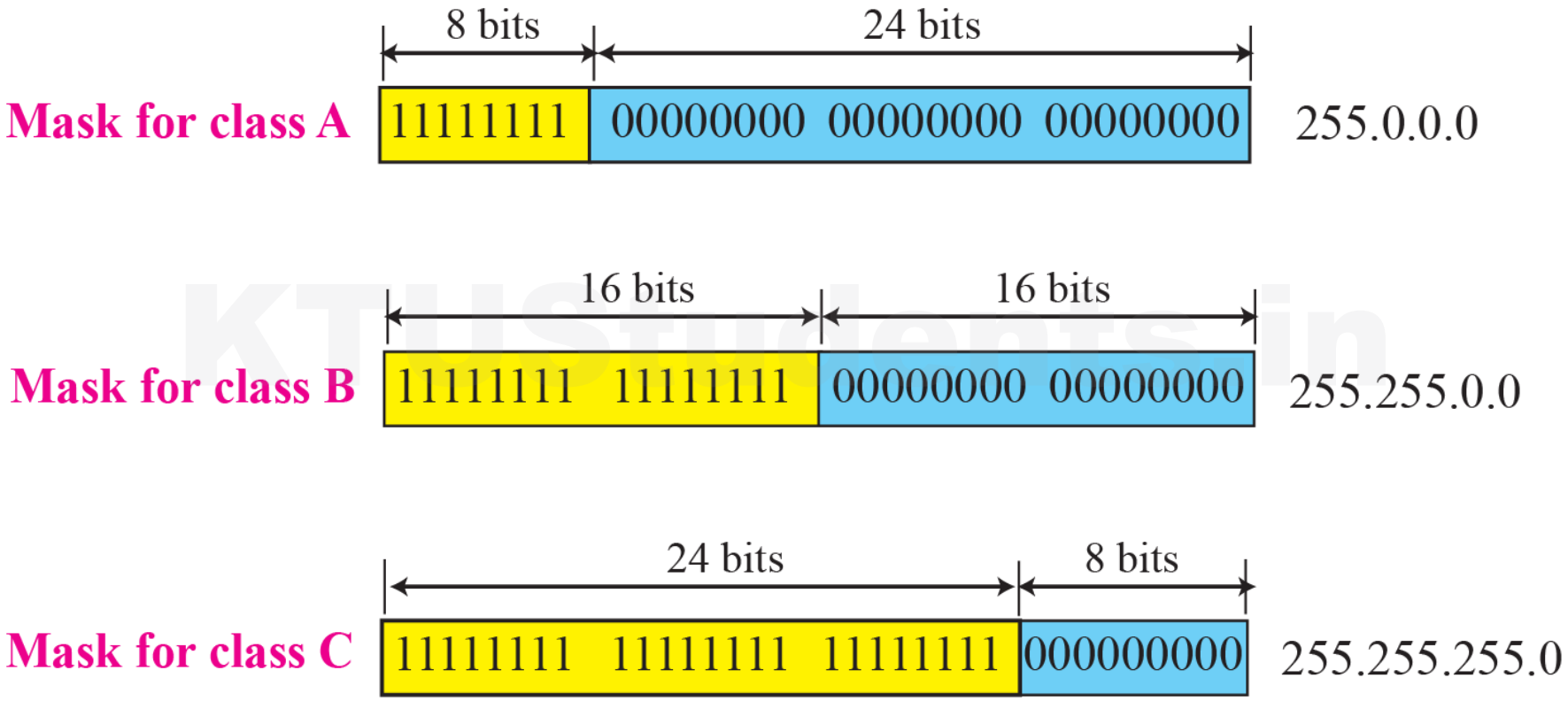
KTUStudents.in

A Trial Separation

- Subnet masks apply only to Class A, B or C IP addresses.
- The subnet mask is like a filter that is applied to a message's destination IP address.
- Its objective is to determine if the local network is the destination network.

KTUStudents.in

Network mask



Default Standard Subnet Masks

- There are default standard subnet masks for Class A, B and C addresses:

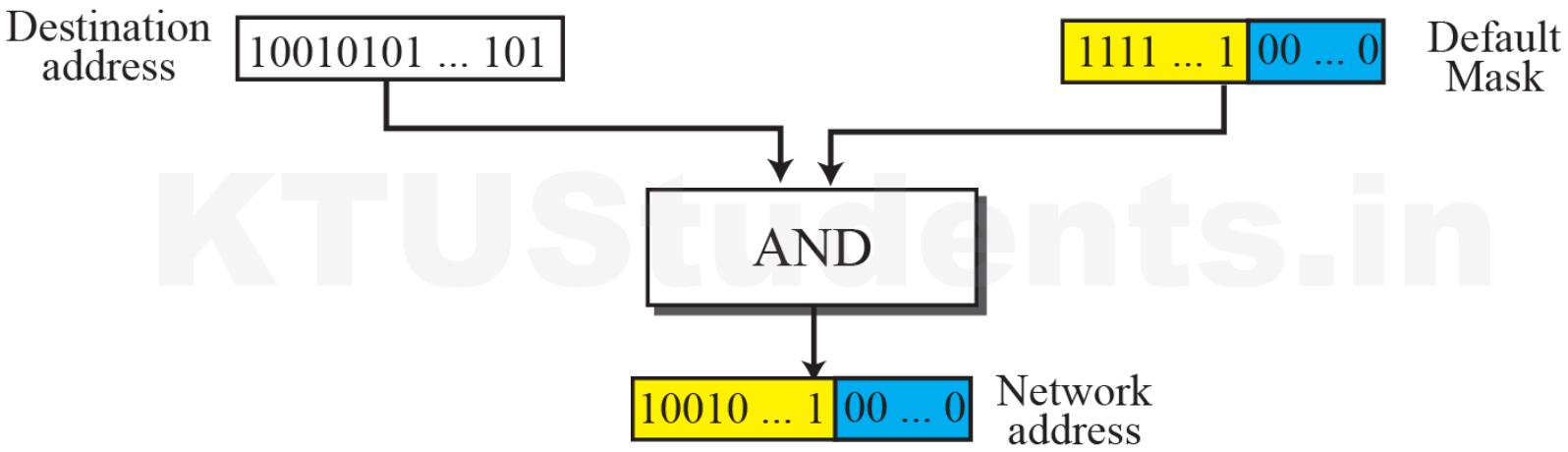
Default Subnet Masks	
Address Class	***Subnet Mask***
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Mask

- A mask is a 32-bit binary number.
- The mask is ANDeD with IP address to get
  - The bloc address (Network address)
  - Mask And IP address = Block Address

KTUStudents.in

Finding a network address using the default mask



KTUStudents.in

Subnetting Networks ID

- A 3-step example of how the default Class A subnet mask is applied to a Class A address:

KTUStudents.in

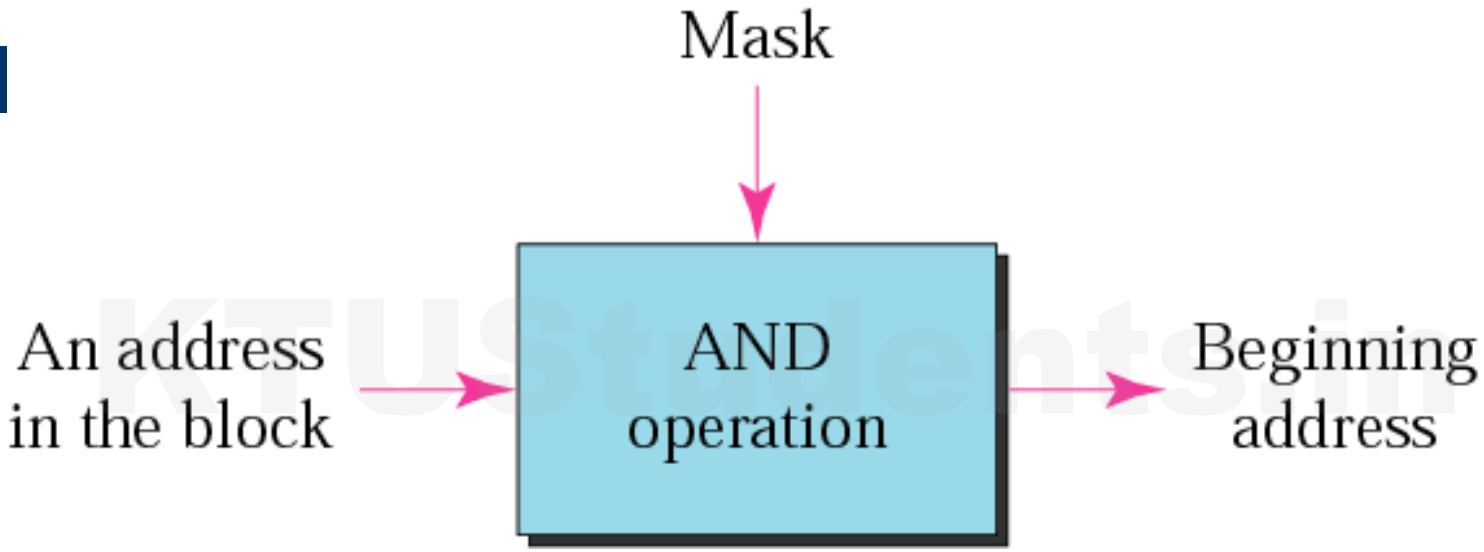
Decimal		Binary
IP Address	123.123.123.001	01111011.01111011.01111011.00000001
Subnet Mask	255.0.0.0	11111111.00000000.00000000.00000000
Network ID	123.0.0.0	01111011.00000000.00000000.00000000

Note

The network address is the beginning address of each block. It can be found by applying the default mask to any of the addresses in the block (including itself). It retains the netid of the block and sets the hostid to zero.

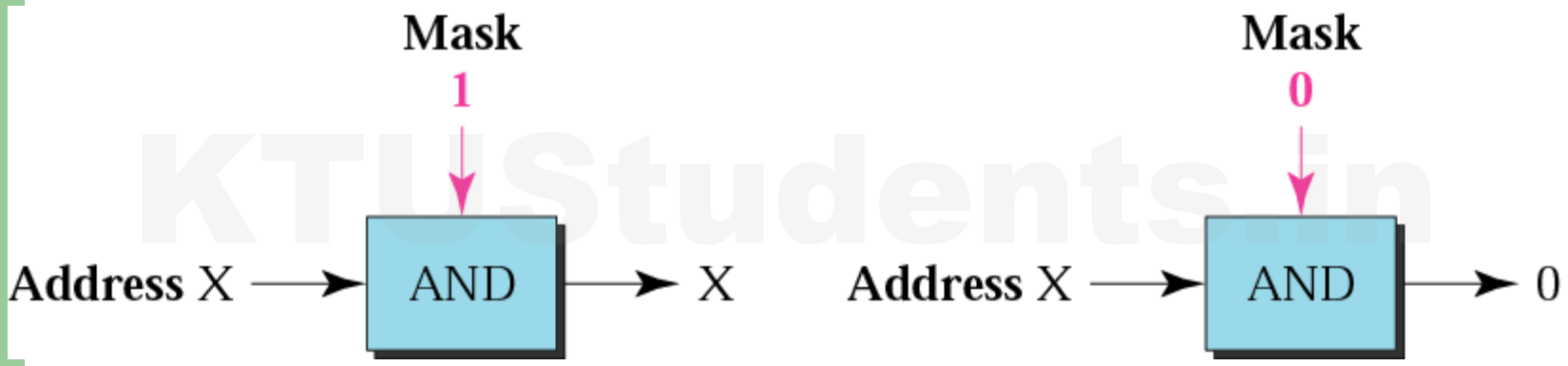
KTUStudents.in

Masking concept



KTUStudents.in

AND operation



KTUStudents.in

Example 11

- The subnet mask goes like this:

1. If a destination IP address is 206.175.162.21, we know that it is a Class C address & that its binary equivalent is:
   11001110.10101111.10100010.00010101

KTUStudents.in

Example 11

3. When these two binary numbers (the IP address & the subnet mask) are combined using Boolean Algebra, the Network ID of the destination network is the result:

206.175.162.21	11001110.10101111.10100010.00010101
and	
255.255.255.0	11111111.11111111.11111111.00000000
yields	
	11001110.10101111.10100010.00000000

4. The result is the IP address of the network which in this case is the same as the local network & means that the message is for a node on the local network.

KTUStudents.in

Module 4

Routing: Routing and Forwarding, Static routing and Dynamic Routing

Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm)

Routing Protocols: Routing Information protocol (RIP), Open

Shortest Path First (OSPF), Border Gateway Protocol (BGP),MPLS

DOWNLOADED FROM KTUASSIST.IN

Network Layer

- This module describes the delivery, forwarding and routing of IP packets to their final destinations
- Delivery refers to the way a packet is handled by the underlying networks under the control of the network layer
- Forwarding refers to the way a packet is delivered to the next station
- Routing refers to the way routing tables are created to help in forwarding
- Routing protocols are used to continuously update the routing tables that are consulted for forwarding and routing

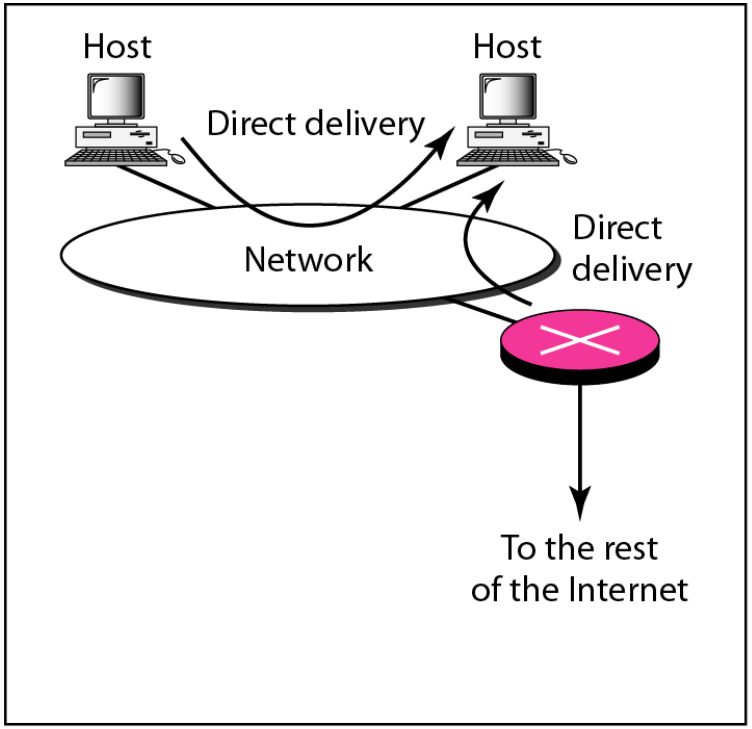
DOWNLOADED FROM KTUASSIST.IN

Delivery

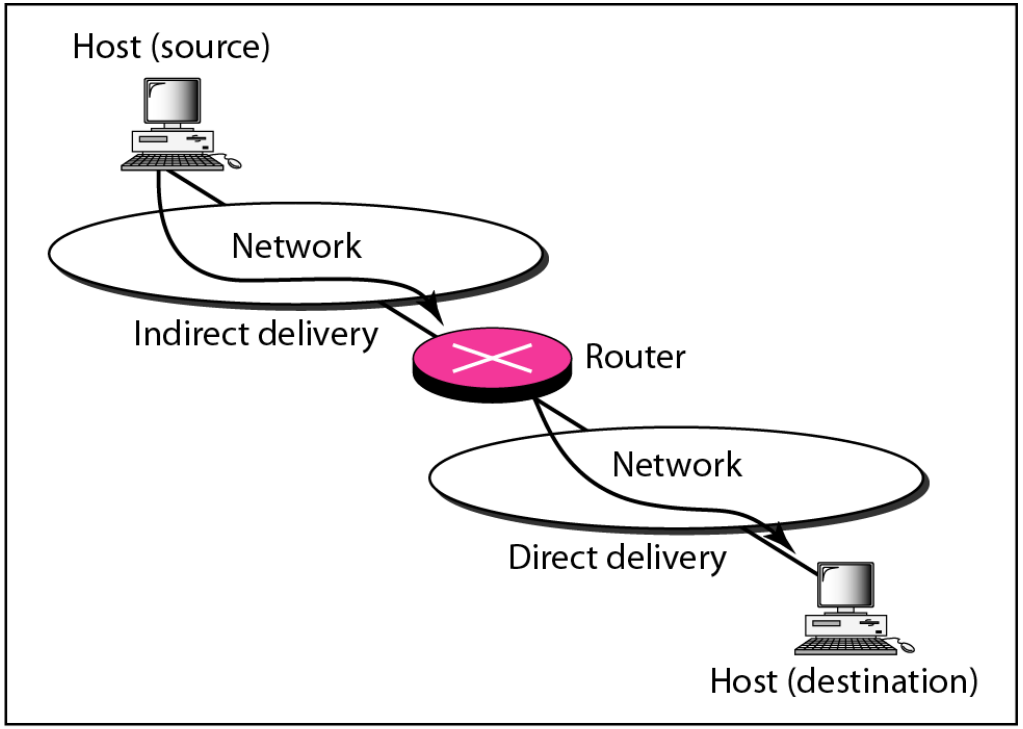
- The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.
- The delivery of a packet to its final destination is accomplished by using two different methods of delivery, direct and indirect.

DOWNLOADED FROM KTUASSIST.IN

Direct and Indirect delivery



a. Direct delivery



b. Indirect and direct delivery

DOWNLOADED FROM KTUASSIST.IN

Direct Delivery

- Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host

DOWNLOADED FROM KTUASSIST.IN

Indirect Delivery

- If the destination host is not on the same network as the deliverer, the packet is delivered indirectly.
- In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination
- Note that the last delivery is always a direct delivery

DOWNLOADED FROM KTUASSIST.IN

FORWARDING

- Forwarding means to place the packet in its route to its destination.
- Forwarding requires a host or a router to have a routing table.
- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

DOWNLOADED FROM KTUASSIST.IN

Forwarding Techniques

- Several techniques can make the size of the routing table manageable and also handle issues such as security
  - Next-Hop Method versus Route Method
  - Network –Specific Method Versus Host-Specific Method
  - Default Method

DOWNLOADED FROM KTUASSIST.IN

Route method versus next-hop method

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

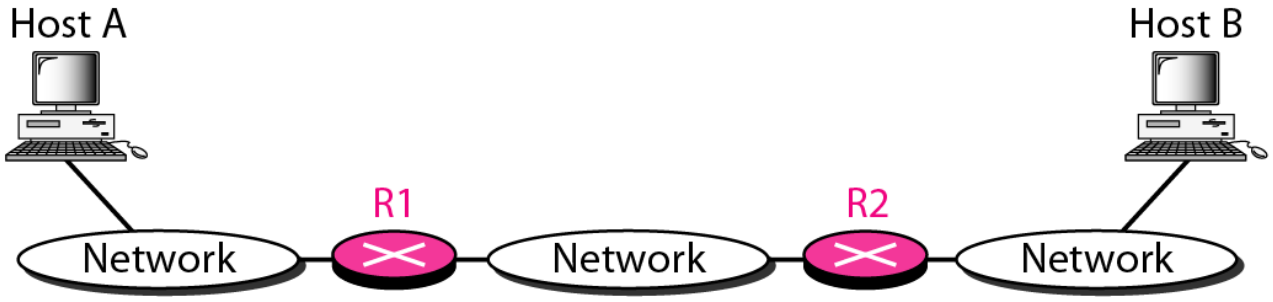
Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

Destination	Next hop
Host B	---



DOWNLOADED FROM KTUASSIST.IN

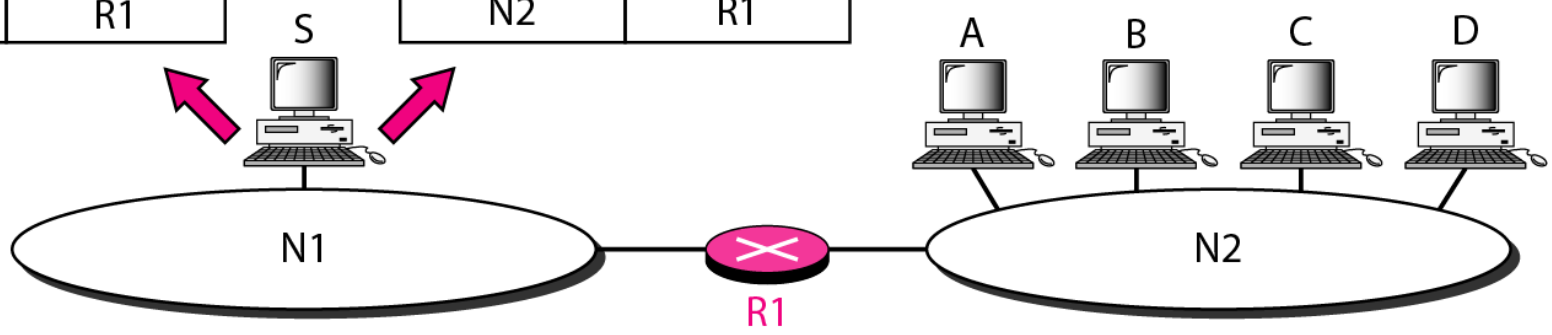
Host-specific versus Network-specific method

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

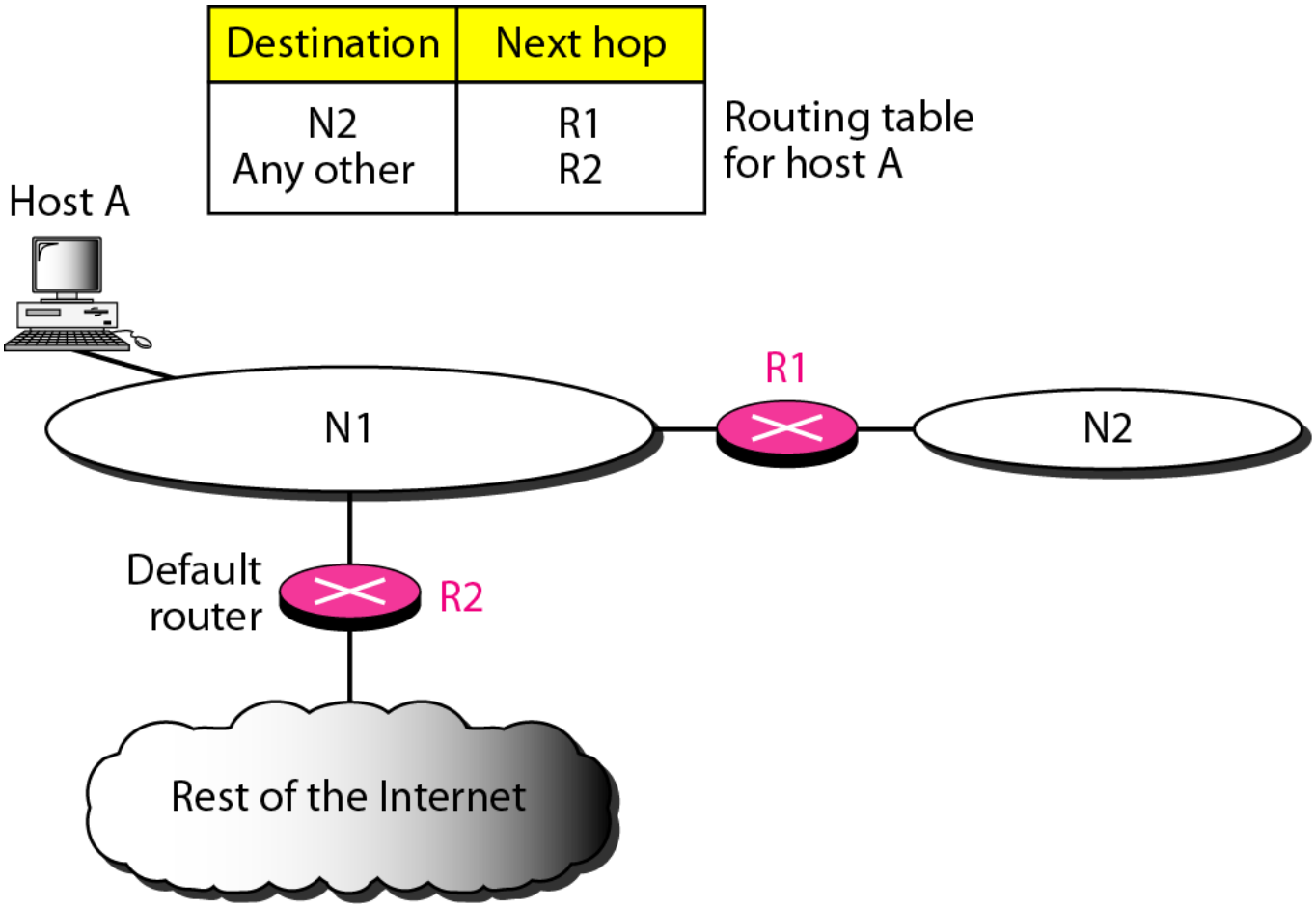
Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



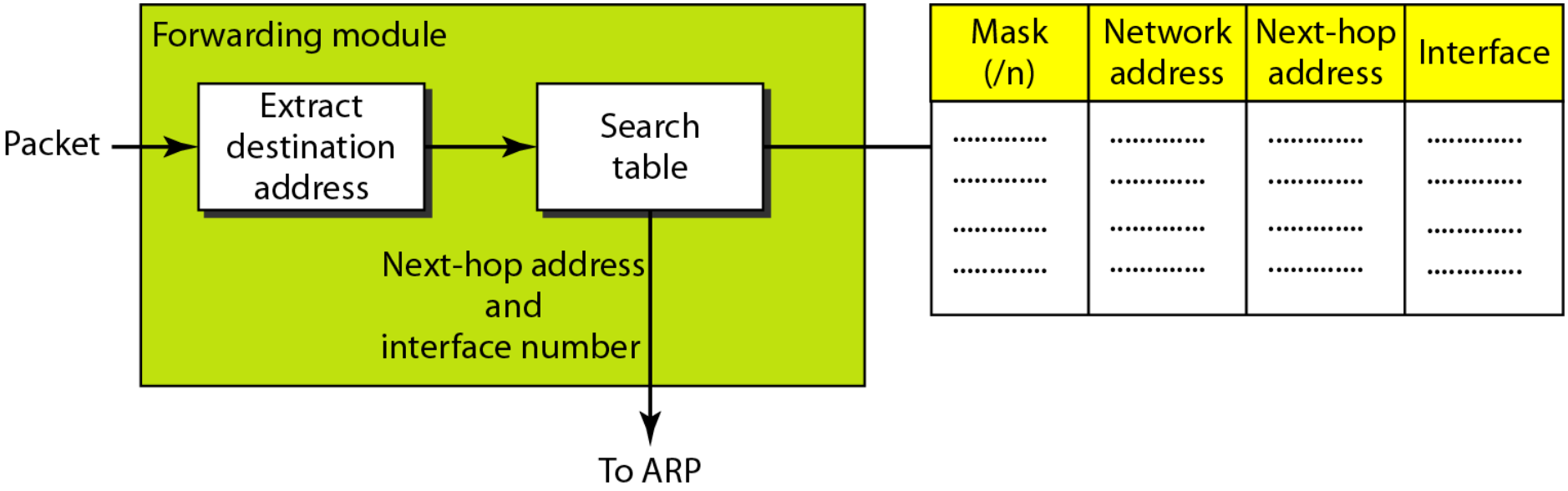
DOWNLOADED FROM KTUASSIST.IN

Default method



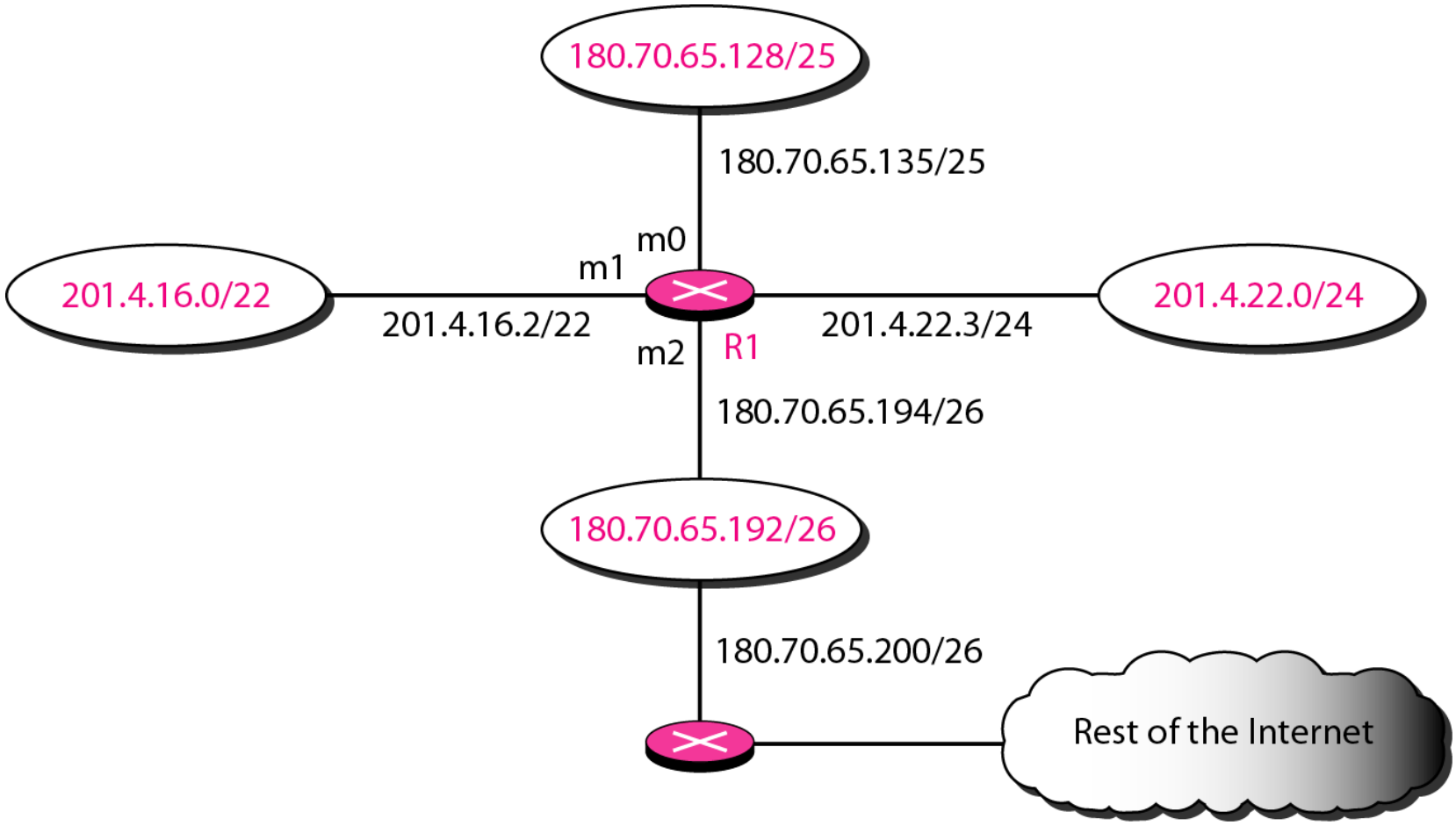
DOWNLOADED FROM KTUASSIST.IN

Simplified forwarding module in classless address



DOWNLOADED FROM KTUASSIST.IN

Make a routing table for router R1, using the configuration in Figure



DOWNLOADED FROM KTUASSIST.IN

Routing table for router

Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

DOWNLOADED FROM KTUASSIST.IN

Forwarding Process

- Show the forwarding process if a packet arrives at R1 in Figure with the destination address 180.70.65.140.

DOWNLOADED FROM KTUASSIST.IN

Show the forwarding process if a packet arrives at R1 in Figure with the destination address 180.70.65.140.

Solution

The router performs the following steps:

1. *The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.*
2. *The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address and the interface number m0 are passed to ARP for further processing.*

DOWNLOADED FROM KTUASSIST.IN

Show the forwarding process if a packet arrives at R1 in Figure with the destination address 201.4.22.35.

Solution

The router performs the following steps:

1. *The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address.*
2. *The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).*

DOWNLOADED FROM KTUASSIST.IN

3. *The third mask (/24) is applied to the destination address. The result is 201.4.22.0, which matches the corresponding network address. The destination address of the packet and the interface number m3 are passed to ARP.*

DOWNLOADED FROM KTUASSIST.IN

Show the forwarding process if a packet arrives at R1 in Figure with the destination address 18.24.32.78.

DOWNLOADED FROM KTUASSIST.IN

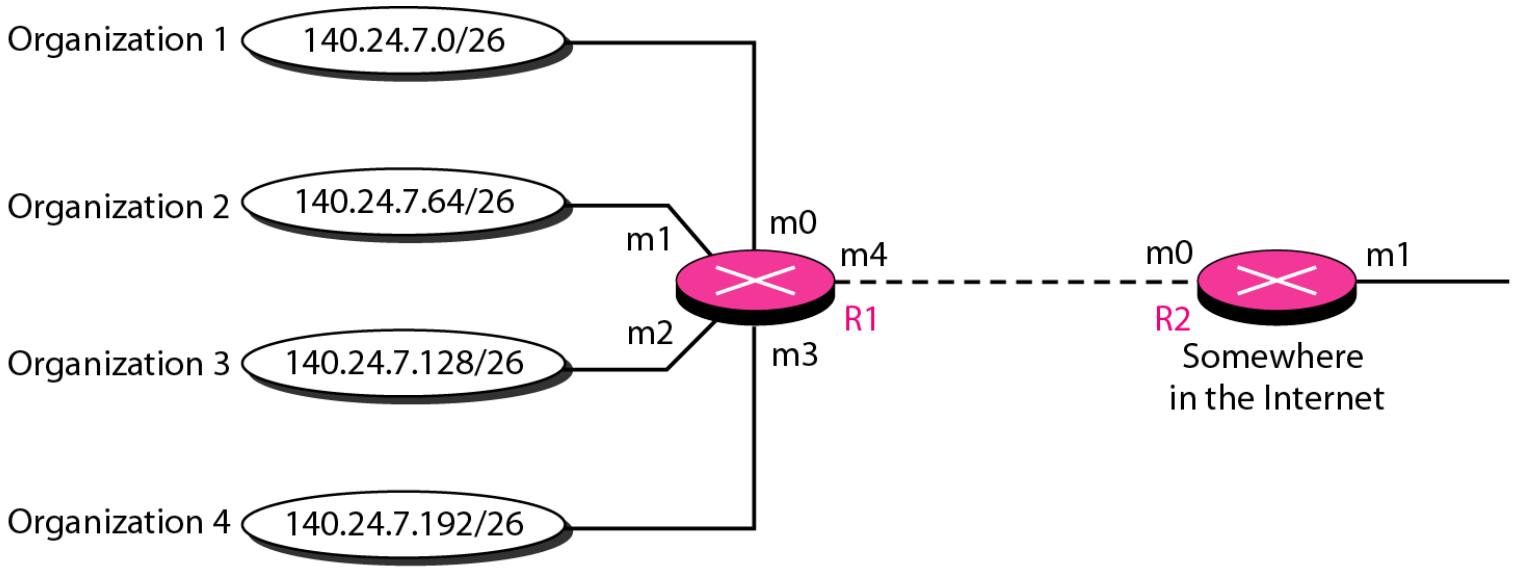
Show the forwarding process if a packet arrives at R1 in Figure with the destination address 18.24.32.78.

Solution

This time all masks are applied, one by one, to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to someplace else in the Internet.

DOWNLOADED FROM KTUASSIST.IN

Address Aggregation



Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

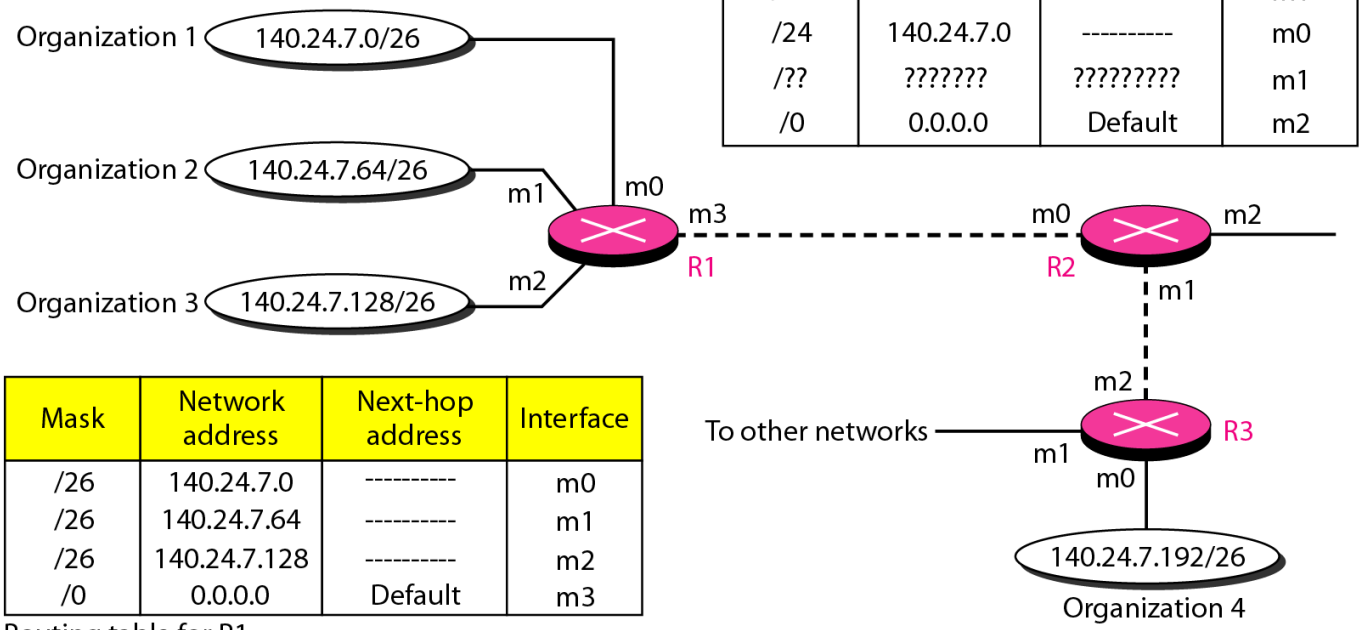
Routing table for R1

Mask	Network address	Next-hop address	Interface
/24	140.24.7.0	----------	m0
/0	0.0.0.0	Default	m1

Routing table for R2

DOWNLOADED FROM KTUASSIST.IN

Longest Mask Matching



Routing table for R2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m1
/24	140.24.7.0	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/0	0.0.0.0	Default	m3

Routing table for R1

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

Routing table for R3

DOWNLOADED FROM KTUASSIST.IN

As an example of hierarchical routing, let us consider Figure 22.9. A regional ISP is granted 16,384 addresses starting from 120.14.64.0. The regional ISP has decided to divide this block into four subblocks, each with 4096 addresses. Three of these subblocks are assigned to three local ISPs; the second subblock is reserved for future use. Note that the mask for each block is /20 because the original block with mask /18 is divided into 4 blocks.

The first local ISP has divided its assigned subblock into 8 smaller blocks and assigned each to a small ISP. Each small ISP provides services to 128 households, each using four addresses.

DOWNLOADED FROM KTUASSIST.IN

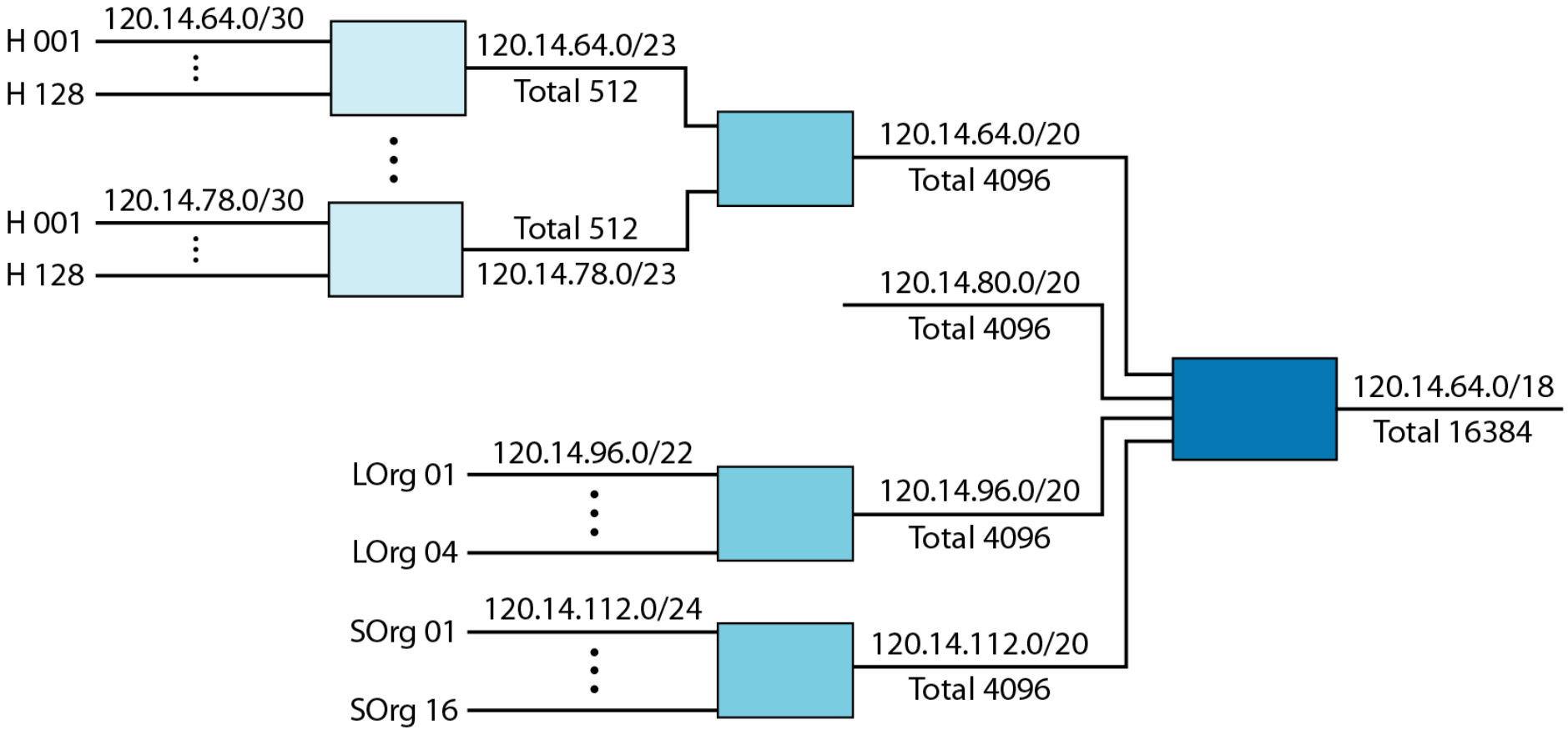
The second local ISP has divided its block into 4 blocks and has assigned the addresses to four large organizations.

The third local ISP has divided its block into 16 blocks and assigned each block to a small organization. Each small organization has 256 addresses, and the mask is /24.

There is a sense of hierarchy in this configuration. All routers in the Internet send a packet with destination address 120.14.64.0 to 120.14.127.255 to the regional ISP.

DOWNLOADED FROM KTUASSIST.IN

Hierarchical routing with ISPs



DOWNLOADED FROM KTUASSIST.IN

Common fields in a routing table

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
.....	.....	.....	.....	.....	.....	.....

DOWNLOADED FROM KTUASSIST.IN

Static and Dynamic Routing Tables

- A routing table can be either static or dynamic.
- A static table is one with manual entries.
- A dynamic table is one that is updated automatically when there is a change somewhere in the Internet.
- A routing protocol is a combination of rules and procedures that lets routers in the Internet inform each other of changes.

DOWNLOADED FROM KTUASSIST.IN

Comparison between Static and Dynamic Routing

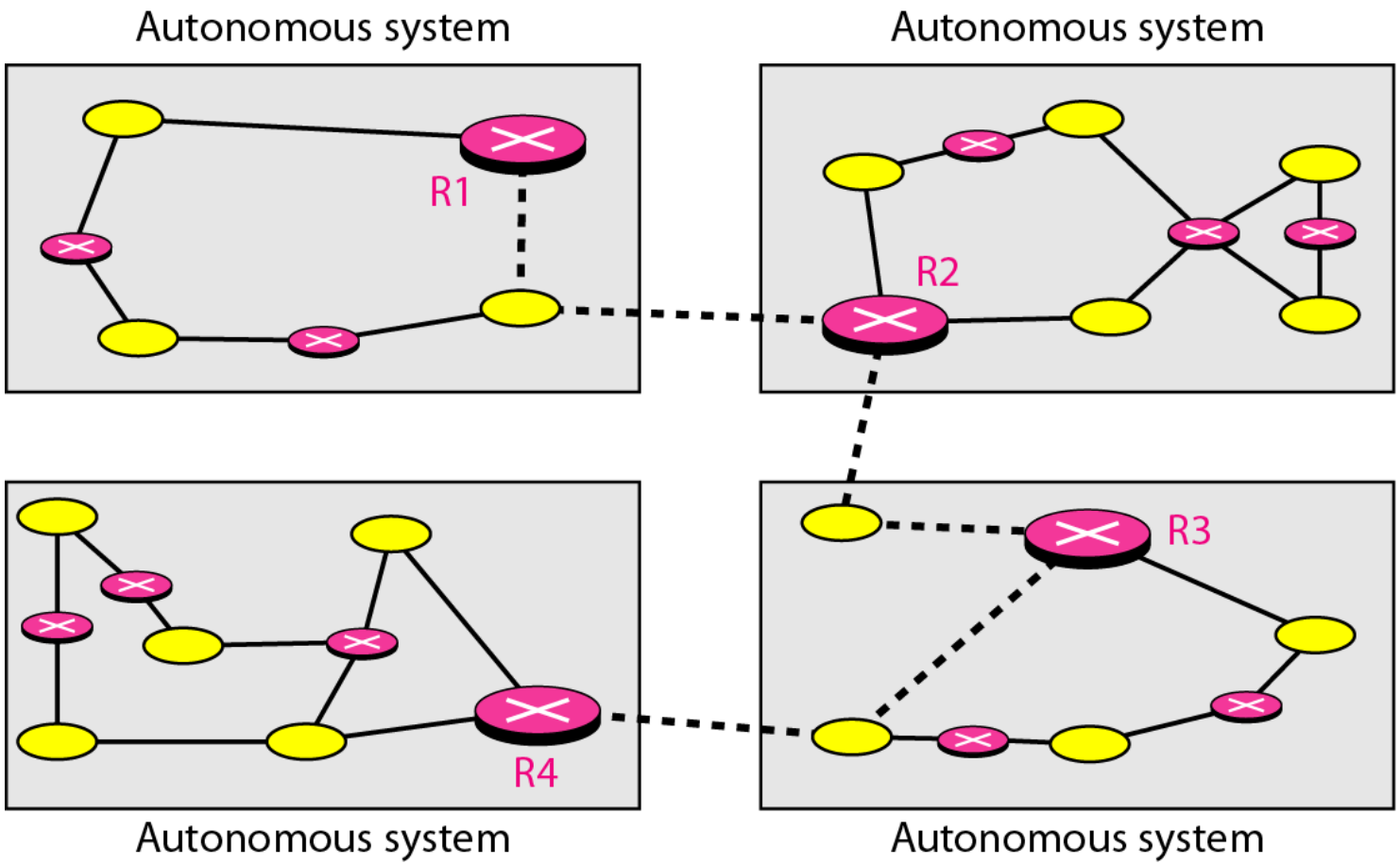
- Static Routing
  - Static routing is ideal for small networks
  - Configuring static routers involve less cost and can be easily maintained by the network administrator
  - Routers are not updated dynamically in the routing table and hence cannot detect inactive routes

Dynamic Routing

- Dynamic routing is suitable for large networks
- It involves cost in terms of CPU processes and bandwidth on the network links
- Routing protocols update the routing table with the updates routes

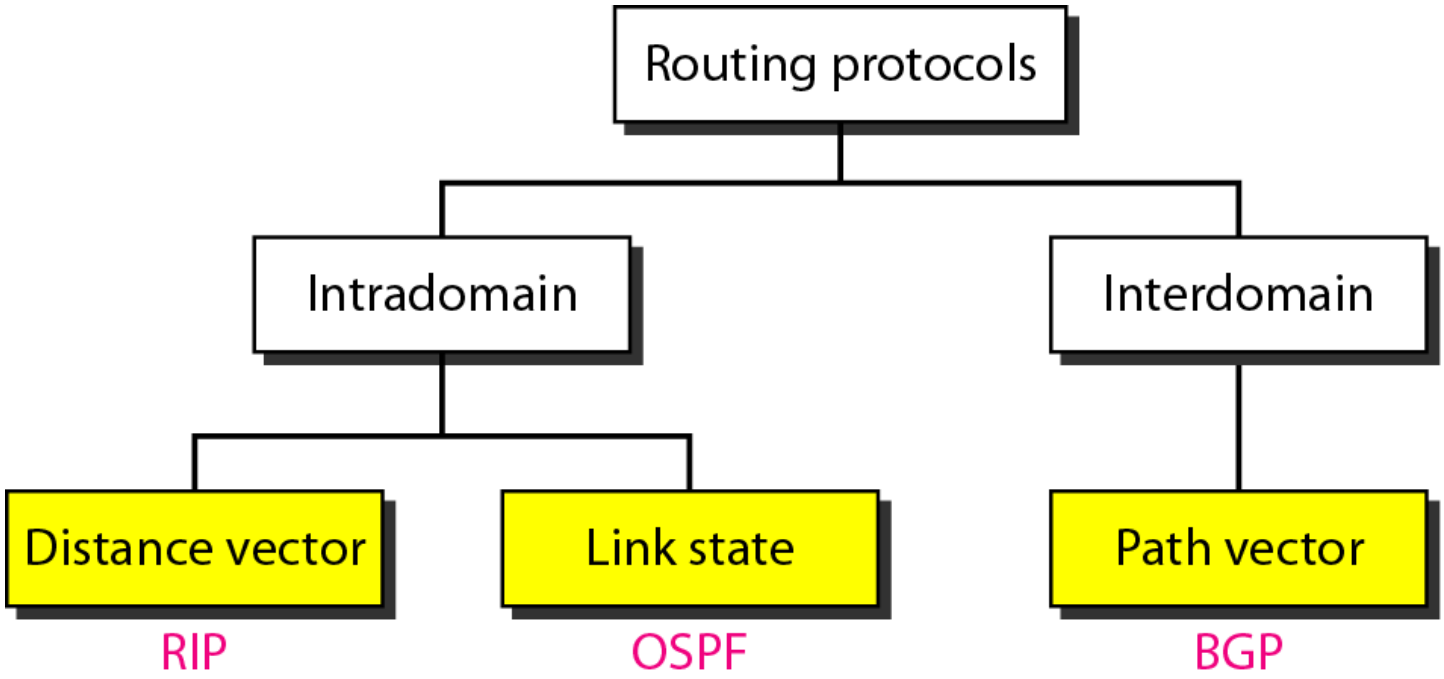
DOWNLOADED FROM KTUASSIST.IN

Autonomous Systems(AS)



DOWNLOADED FROM KTUASSIST.IN

Popular Routing Protocols



DOWNLOADED FROM KTUASSIST.IN

Distance Vector Routing

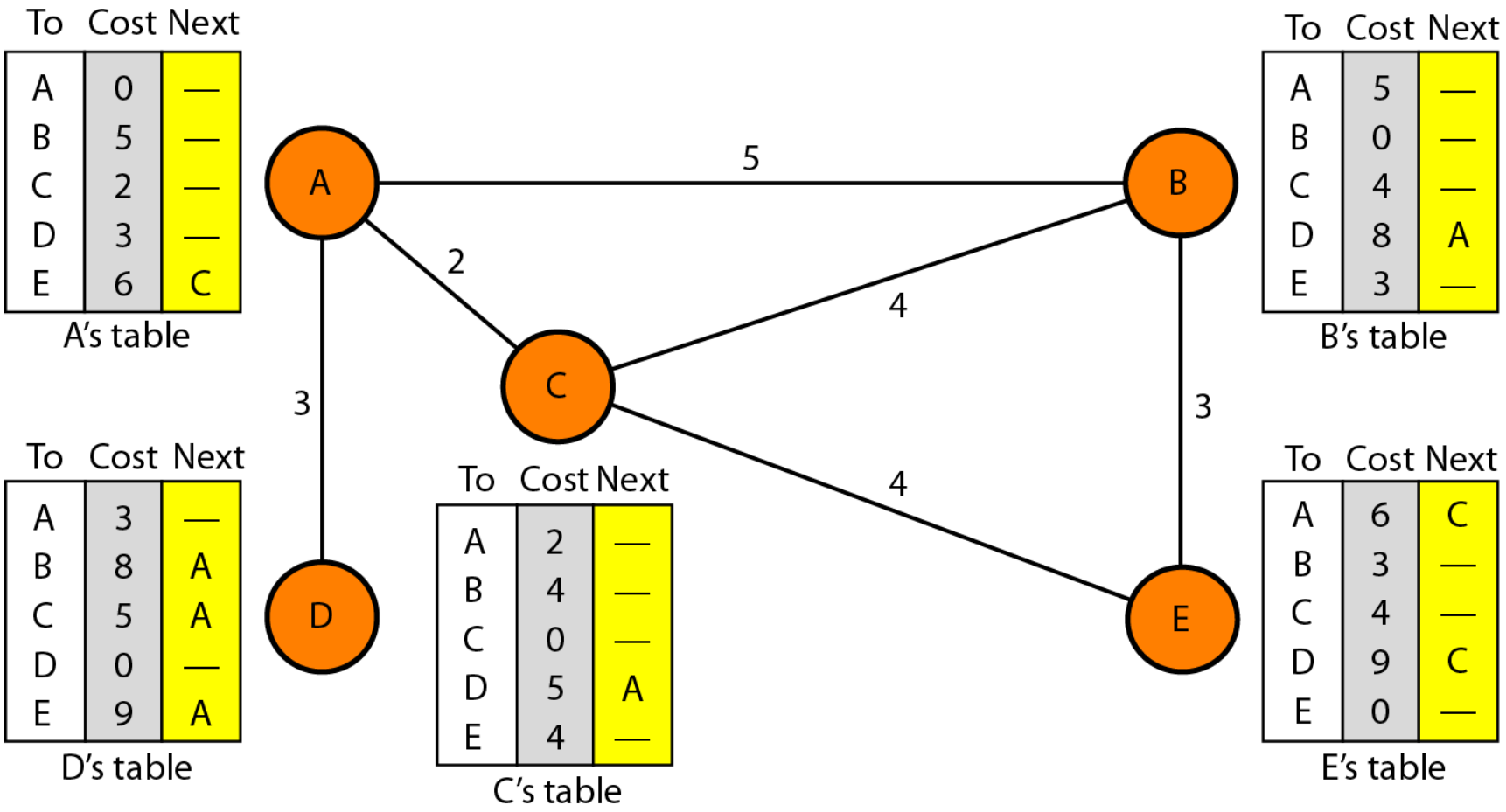
DOWNLOADED FROM KTUASSIST.IN

Distance Vector Routing

- In distance vector routing, the least cost route between any two nodes is the route with minimum distance
- In this protocol, each node maintains a table of minimum distance to every node.

DOWNLOADED FROM KTUASSIST.IN

Distance vector routing tables



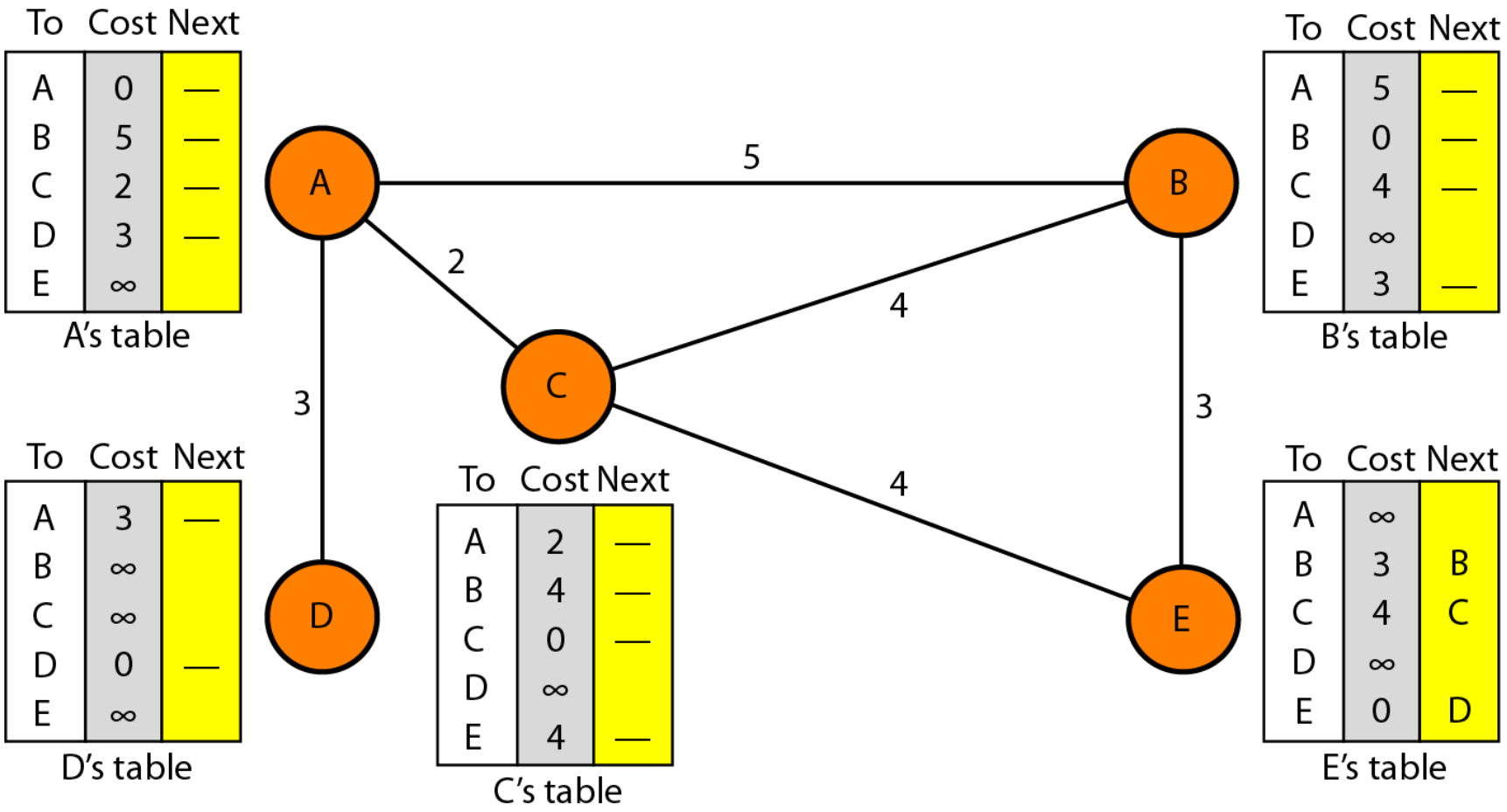
DOWNLOADED FROM KTUASSIST.IN

Distance Vector Routing

- Building Routing Table:
  - Initialization
  - Sharing
  - Updating

DOWNLOADED FROM KTUASSIST.IN

Initialization of tables in distance vector routing



DOWNLOADED FROM KTUASSIST.IN

Initialization

- At the beginning, each node can know only the distance between itself and its immediate neighbors, those directly connected to it.(Just assume that each node can send a message to its immediate neighbors and find the distance between itself and these neighbors)
- The distance for any entry that is not a neighbor is marked as infinity(unreachable)

DOWNLOADED FROM KTUASSIST.IN

Sharing

- The whole idea of distance vector routing is the sharing of information between neighbors.
- Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E.
- In other words, nodes A and C, can improve their routing tables if they help each other
- While sharing only the first two columns are shared.(ie, destination and cost fields only)

DOWNLOADED FROM KTUASSIST.IN

Note

In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

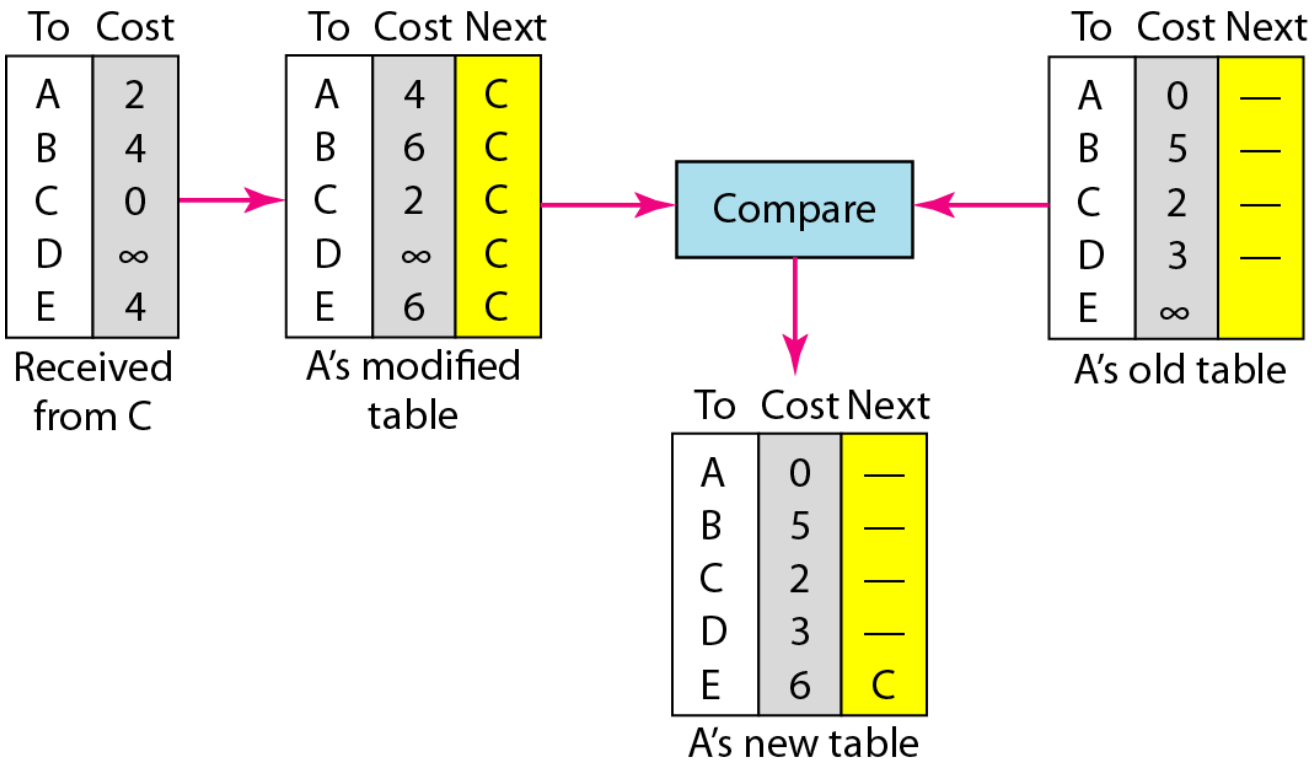
DOWNLOADED FROM KTUASSIST.IN

Updating

- When a node receives a two column table from a neighbor, it needs to update its routing table. Updating takes three steps:
  - The receiving node needs to add the cost between itself and the sending node to each value in the second column.
  - The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from that row
  - The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table
    - If the next node entry is different, the receiving node chooses the row with the smaller cost. If there is tie, the old one is kept
    - If the next node entry is same, the receiving node chooses the ne

DOWNLOADED FROM KTUASSIST.IN

Updating in distance vector routing



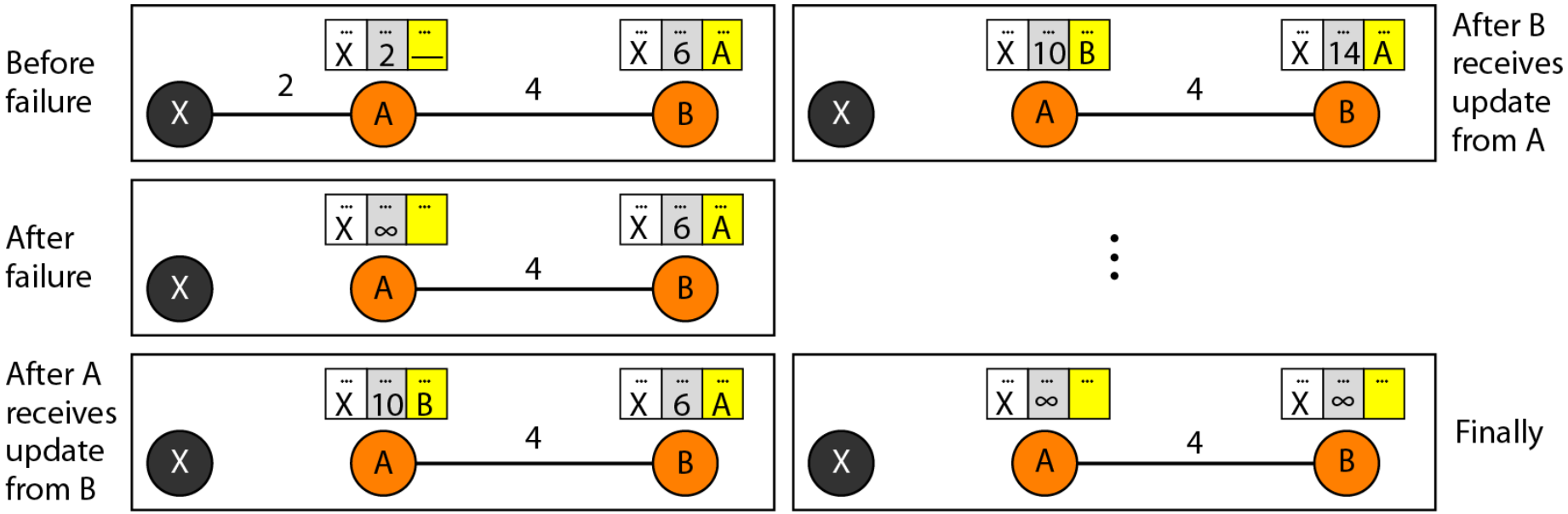
DOWNLOADED FROM KTUASSIST.IN

When to Share

- The table is sent both periodically and when there is a change in the table
  - Periodic Update: A node sends its routing table, normally every 30 seconds, in a periodic update
  - Triggered Update: A node sends its two column routing table to its neighbors any time there is a change in its routing table. This is called triggered update. The change can result from the following.
    - A node receives a table from a neighbor, resulting in changes in its own table after updating
    - A node detects some failure in the neighboring links which results in a distance change to infinity

DOWNLOADED FROM KTUASSIST.IN

Two-node instability: Count to infinity Problem



DOWNLOADED FROM KTUASSIST.IN

Solutions to Count to infinity

- Defining infinity: The first solution is to redefine infinity to a smaller number, such as 100.This will make the system stable in fewer updates. Most implementations of the distance vector protocol define 16 as infinity. However, this means that the distance vector routing cannot be used in large systems
- Split Horizon

DOWNLOADED FROM KTUASSIST.IN

RIP(Routing Information Protocol)

- It is an intradomain routing protocol used inside an autonomous system.
- It is a simple protocol based on distance vector routing

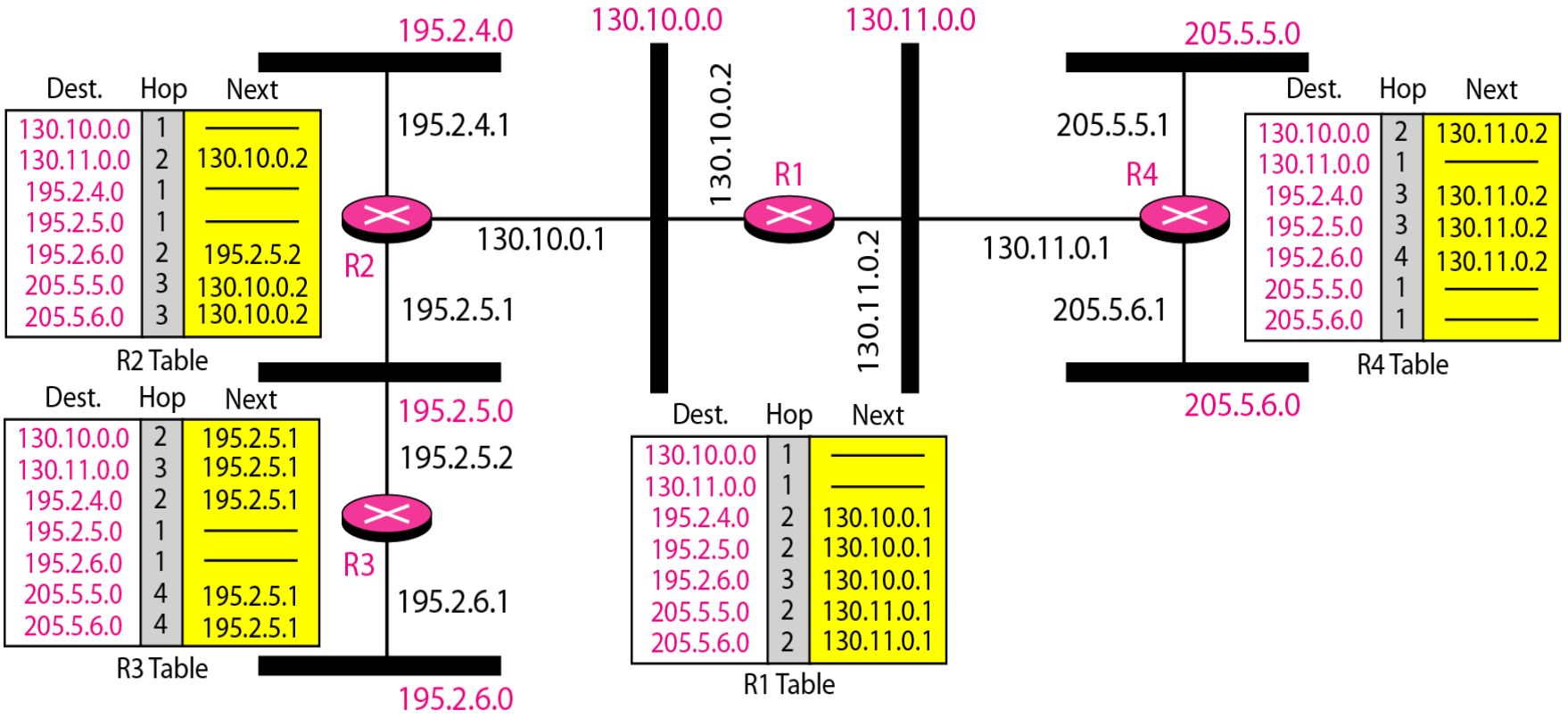
DOWNLOADED FROM KTUASSIST.IN

RIP(Routing Information Protocol)

- RIP implements distance vector routing with some considerations:
  - In an AS, there are routers and networks; routers have routing table while networks do not
  - The destination in a routing table is a network, which means the first column defines the network address
  - The metric used by RIP is very simple; the distance is defined as the number of links(networks) to reach the destination. For this reason, the metric in RIP is called a hop count
  - Infinity is defined as 16,which means that any route in an AS using RIP cannot have more than 15 hops
  - The next node column defines the address of the router to which the packet is to be sent to reach its destination

DOWNLOADED FROM KTUASSIST.IN

Example of a domain using RIP



DOWNLOADED FROM KTUASSIST.IN

Link State Routing

DOWNLOADED FROM KTUASSIST.IN

Link State Routing

- In link state routing, if each node in the domain has the entire topology of the domain, the node can use Dijkstra's algorithm to build a routing table

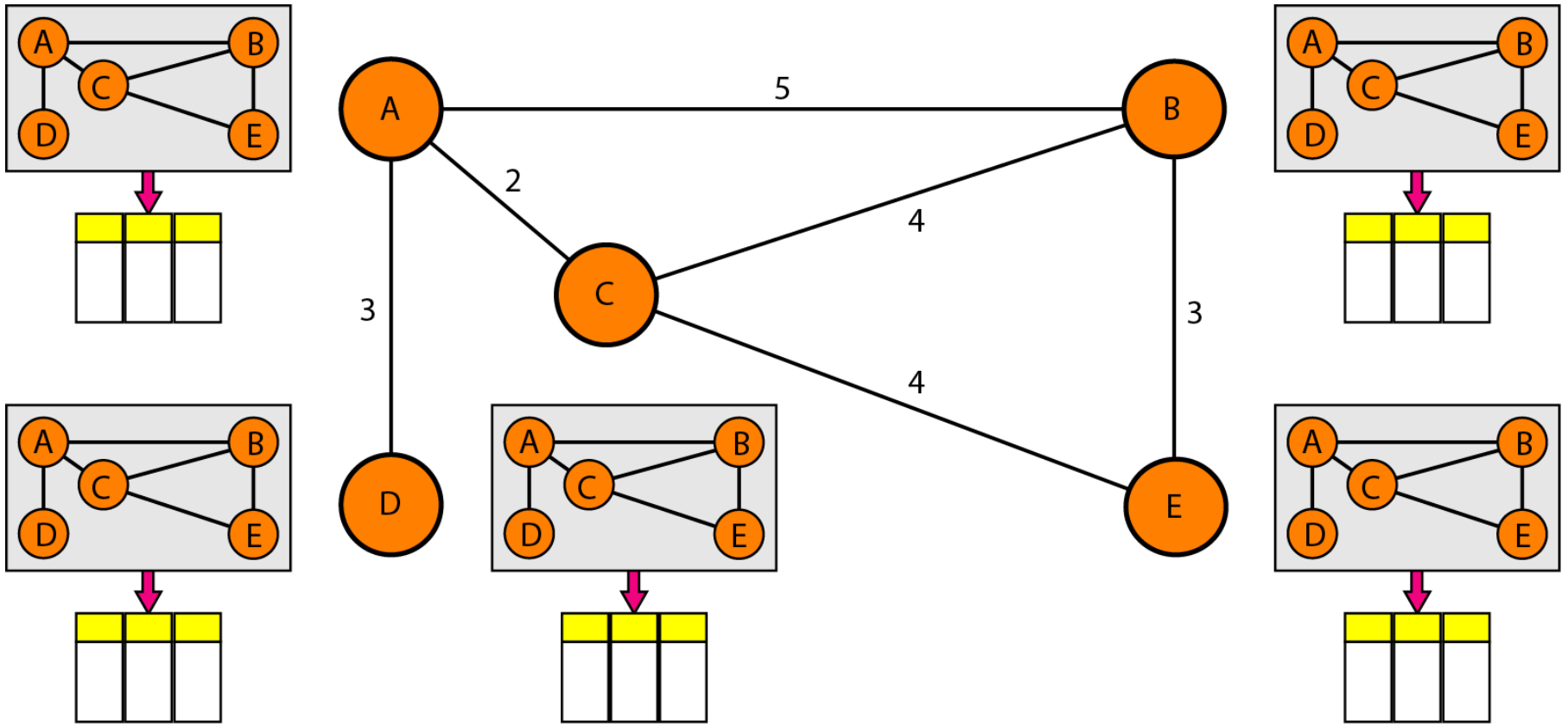
DOWNLOADED FROM KTUASSIST.IN

Link State Routing

- At the beginning although global knowledge about the topology is not clear, each node has partial knowledge;it knows the state(condition and cost) of its links
- Then the whole topology can be complied from the partial knowledge of each node.

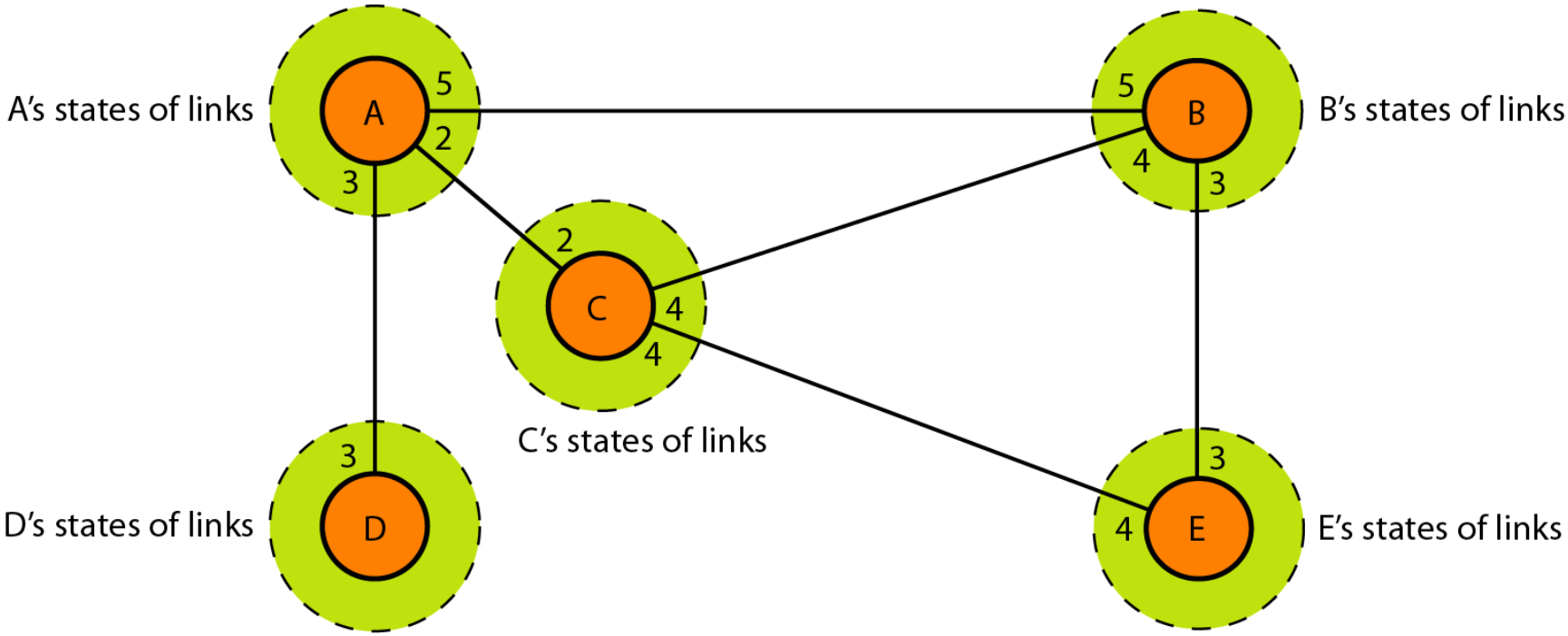
DOWNLOADED FROM KTUASSIST.IN

Concept of Link State Routing



DOWNLOADED FROM KTUASSIST.IN

Link state knowledge



DOWNLOADED FROM KTUASSIST.IN

Building Routing Tables

- In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least cost node to every other node
  - Creation of the states of the links by each node, called the link state packet(LSP)
  - Dissemination of LSPs to every other node(router),called flooding
  - Formation of a shortest path tree for each node
  - Calculation of a routing table based on the shortest path tree

DOWNLOADED FROM KTUASSIST.IN

Creation of LSPs

- A LSP carries the list of links, the node identity, a sequence number, and age
- Sequence number is used to identify new LSPs from old ones
- Age prevents old LSPs from remaining in the domain for long time.
- LSPs are generated on two occasions:
  - When there is a change in the topology of the domain
  - On a periodic basis

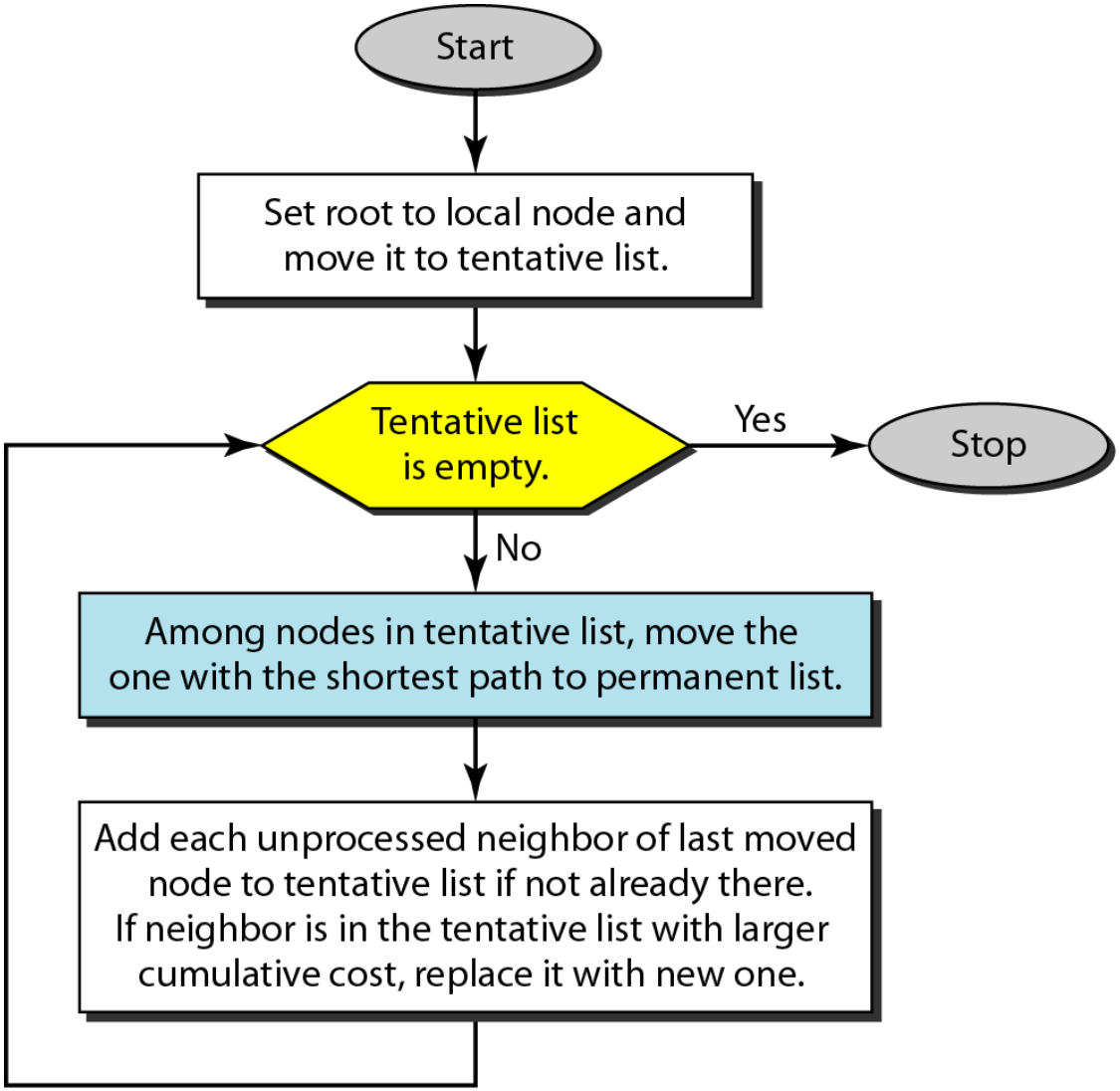
DOWNLOADED FROM KTUASSIST.IN

Flooding of LSPs

- The creating node sends a copy of the LSP out of each interface
- A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has, it discards the LSP. If it is newer, the node does the following:
  - It discards the old LSP and keeps the new one
  - It sends a copy of it out of each interface except the one from which the packet arrived.

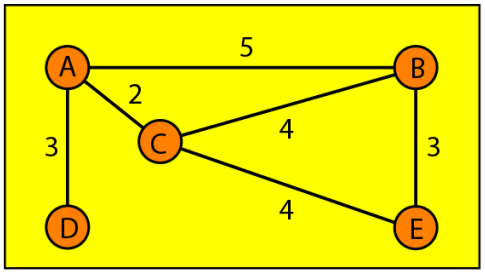
DOWNLOADED FROM KTUASSIST.IN

Dijkstra Algorithm

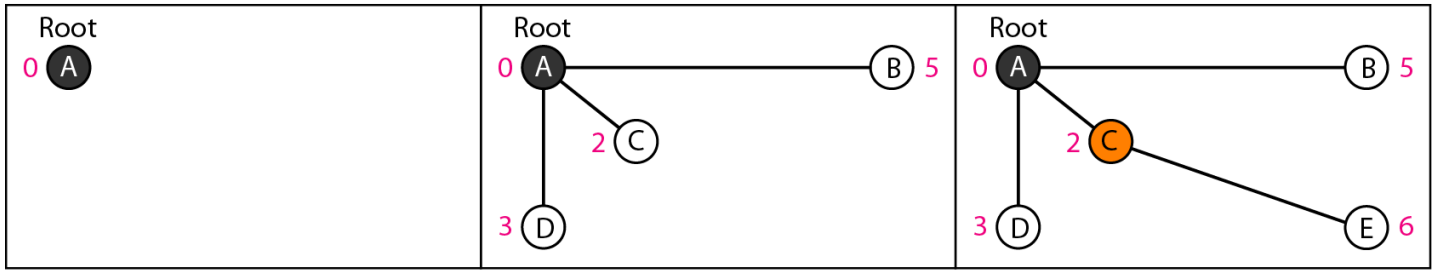


DOWNLOADED FROM KTUASSIST.IN

Example of formation of shortest path tree



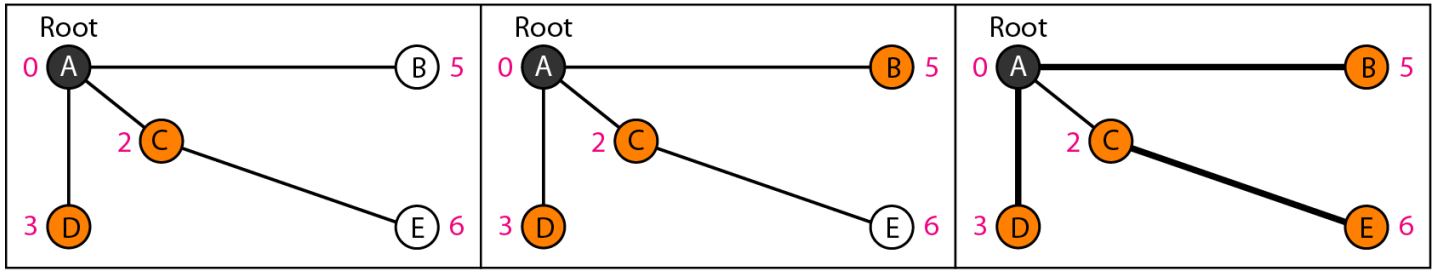
Topology



1. Set root to A and move A to tentative list.

2. Move A to permanent list and add B, C, and D to tentative list.

3. Move C to permanent and add E to tentative list.



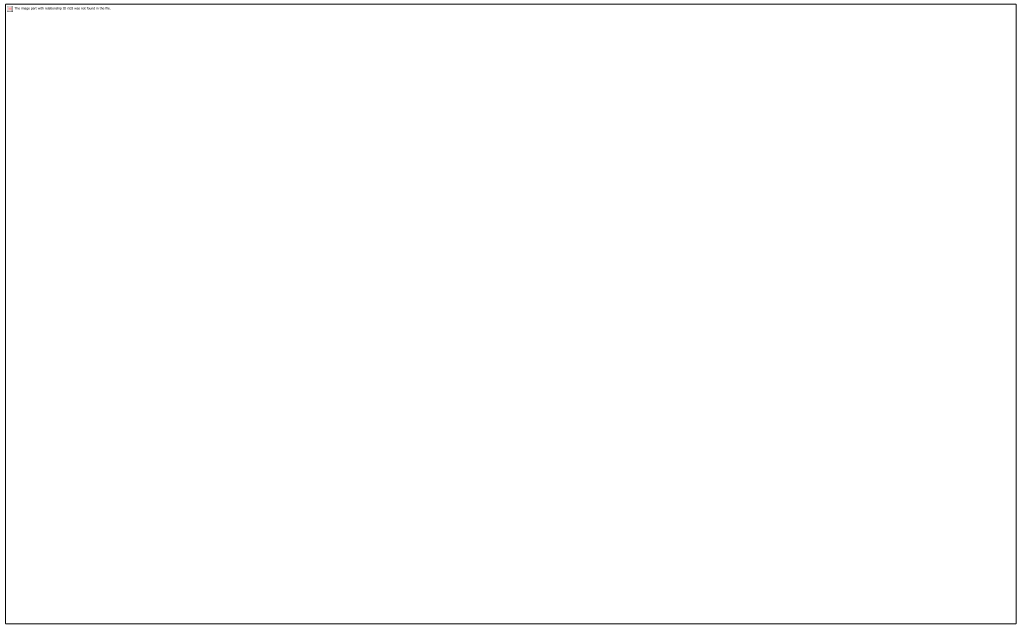
4. Move D to permanent list.

5. Move B to permanent list.

6. Move E to permanent list (tentative list is empty).

DOWNLOADED FROM KTUASSIST.IN

Routing table for node A



DOWNLOADED FROM KTUASSIST.IN

Open Shortest Path First (OSPF)

DOWNLOADED FROM KTUASSIST.IN

Open Shortest Path First

- It is an intradomain routing protocol and is based on link state routing

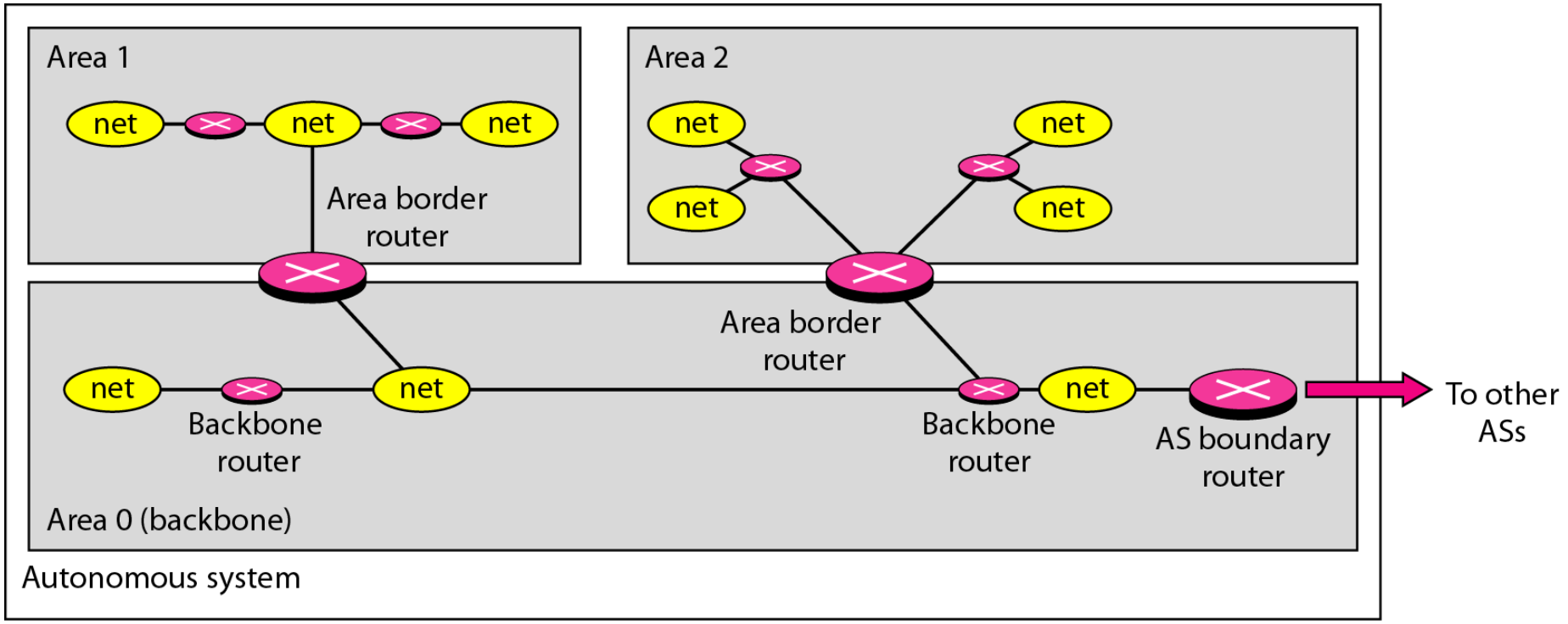
DOWNLOADED FROM KTUASSIST.IN

Open Shortest Path First

- OSPF Areas: OSPF divides an AS into Areas which is a collection of Network, Hosts and Routers.
  - Routers inside the area flood the area with routing information
  - At the border of an area, special routers called Area border routers summarize the information about the area and send it to other areas
  - All the areas must be connected to the ‘backbone’-a special area among the areas in an AS

DOWNLOADED FROM KTUASSIST.IN

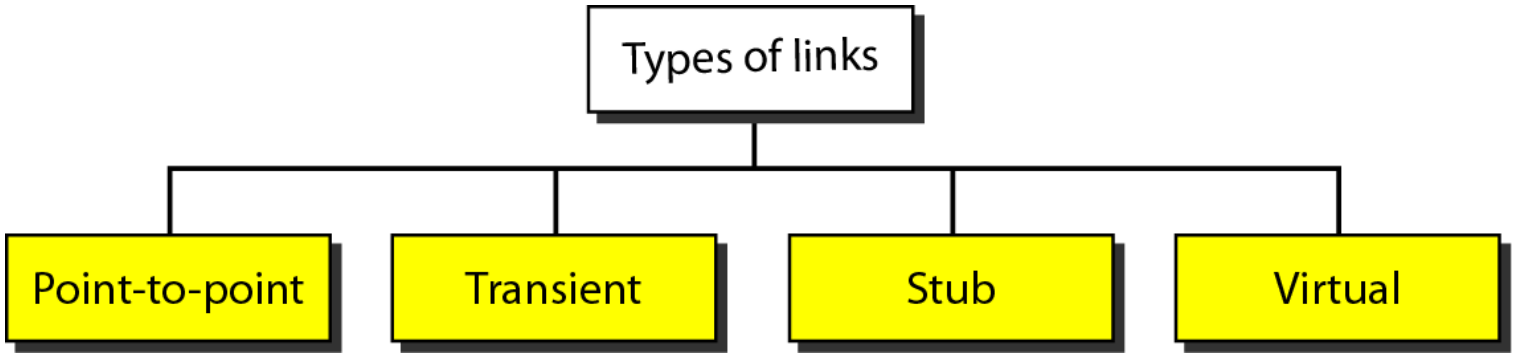
Areas in an Autonomous System



DOWNLOADED FROM KTUASSIST.IN

Types of Links

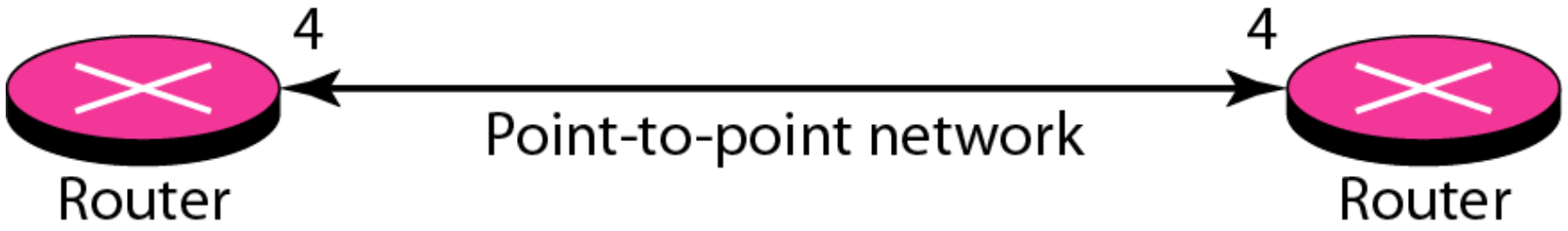
- A connection is called a link
- Connection between two routers is called a link



DOWNLOADED FROM KTUASSIST.IN

Point-to-Point link

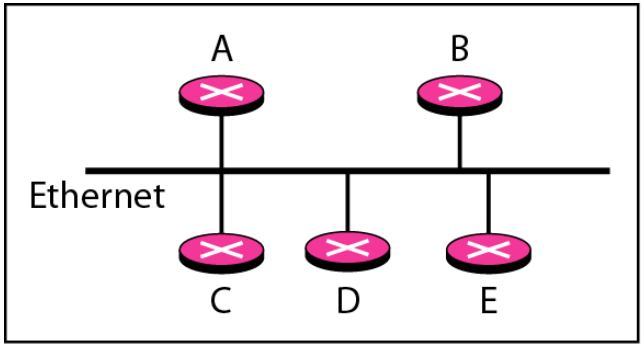
- Connects two routers without any other host or router in between



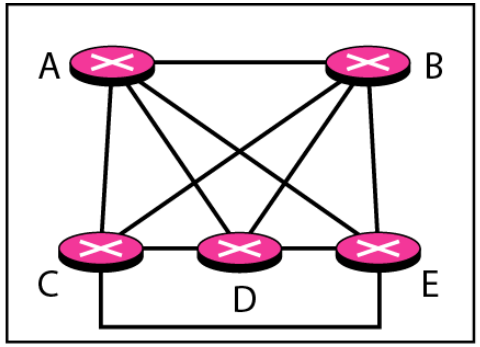
DOWNLOADED FROM KTUASSIST.IN

Transient Link

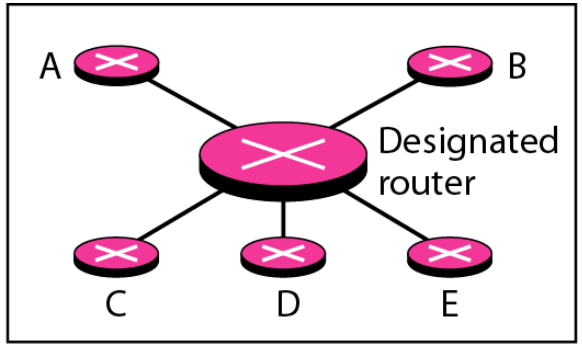
- It is a network with several routers attached to it.



a. Transient network



b. Unrealistic representation

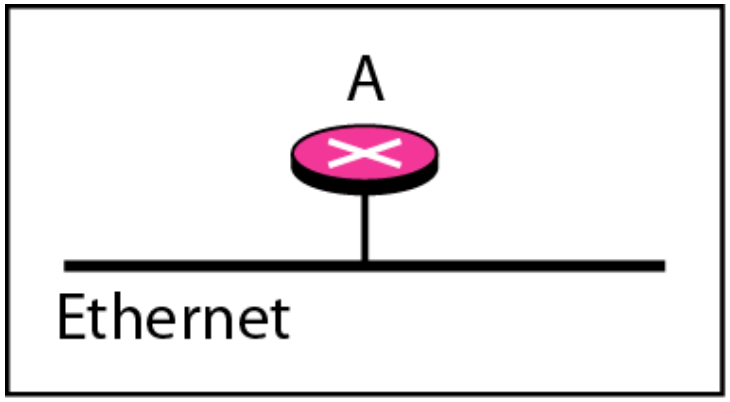


c. Realistic representation

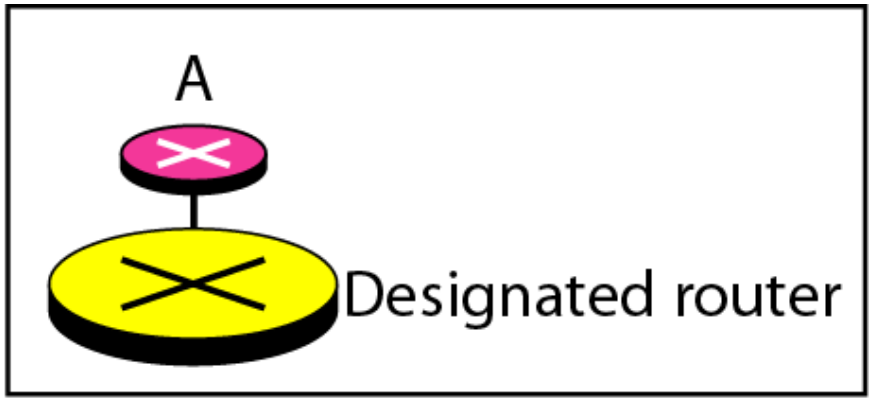
DOWNLOADED FROM KTUASSIST.IN

Stub Link

- It is a network that is connected to only one router
- Data packets enter network through the single router and leave the network through this same router



a. Stub network



b. Representation

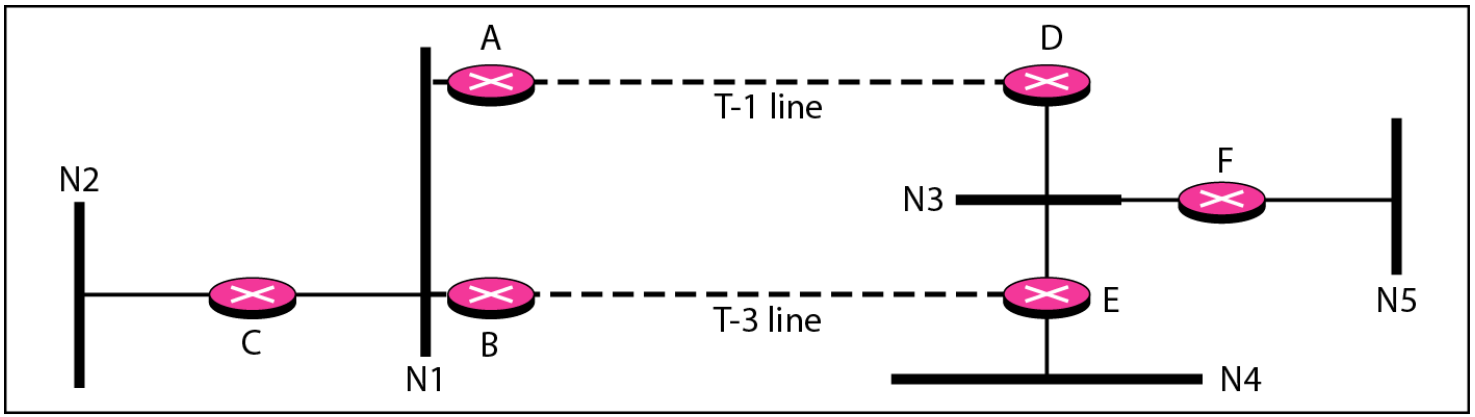
DOWNLOADED FROM KTUASSIST.IN

Virtual Link

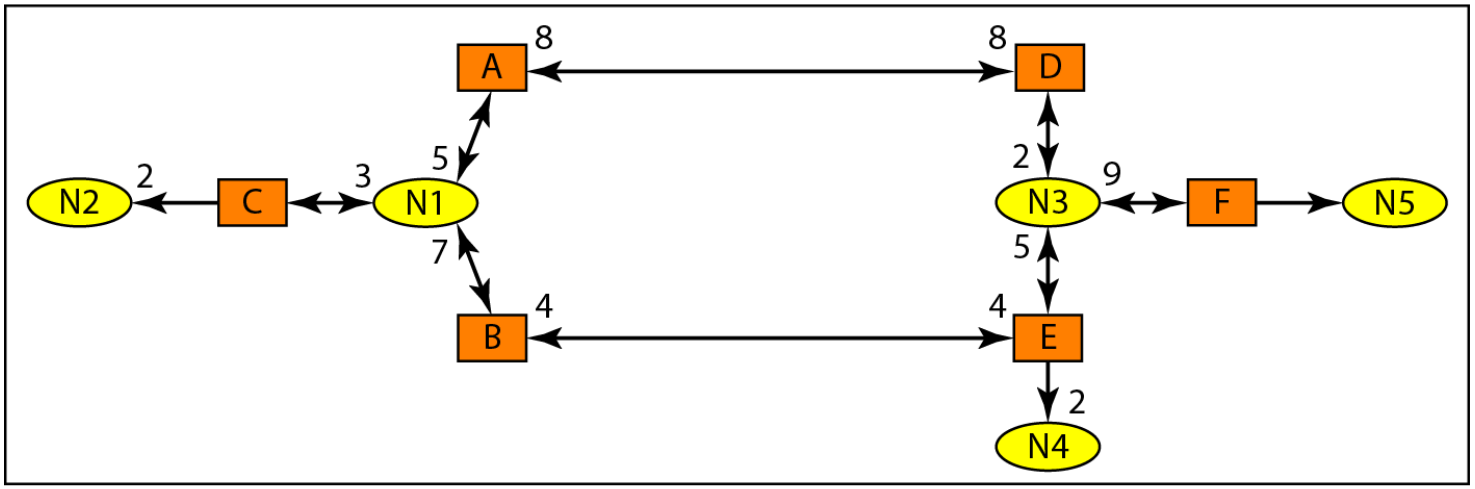
- When the link between two routers is broken, the administration may create a virtual link between them, using a longer path that probably goes through several routers

DOWNLOADED FROM KTUASSIST.IN

Example of an AS and its Graphical Representation in OSPF



a. Autonomous system



b. Graphical representation

DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing

DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing

- It is an interdomain routing protocol
- In this routing, a router has a list of Networks that can be reached with the path to reach each one
- As the name suggests, it tells us the path

DOWNLOADED FROM KTUASSIST.IN

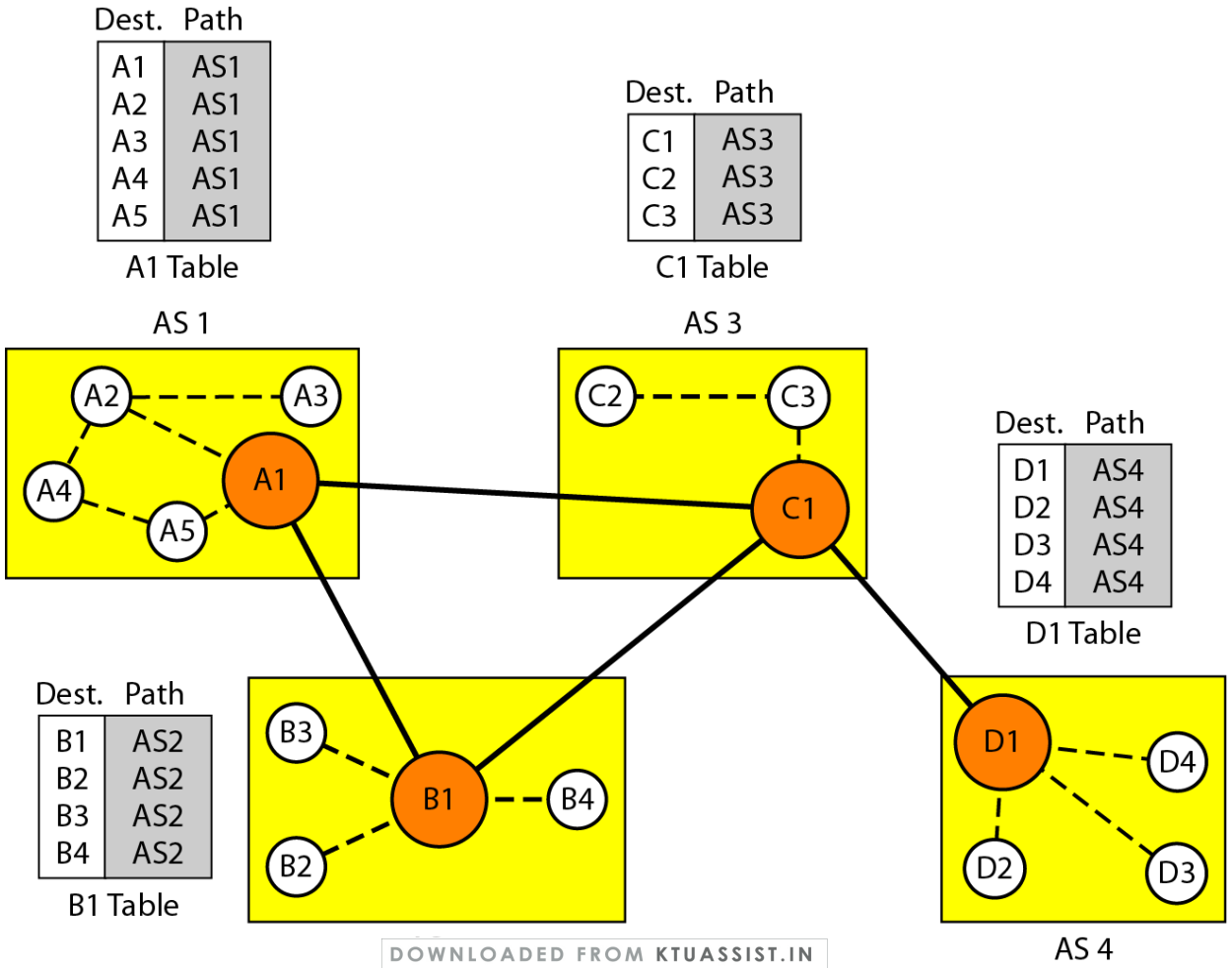
Path Vector Routing

- Speaker Node: In path vector routing, we assume that there is one node in each AS that acts on behalf of the entire AS.
- The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs.

DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing: Initialization

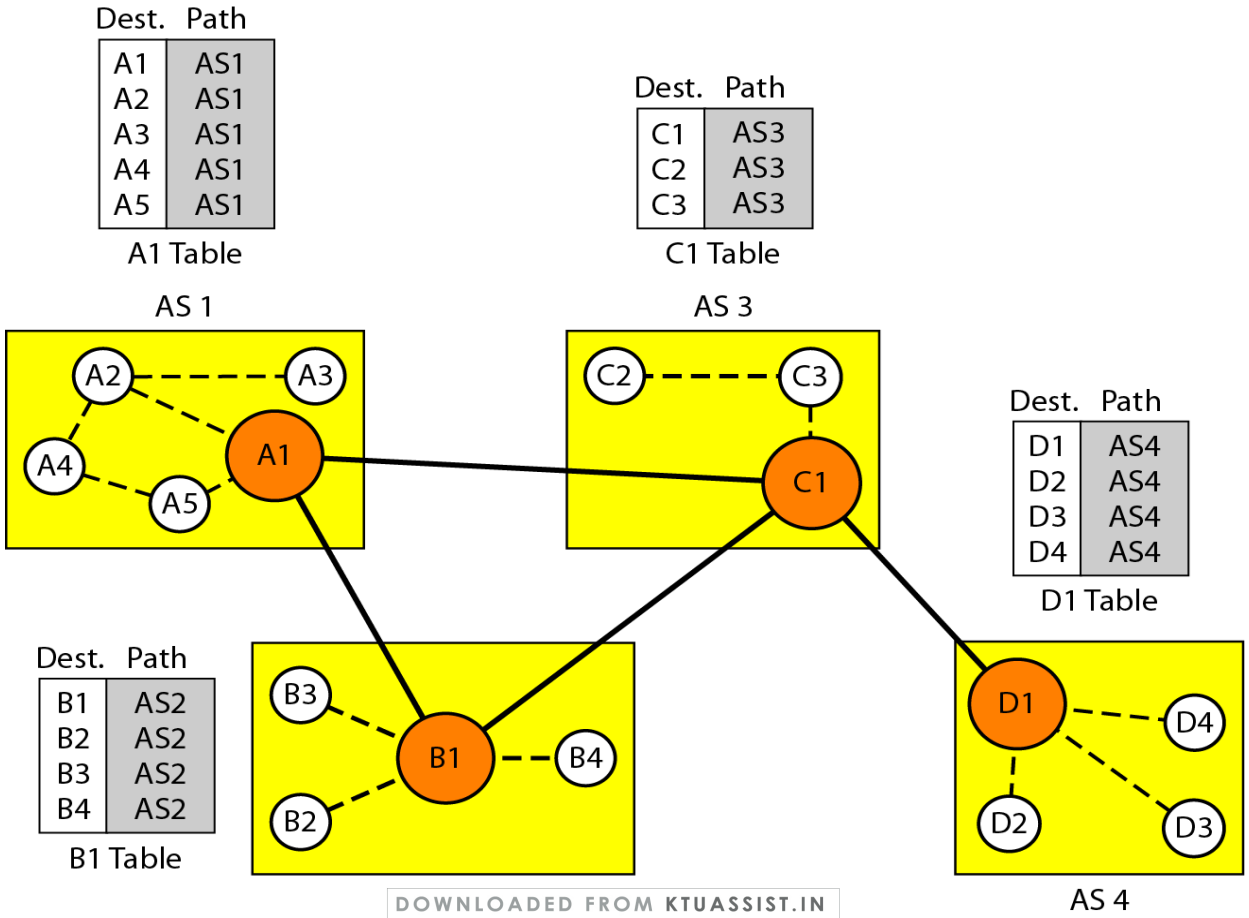
- At the beginning, each speaker node can know only the reachability of nodes inside its AS.



DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing: Sharing

- A speaker in an AS shares its tables with immediate neighbors. Here node A1 shares its table with nodes B1 and C1 and so on.



DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing: Updating

- When a speaker receives a two column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table.

Dest.	Path
A1 … A5	AS1
B1 … B4	AS1-AS2 … AS1-AS2
C1 … C3	AS1-AS3 … AS1-AS3
D1 … D4	AS1-AS2-AS4 … AS1-AS2-AS4

A1 Table

Dest.	Path
A1 … A5	AS2-AS1
B1 … B4	AS2 … AS2
C1 … C3	AS2-AS3 … AS2-AS3
D1 … D4	AS2-AS3-AS4 … AS2-AS3-AS4

B1 Table

Dest.	Path
A1 … A5	AS3-AS1
B1 … B4	AS3-AS2 … AS3-AS2
C1 … C3	AS3 … AS3
D1 … D4	AS3-AS4 … AS3-AS4

C1 Table

Dest.	Path
A1 … A5	AS4-AS3-AS1
B1 … B4	AS4-AS3-AS2 … AS4-AS3-AS2
C1 … C3	AS4-AS3 … AS4-AS3
D1 … D4	AS4 … AS4

D1 Table

DOWNLOADED FROM KTUASSIST.IN

Path Vector Routing: Updating

- When a speaker receives a two column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table.
- Loop Prevention: When a router receives a message, it checks to see if its AS is in the path list to the destination. If it is, looping is involved and the message is ignored
- Policy Routing: When a speaker receives a routing table from its neighbor, if one of the AS listed in the path is against its policy, it can ignore that path.
- Optimum Path: A path from AS4 to AS1 can be AS4-AS3-AS2-AS1 or it can be AS4-AS3-AS1.For the tables, we choose the one that had the smaller number of ASs, but this is not always the case. Other considerations, such as security, safety and reliability can also be applied

DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- BGP is an interdomain protocol using path vector routing

DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- Types of Autonomous Systems:
  - Stub AS
  - Multihomed AS
  - Transit AS

DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- Types of Autonomous Systems:
  - Stub AS: A stub AS has only one connection to another AS. The host in the AS can send data traffic to other ASs. Data traffic cannot pass through a stub AS.A stub AS is either a source or sink.
  - Multihomed AS
  - Transit AS

DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- Types of Autonomous Systems:
  - Stub AS
  - Multihomed AS: A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic.
  - Transit AS

DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- Types of Autonomous Systems:
  - Stub AS
  - Multihomed AS
  - Transit AS:A transit AS is a multihomed AS that also allows transient traffic.

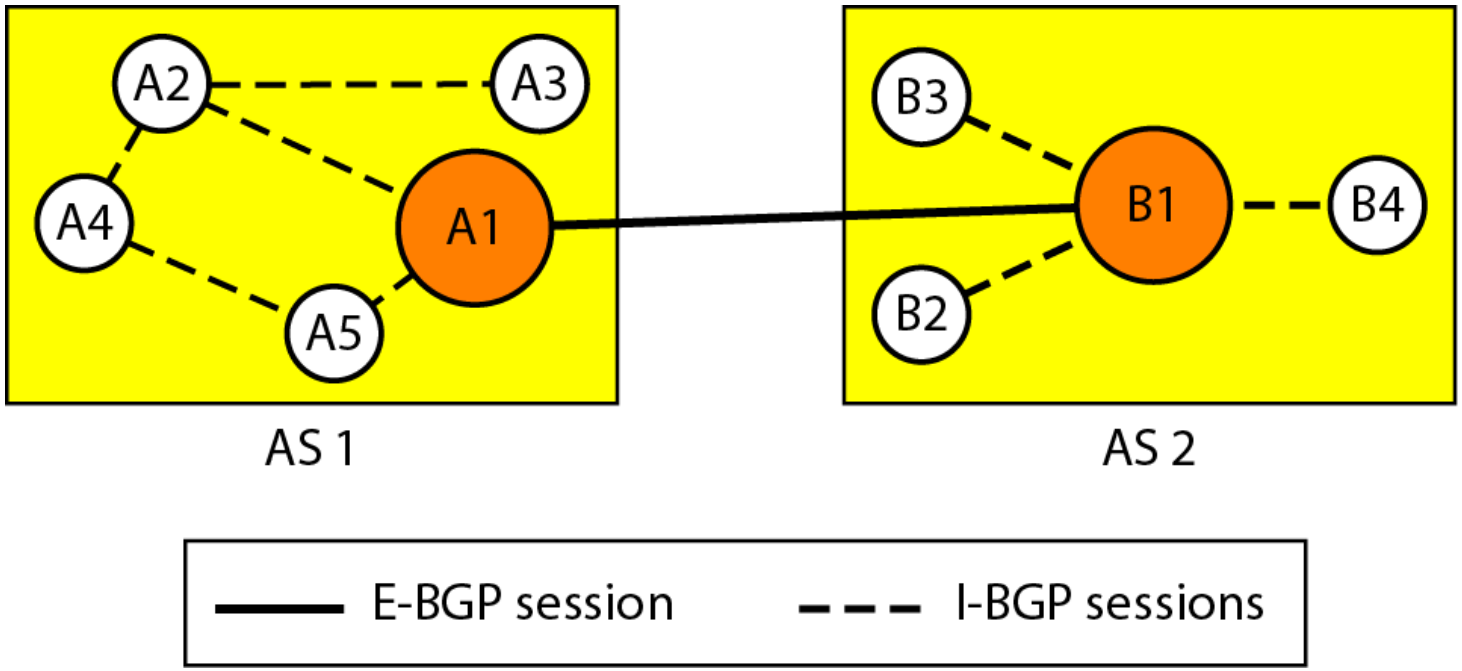
DOWNLOADED FROM KTUASSIST.IN

Border Gateway Protocol(BGP)

- Path Attributes:
  - Divided into two broad categories: Well-known attribute and optional attribute
  - Well-known attribute: is the one that every BGP router must recognize
  - Optional Attribute: is the one that needs not be recognized by every router.

DOWNLOADED FROM KTUASSIST.IN

BGP Sessions: Internal and External



DOWNLOADED FROM KTUASSIST.IN

Module 5

Transport Layer –UDP, TCP

Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics

Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP

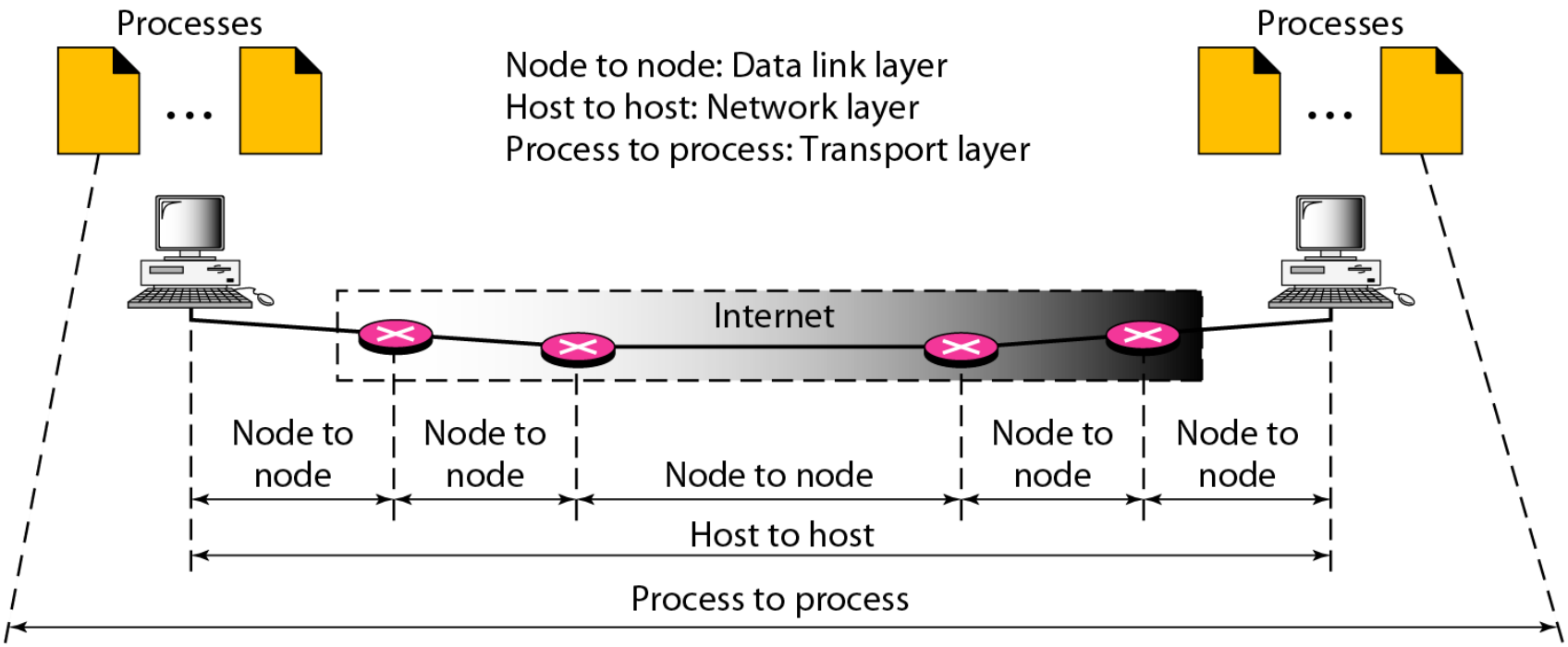
DOWNLOADED FROM KTUASSIST.IN

Transport Layer: Process to Process Delivery

- The transport layer is responsible for process-to-process delivery—the delivery of a packet, part of a message, from one process to another.
- Two processes communicate in a client/server relationship
- A process on the local host, called a client, needs services from a process usually on the remote host, called a server

DOWNLOADED FROM KTUASSIST.IN

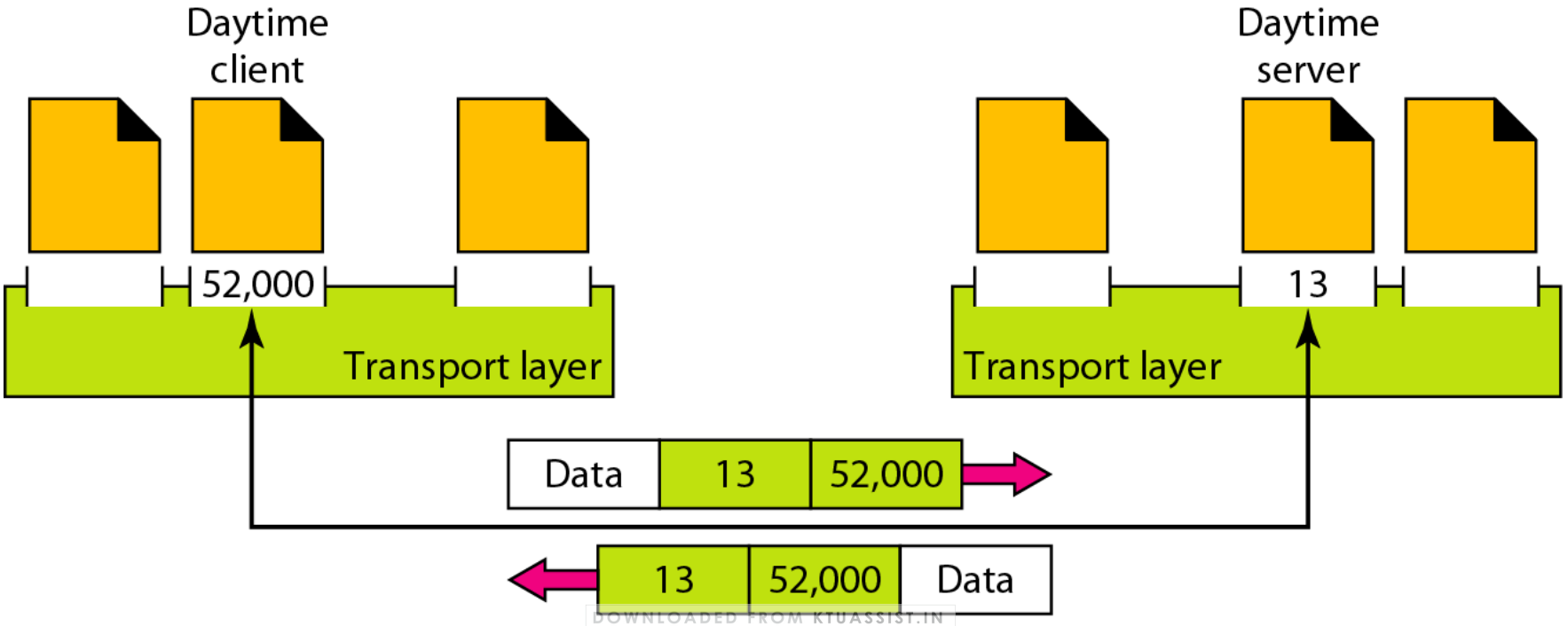
Types of Data Deliveries



DOWNLOADED FROM KTUASSIST.IN

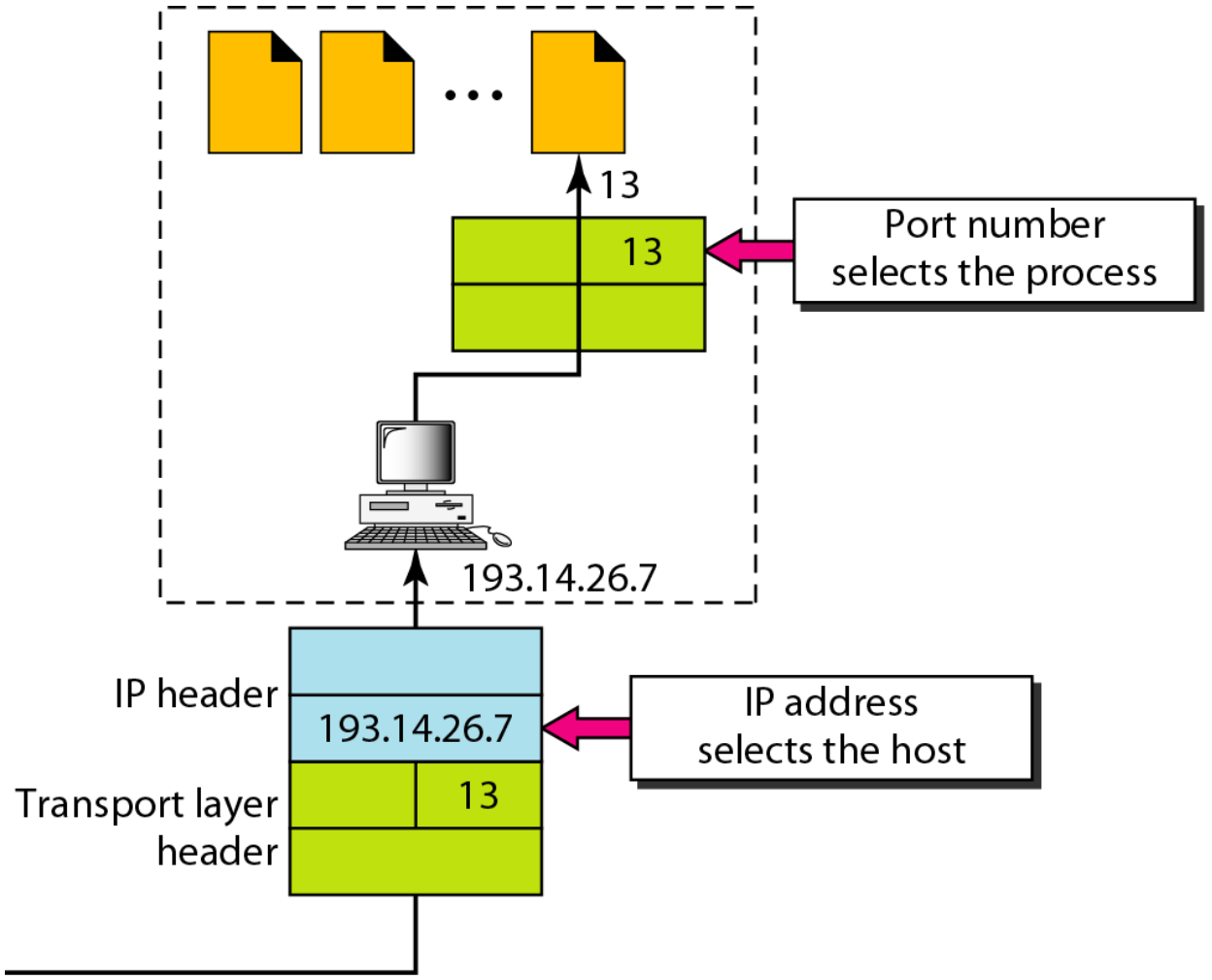
Port Numbers

- In the internet model, port numbers are 16bit integers between 0 to 65,535
- Client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number
- The internet has decided to use universal port numbers for servers; they are called well-known port numbers



DOWNLOADED FROM KTUASSIST.IN

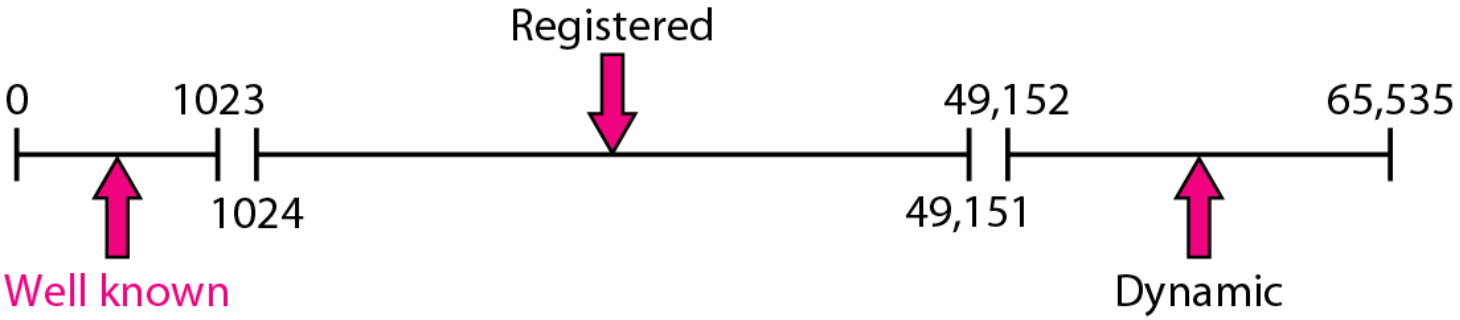
IP Addresses versus Port Numbers



DOWNLOADED FROM KTUASSIST.IN

IANA(Internet Assigned Number Authority) Ranges

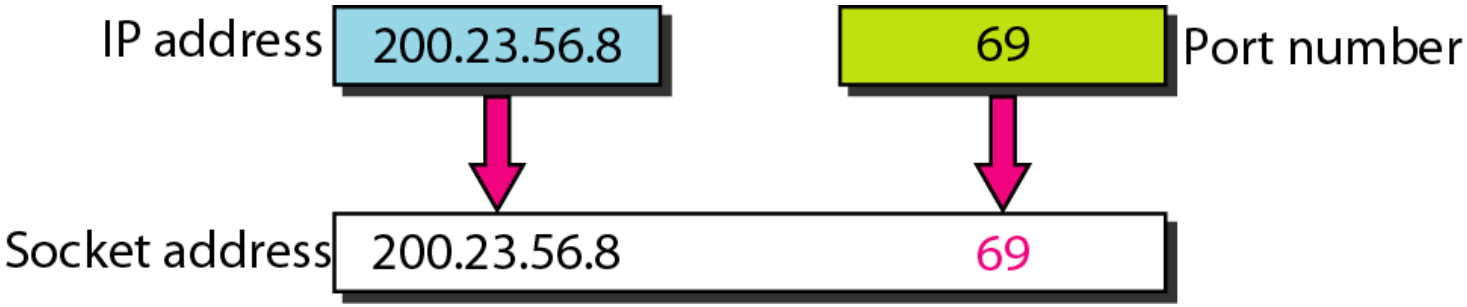
- The IANA has divided the port numbers into three ranges
  - Well Known ports: Port numbers from 0 to 1023
  - Registered Ports: Port numbers form 1024 to 49,151
  - Dynamic Ports : Port numbers form 49,152 to 65,535



DOWNLOADED FROM KTUASSIST.IN

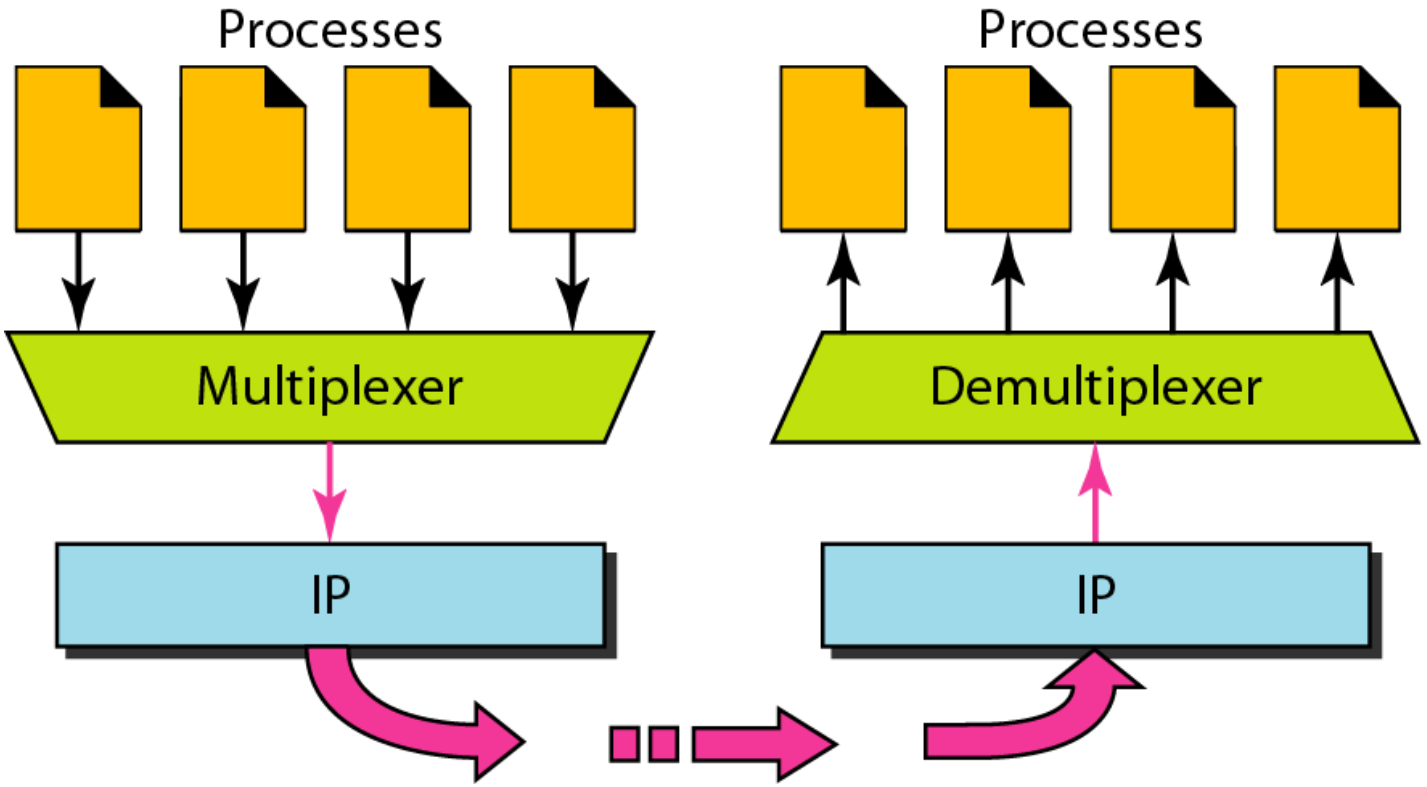
Socket address

- The combination of an IP address and a port number is called a socket address



DOWNLOADED FROM KTUASSIST.IN

Multiplexing and Demultiplexing



DOWNLOADED FROM KTUASSIST.IN

Connectionless Versus Connection-Oriented Service

- A transport layer protocol can either be connectionless or connection-oriented
  - Connectionless Service
    - In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release
    - One of the Protocols in the transport layer UDP is connectionless
  - Connection-Oriented Service
    - In a connection-oriented service, a connection is first established between the sender and the receiver.
    - Data are transferred
    - At the end, the connection is released.
    - One of the Protocols in the transport layer TCPP is connection-oriented

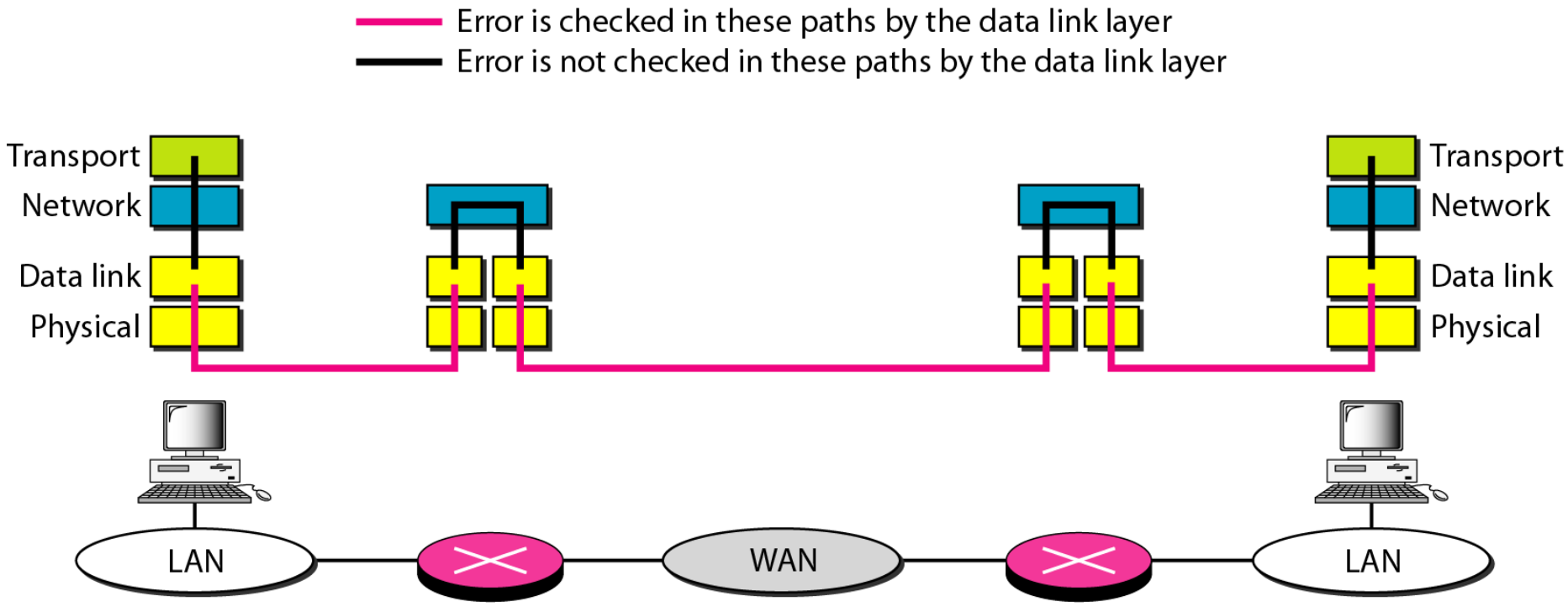
DOWNLOADED FROM KTUASSIST.IN

Reliable versus Unreliable

- The transport layer service can be reliable or unreliable
- If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer
- This means a slower and more complex service
- On the other hand, if the application program does not need reliability, then an unreliable protocol can be used
- UDP is connectionless and unreliable
- TCP is connection-oriented and reliable

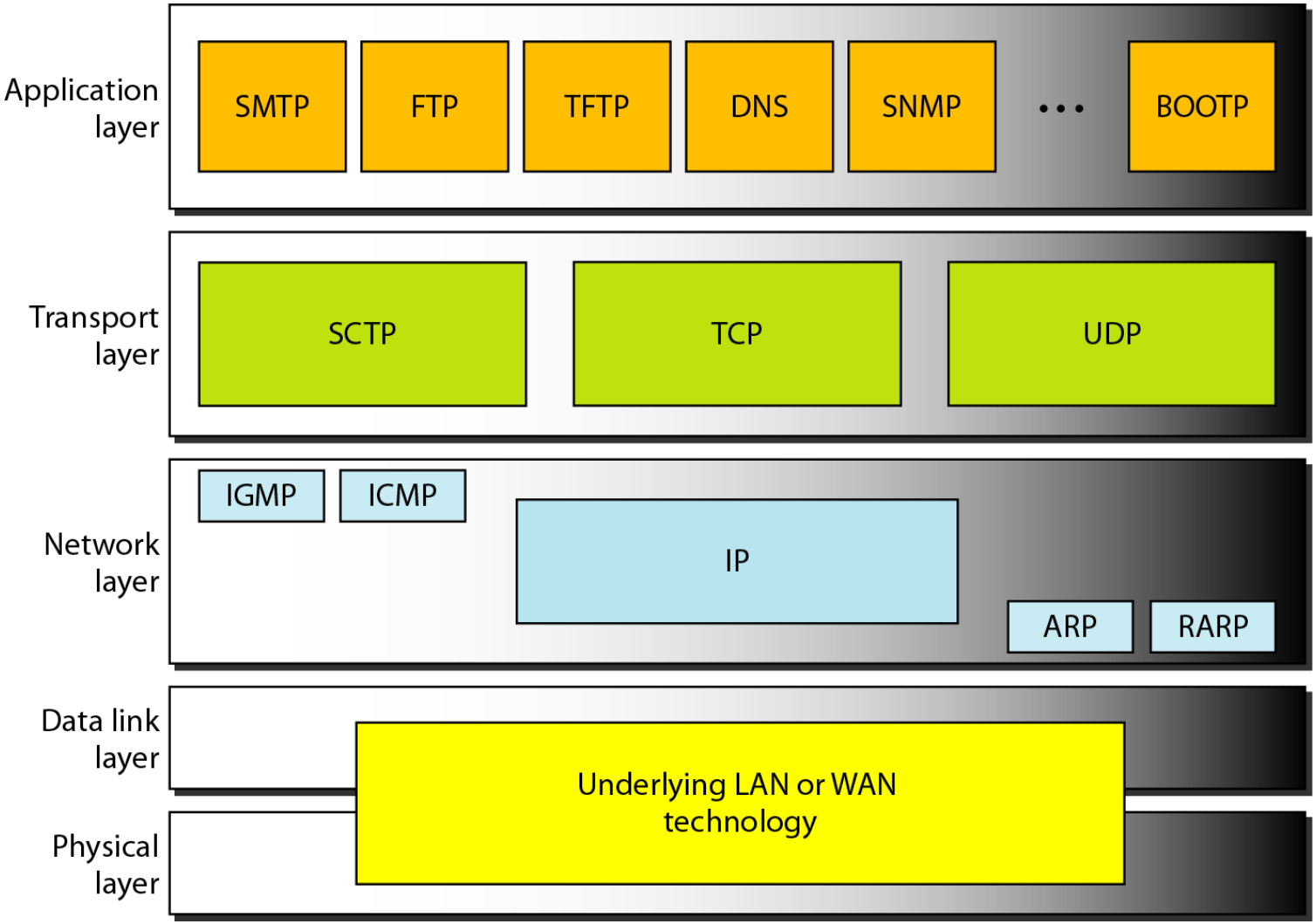
DOWNLOADED FROM KTUASSIST.IN

Error control



DOWNLOADED FROM KTUASSIST.IN

Position of UDP, TCP, and SCTP in TCP/IP suite



DOWNLOADED FROM KTUASSIST.IN

USER DATAGRAM PROTOCOL (UDP)

- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol.
- It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.

DOWNLOADED FROM KTUASSIST.IN

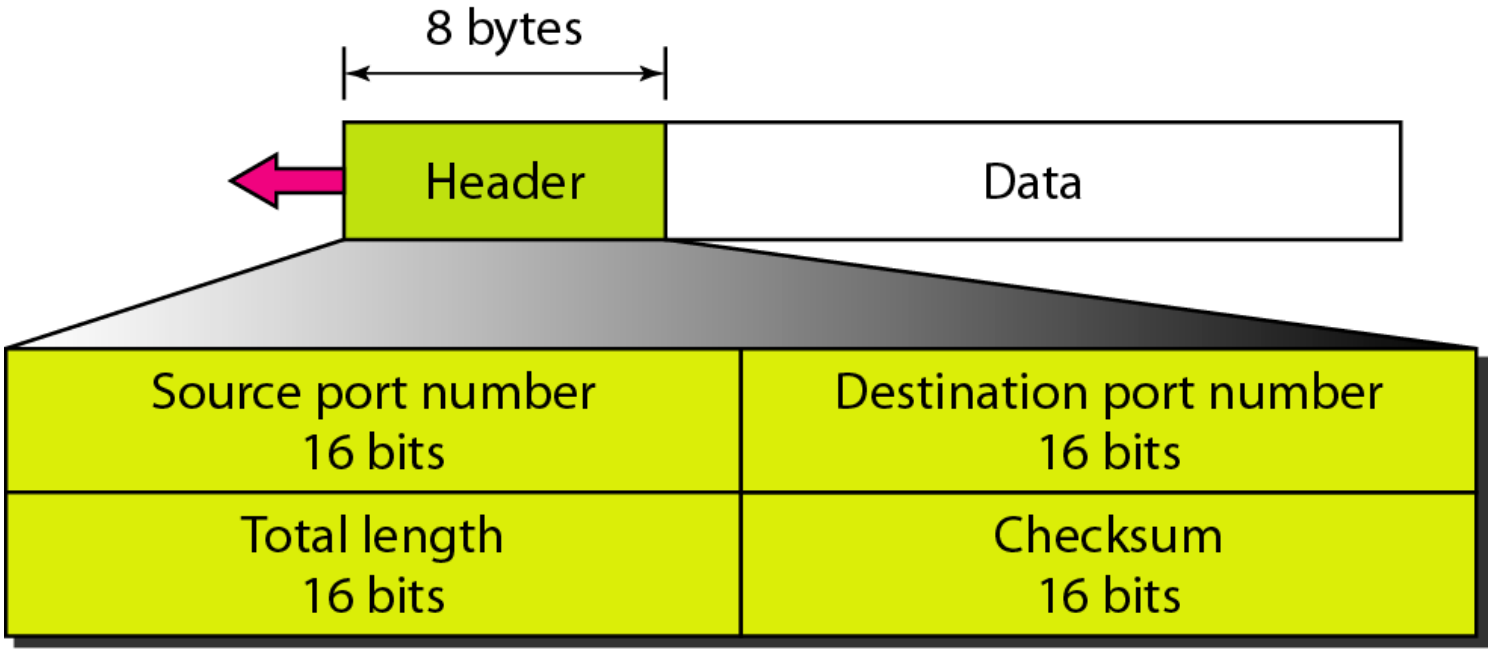
Well-known ports used with UDP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

DOWNLOADED FROM KTUASSIST.IN

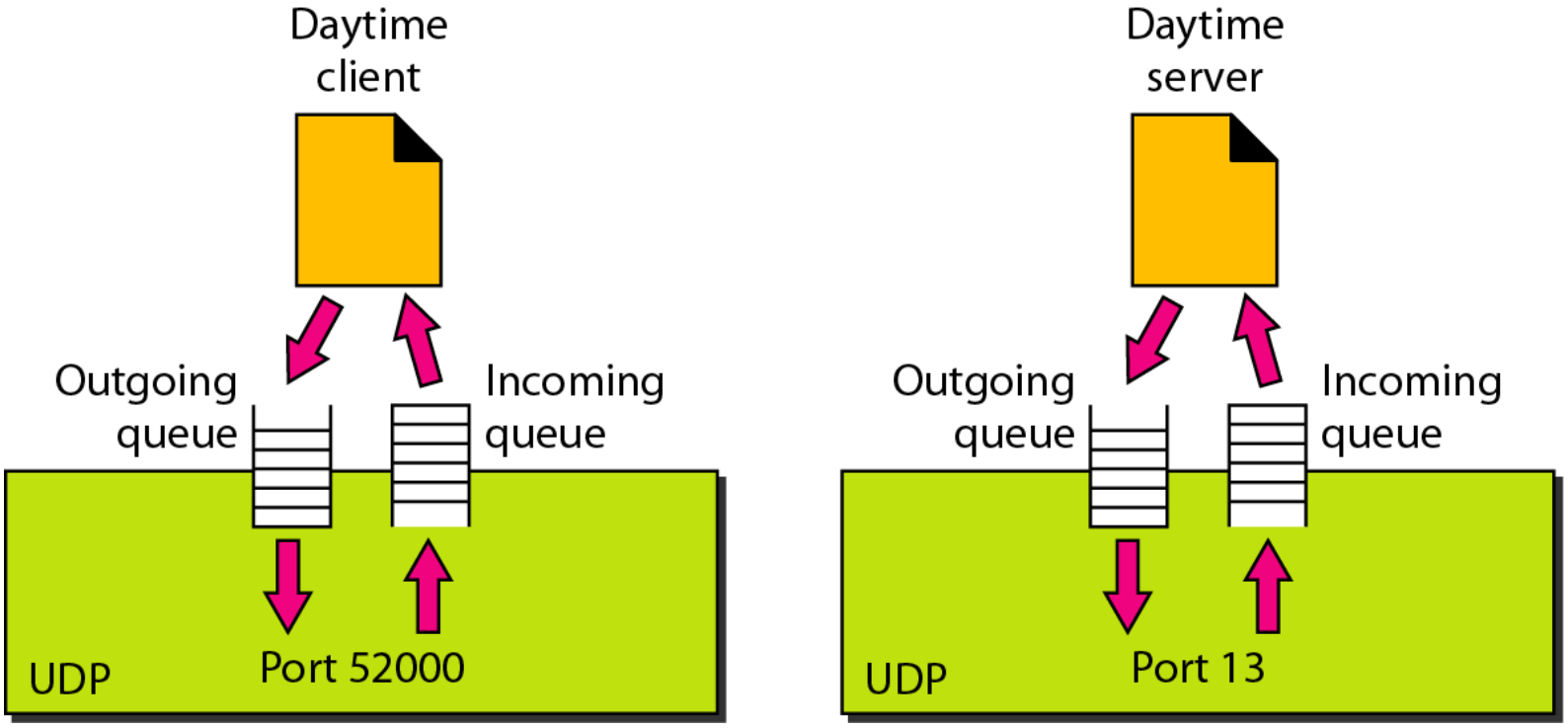
User Datagram Format

- UDP packets, called user datagrams, have fixed size header of 8 bytes.
- Figure below shows the format of a user datagram



DOWNLOADED FROM KTUASSIST.IN

Queues in UDP



DOWNLOADED FROM KTUASSIST.IN

Use of UDP

- UDP is suitable for a process that requires simple request response communication with little concern for flow and error control
- UDP is used for some route updating protocols such as RIP.
- UDP is suitable for multicasting

DOWNLOADED FROM KTUASSIST.IN

Transmission Control Protocol(TCP)

- TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data.
- In addition, TCP uses flow and error control mechanisms at the transport level.
- In brief, TCP is called a connection-oriented, reliable transport protocol

DOWNLOADED FROM KTUASSIST.IN

TCP Services

- Process-to-process delivery
- Stream delivery service
- Connection-oriented service
- Reliable service

DOWNLOADED FROM KTUASSIST.IN

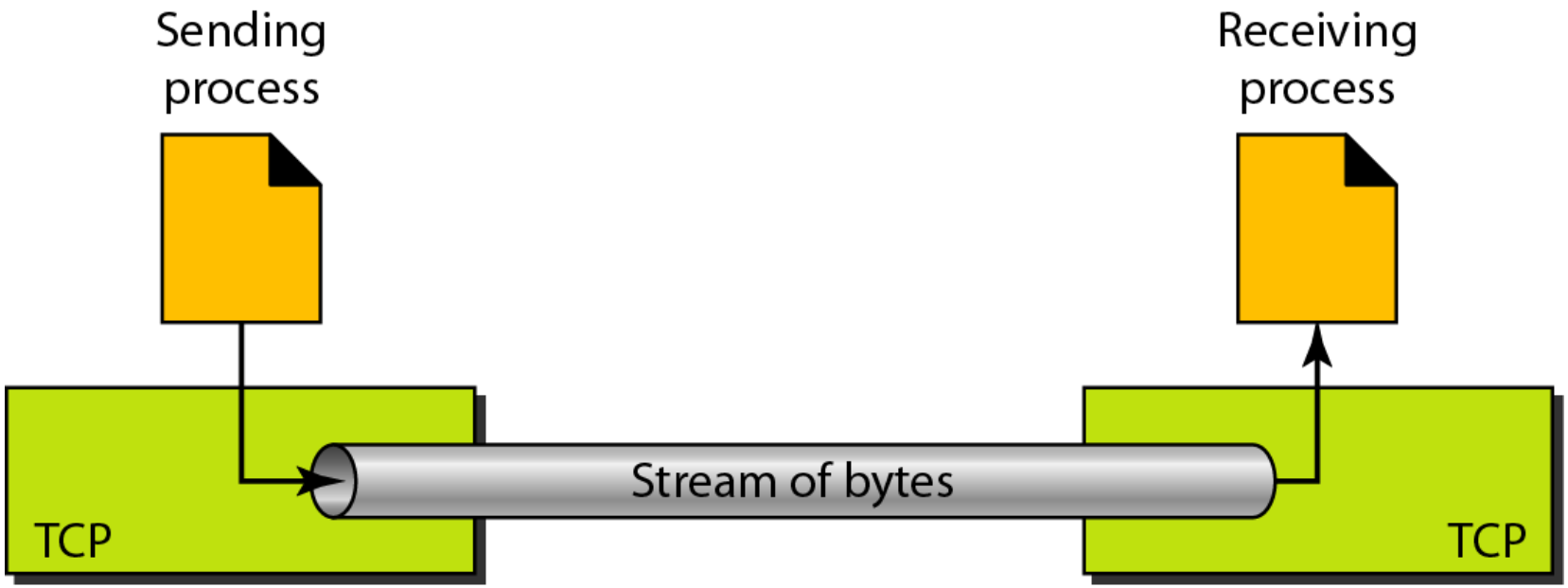
Well-known ports used by TCP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

DOWNLOADED FROM KTUASSIST.IN

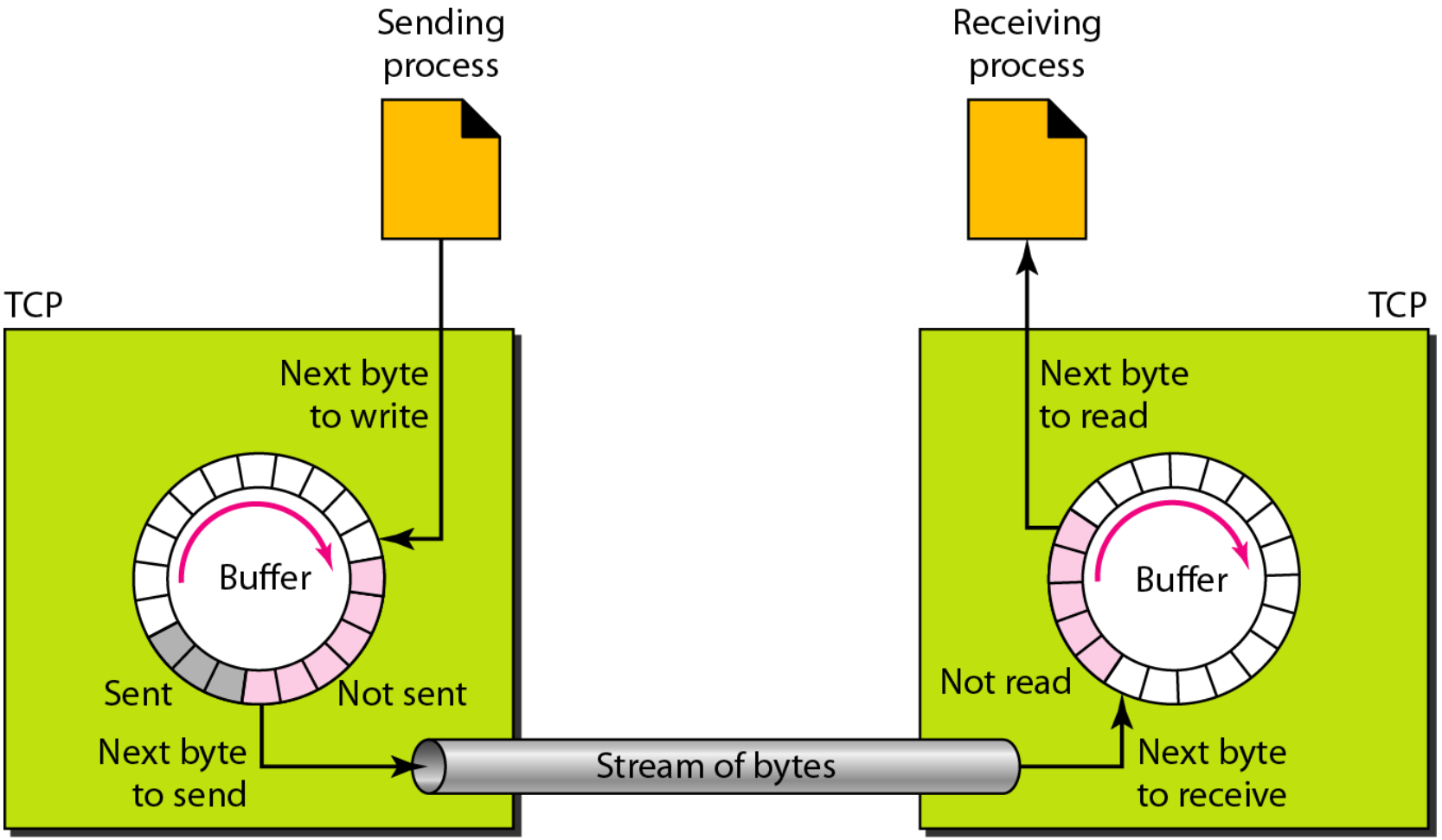
Stream Delivery Service

- TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes



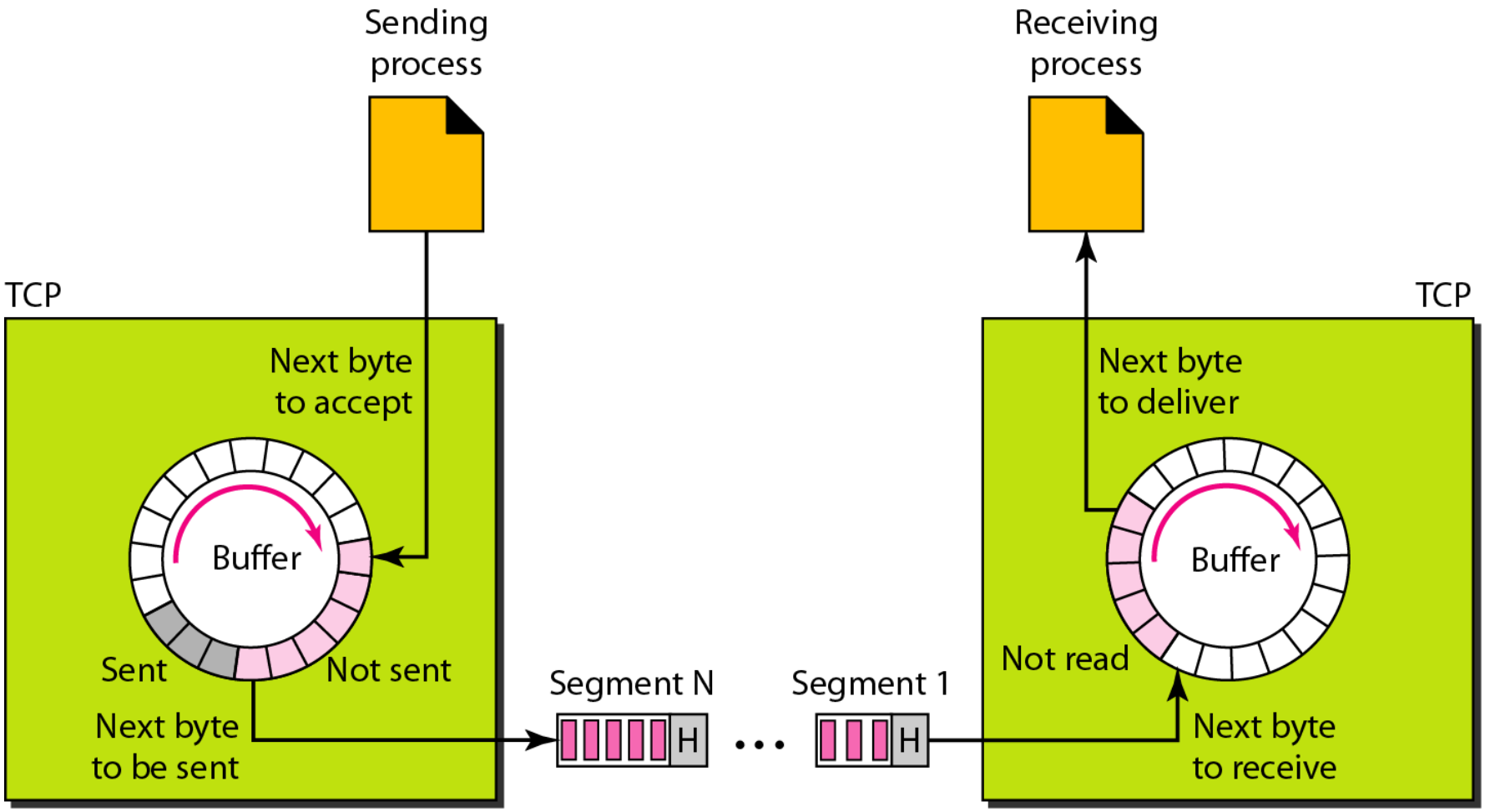
DOWNLOADED FROM KTUASSIST.IN

Sending and Receiving Buffers



DOWNLOADED FROM KTUASSIST.IN

TCP Segments



DOWNLOADED FROM KTUASSIST.IN

Connection-oriented Service

- When a process at site A wants to send and receive data from another process at site B,the following occurs:
  - The two TCPs establish a connection between them
  - Data are exchanged in both directions
  - The connection is terminated

DOWNLOADED FROM KTUASSIST.IN

Reliable Service

- TCP is a reliable transport protocol.
- It uses an acknowledgement mechanism to check the safe and sound arrival of data

DOWNLOADED FROM KTUASSIST.IN

TCP Features

- To provide the services mentioned in the previous slides, TCP has several features
  - Numbering System
  - Flow Control
  - Error Control
  - Congestion Control

DOWNLOADED FROM KTUASSIST.IN

Numbering System

- TCP header contains two fields: Sequence number and Acknowledgement number

The bytes of data being transferred in each connection are numbered by TCP.
The numbering starts with a randomly generated number.

- TCP generates a random number between 0 to 2^{32}-1 for the number of the first byte.
- For example if the random number happens to be 1057 and the total number to be sent is 6000 bytes, the bytes are numbered from 1057 to 7056

DOWNLOADED FROM KTUASSIST.IN

The following shows the sequence number for each segment:

Segment 1	→	**Sequence Number: 10,001 (range: 10,001 to 11,000)**
Segment 2	→	**Sequence Number: 11,001 (range: 11,001 to 12,000)**
Segment 3	→	**Sequence Number: 12,001 (range: 12,001 to 13,000)**
Segment 4	→	**Sequence Number: 13,001 (range: 13,001 to 14,000)**
Segment 5	→	**Sequence Number: 14,001 (range: 14,001 to 15,000)**

The value in the sequence number field of a segment defines the number of the first data byte contained in that segment.

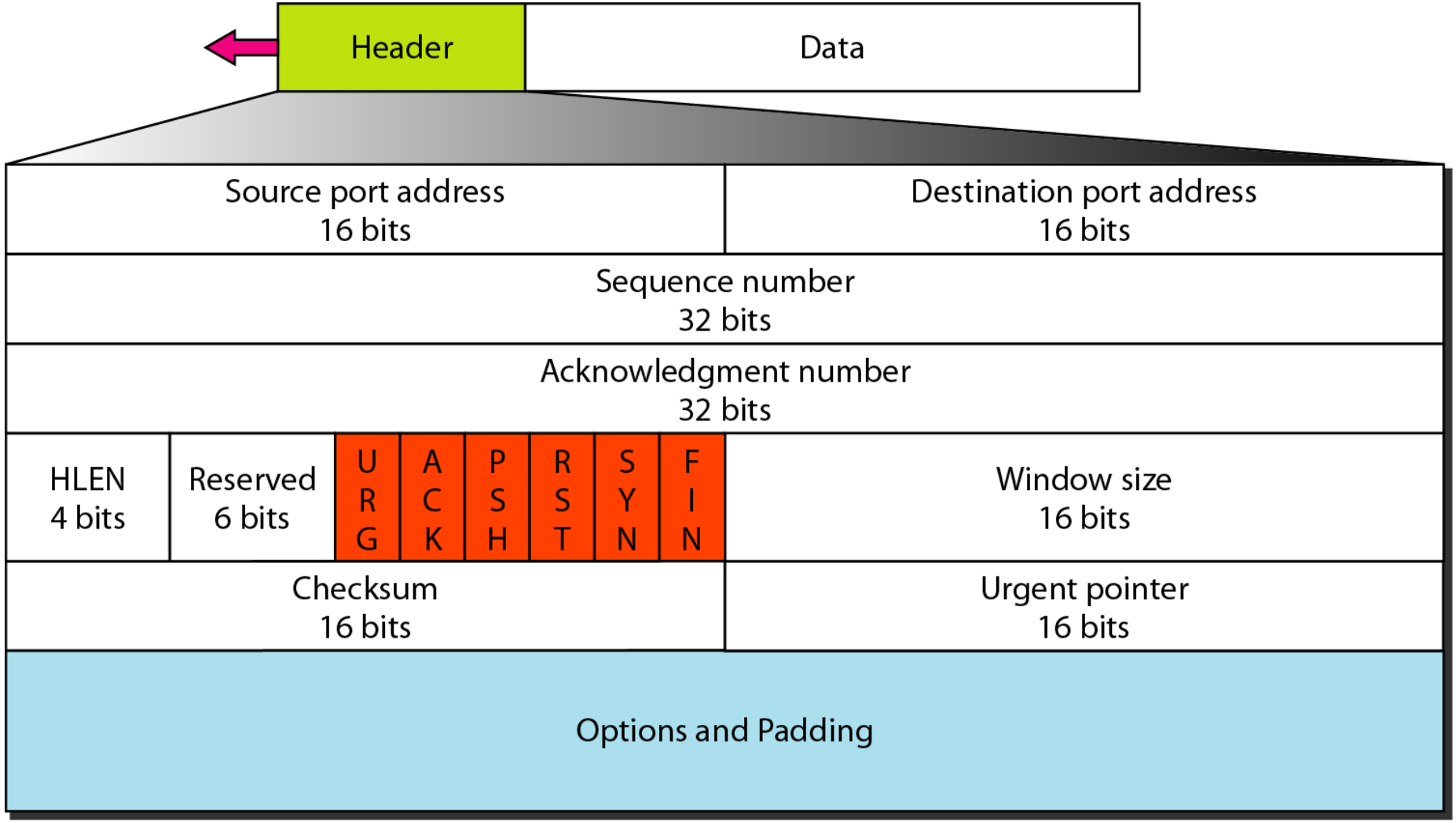
DOWNLOADED FROM KTUASSIST.IN

Acknowledgement number

The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive.
The acknowledgment number is cumulative.

DOWNLOADED FROM KTUASSIST.IN

TCP Segment Format



DOWNLOADED FROM KTUASSIST.IN

Segment

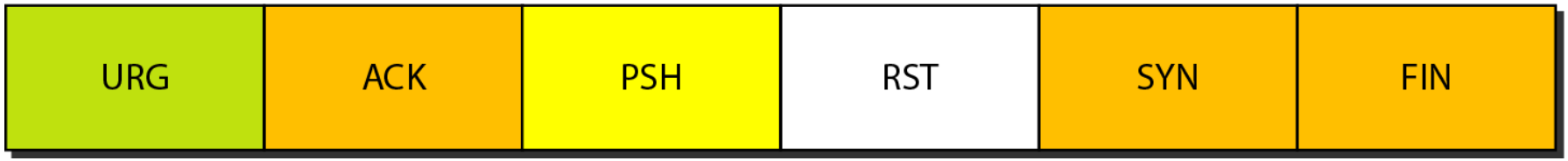
- The segment consists of a 20 to 60 byte header, followed by the application layer program
- The header is 20 bytes if there are no options and upto 60 bytes if it contains options

DOWNLOADED FROM KTUASSIST.IN

Control field

URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push

RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection



DOWNLOADED FROM KTUASSIST.IN

Description of flags in the control field

Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

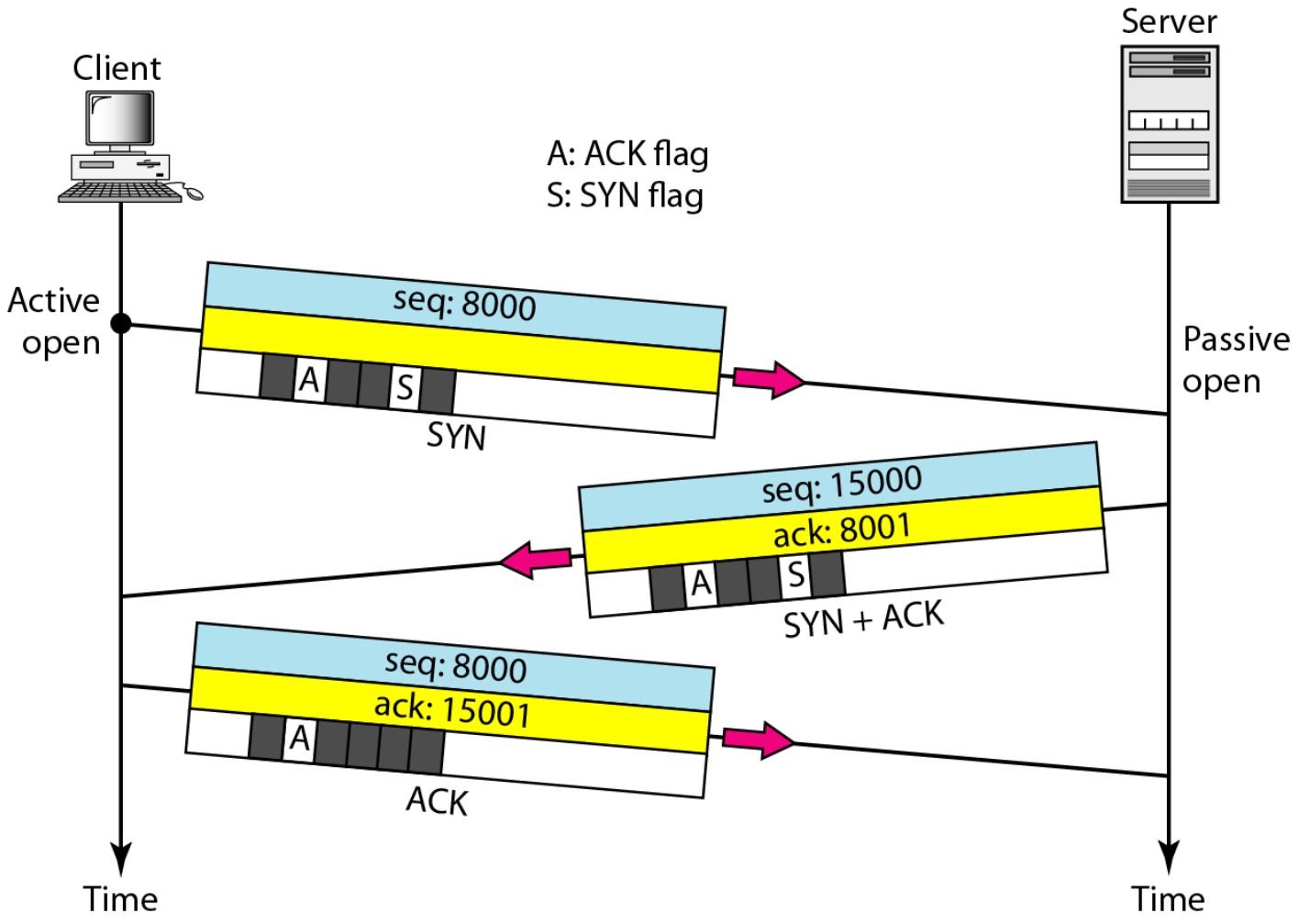
DOWNLOADED FROM KTUASSIST.IN

TCP Connection

- Connection Establishment (using three way handshake method)
- Data Transfer
- Connection termination using *either*
  - Three way Handshake *or*
  - Four way Handshake(Half Close)

DOWNLOADED FROM KTUASSIST.IN

Connection Establishment using Three-way Handshaking



DOWNLOADED FROM KTUASSIST.IN

Note

A SYN + ACK segment cannot carry data, but does consume one sequence number.

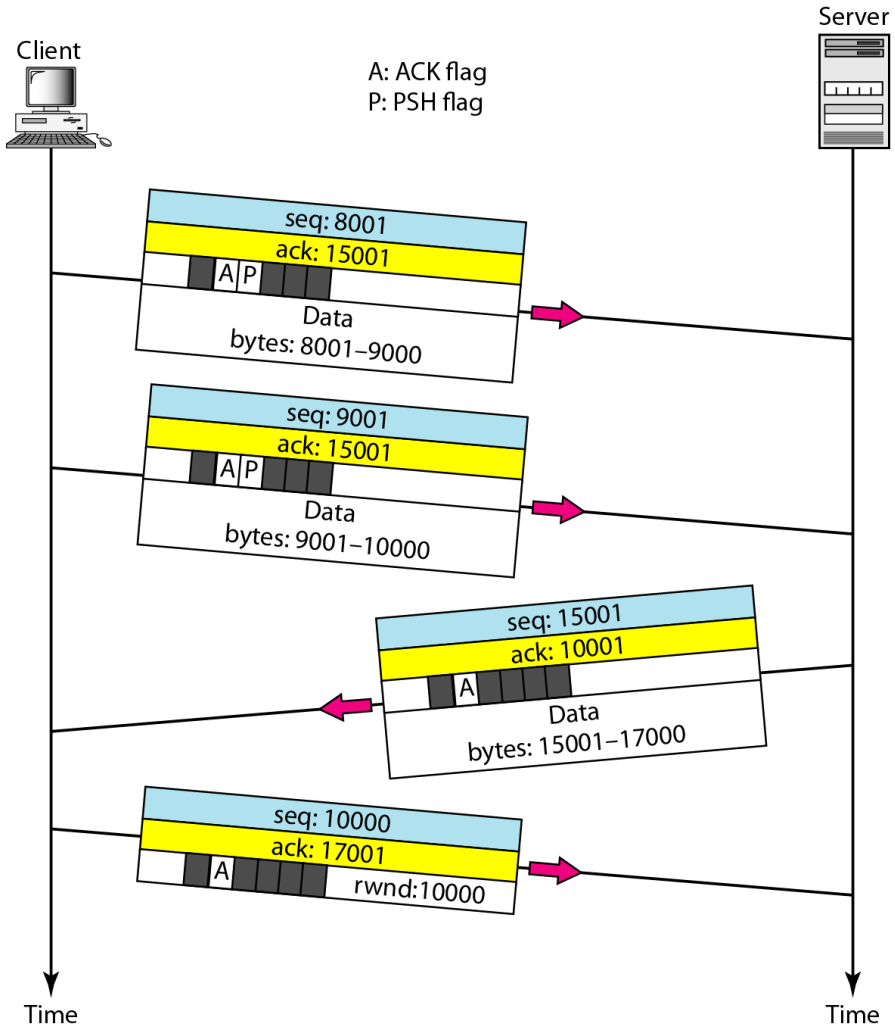
DOWNLOADED FROM KTUASSIST.IN

Note

An ACK segment, if carrying no data, consumes no sequence number.

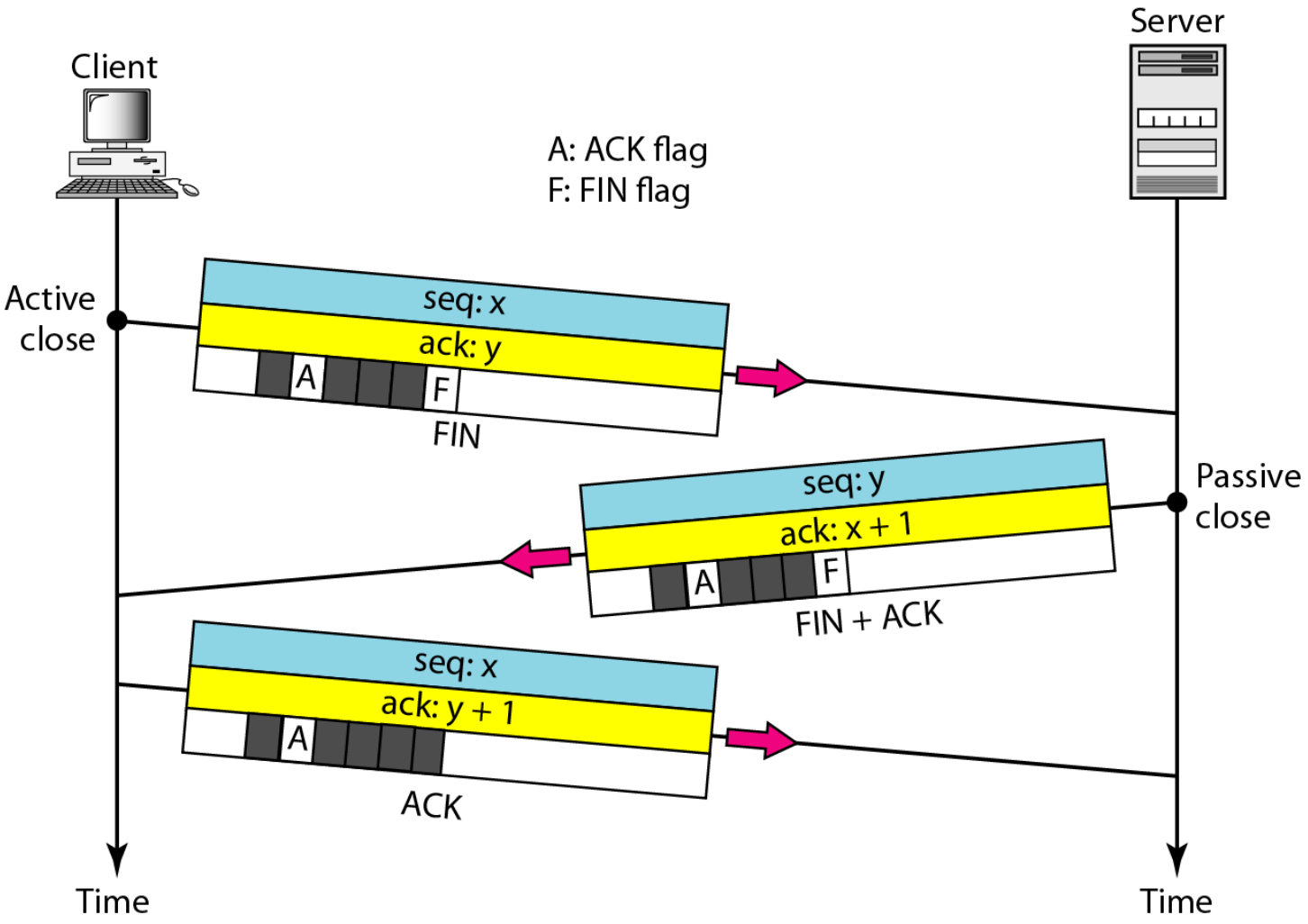
DOWNLOADED FROM KTUASSIST.IN

Data Transfer



DOWNLOADED FROM KTUASSIST.IN

Connection Termination using Three-way Handshaking



DOWNLOADED FROM KTUASSIST.IN

Note

The FIN segment consumes one sequence number if it does not carry data.

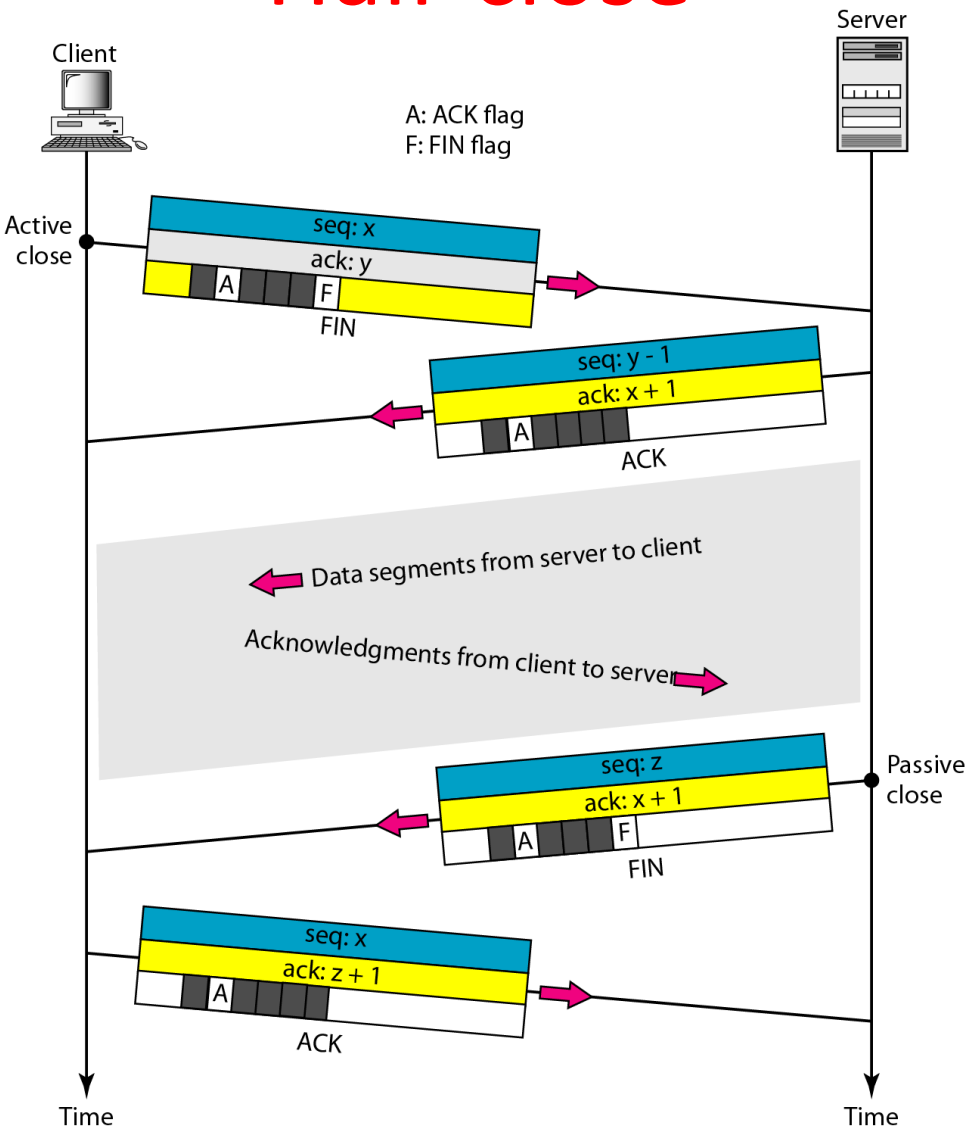
DOWNLOADED FROM KTUASSIST.IN

Note

The FIN + ACK segment consumes
one sequence number if it
does not carry data.

DOWNLOADED FROM KTUASSIST.IN

Half-close



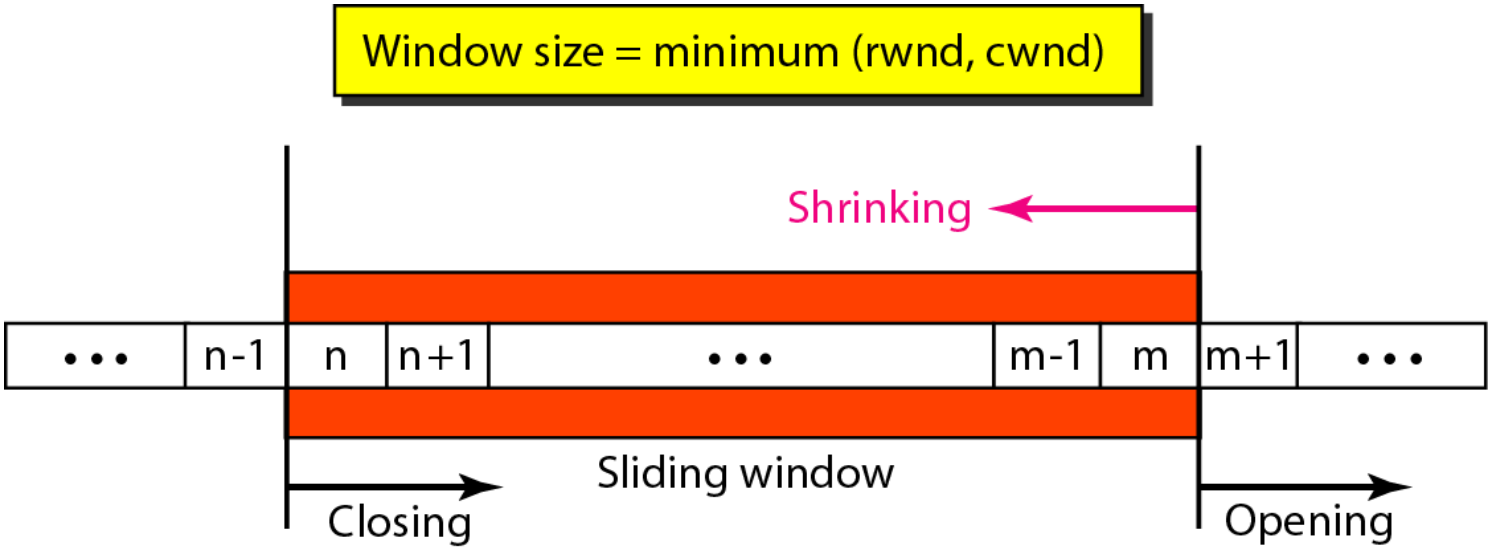
DOWNLOADED FROM KTUASSIST.IN

Flow Control in TCP

- A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data.
- TCP sliding windows are byte-oriented.
- The window size of the sender in TCP flow control mechanism is of variable size. It is the minimum of receiver window(rwnd) size and congestion window (cwnd) size

DOWNLOADED FROM KTUASSIST.IN

Sliding window



DOWNLOADED FROM KTUASSIST.IN

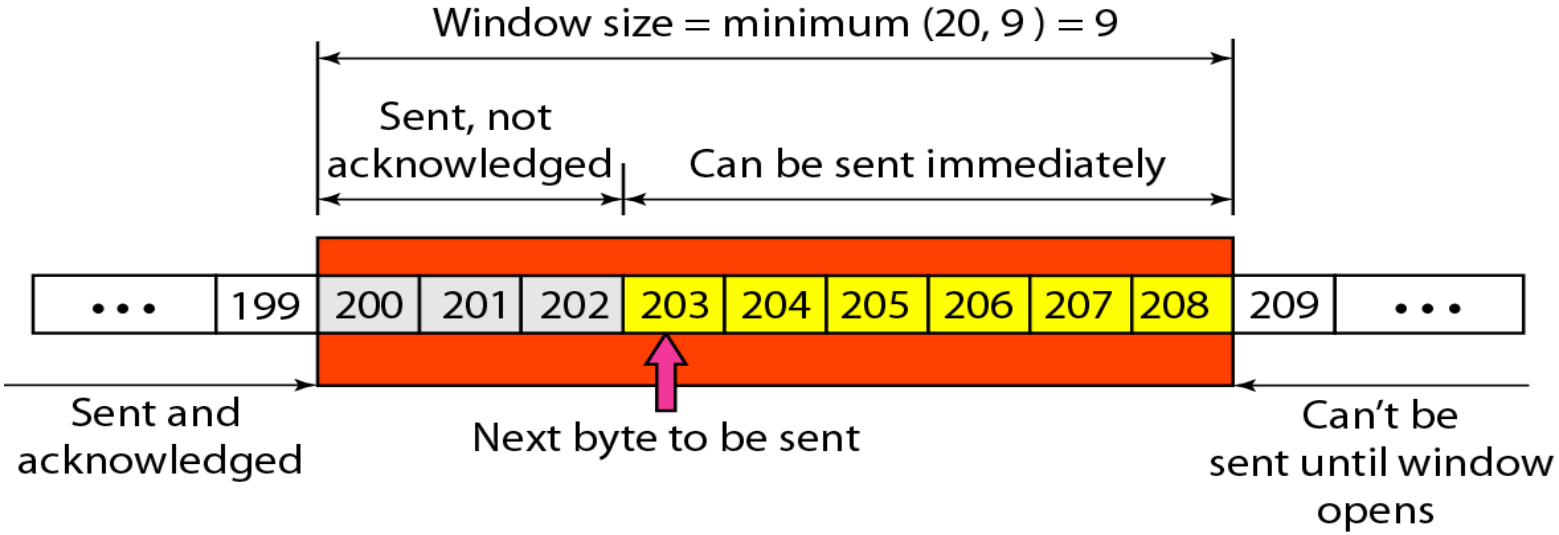
What is the value of the receiver window (rwnd) for host A if the receiver, host B, has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data?

Solution

The value of rwnd = 5000 − 1000 = 4000. Host B can receive only 4000 bytes of data before overflowing its buffer. Host B advertises this value in its next segment to A.

DOWNLOADED FROM KTUASSIST.IN

Figure shows an unrealistic example of a sliding window. The sender has sent bytes up to 202. We assume that cwnd is 20 (in reality this value is thousands of bytes). The receiver has sent an acknowledgment number of 200 with an rwnd of 9 bytes (in reality this value is thousands of bytes). The size of the sender window is the minimum of rwnd and cwnd, or 9 bytes. Bytes 200 to 202 are sent, but not acknowledged. Bytes 203 to 208 can be sent without worrying about acknowledgment. Bytes 209 and above cannot be sent.



DOWNLOADED FROM KTUASSIST.IN

Note

Some points about TCP sliding windows:

- The size of the window is the lesser of rwnd and cwnd.
- The source does not have to send a full window's worth of data.
- The window can be opened or closed by the receiver, but should not be shrunk.
- The destination can send an acknowledgment at any time as long as it does not result in a shrinking window.
- The receiver can temporarily shut down the window; the sender, however, can always send a segment of 1 byte after the window is shut down.

DOWNLOADED FROM KTUASSIST.IN

Error Control in TCP

- TCP provides reliability using error control
- Error control includes mechanisms for detecting corrupted segments, lost segments, out of order segments
- Error detection in TCP is achieved through the use of three simple tools:
  - Checksum
  - Acknowledgement
  - Time out

DOWNLOADED FROM KTUASSIST.IN

Error Control in TCP

- Error detection in TCP is achieved through the use of three simple tools:
  - Checksum: Each segment includes a checksum field which is used to check for a corrupted segment. If a segment is corrupted, it is discarded by the destination TCP
  - Acknowledgement
  - Time out

DOWNLOADED FROM KTUASSIST.IN

Error Control in TCP

- Error detection in TCP is achieved through the use of three simple tools:
  - Checksum
  - Acknowledgement: TCP uses acknowledgements to confirm the receipt of data segments
  - Time out

DOWNLOADED FROM KTUASSIST.IN

Error Control in TCP

- Error detection in TCP is achieved through the use of three simple tools:
  - Checksum
  - Acknowledgement
  - Time out: When a segment is corrupted, lost or delayed, it is retransmitted. A segment is retransmitted on two occasions: when a retransmission timer expires or when the sender receives three duplicate ACKs

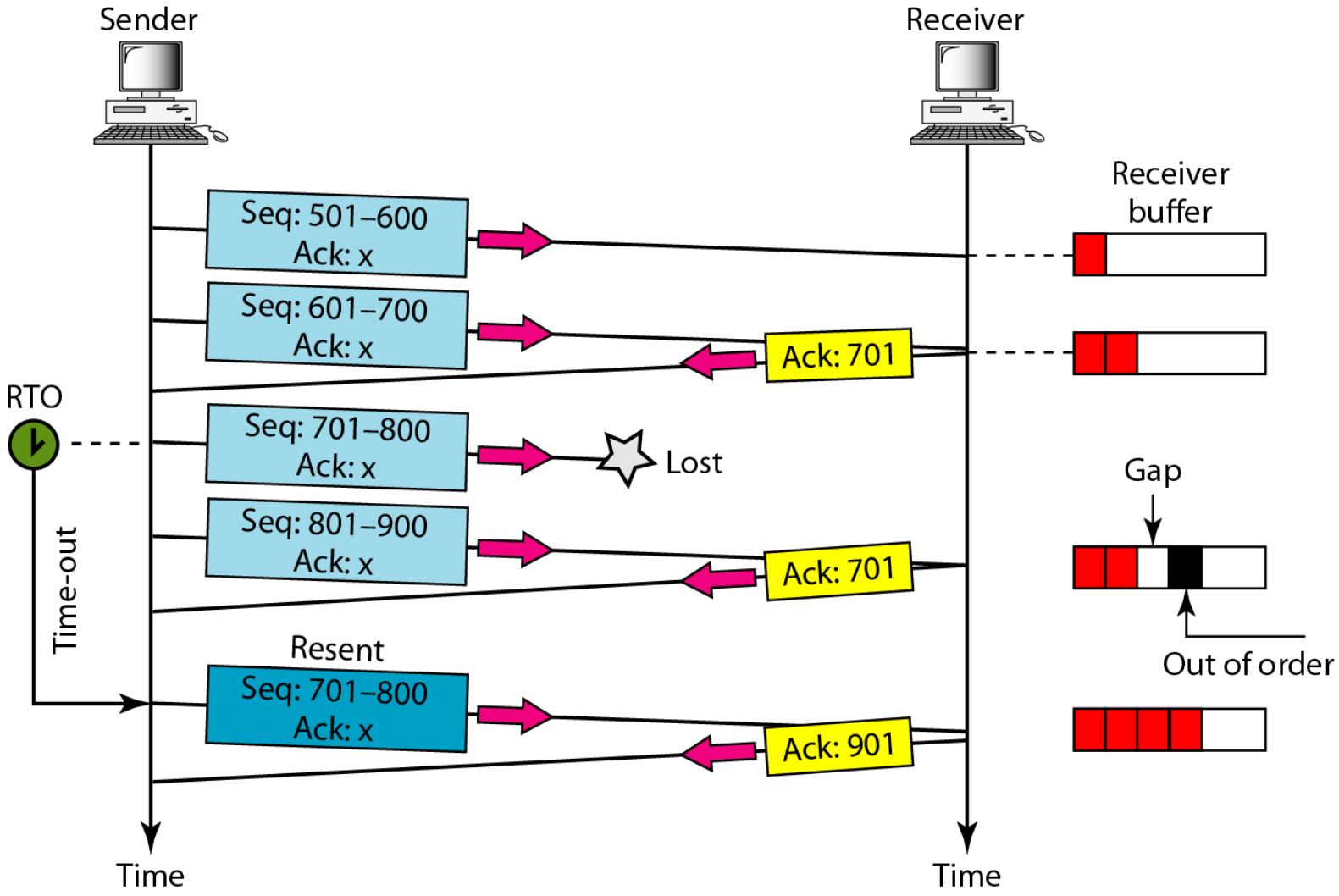
DOWNLOADED FROM KTUASSIST.IN

Note

Data may arrive out of order and be temporarily stored by the receiving TCP, but TCP guarantees that no out-of-order segment is delivered to the process.

DOWNLOADED FROM KTUASSIST.IN

Lost segment



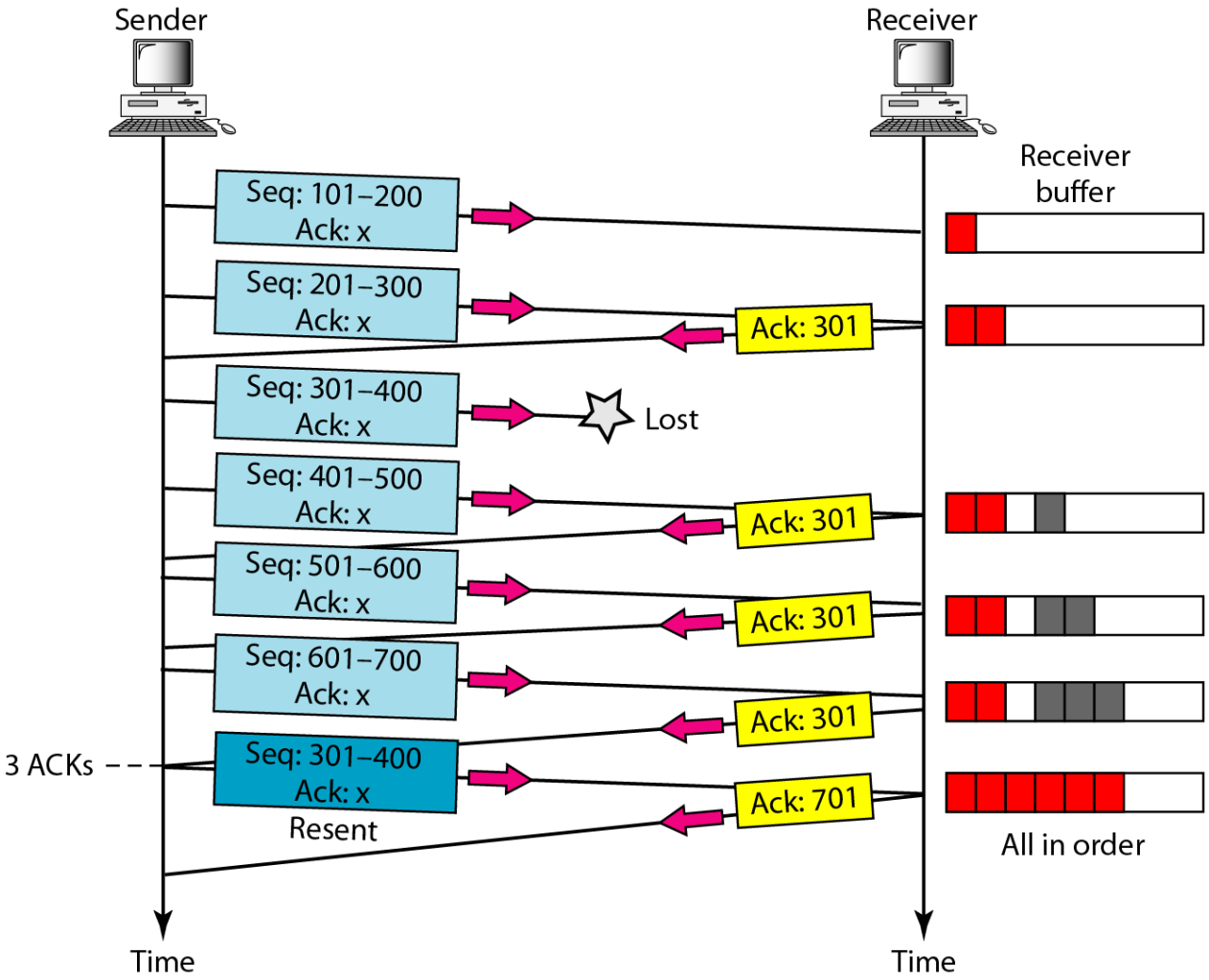
DOWNLOADED FROM KTUASSIST.IN

Note

The receiver TCP delivers only ordered data to the process.

DOWNLOADED FROM KTUASSIST.IN

Fast Retransmission



DOWNLOADED FROM KTUASSIST.IN

Comparison between TCP & UDP

- TCP
  - Connection oriented
  - Relaible
  - Error Control
  - More overhead
  - Slow Transmission
  - Flow Control,Congestion control
  - Examples of applications/protocols using TCP: http,ftp etc.
- UDP
  - Connection less
  - Unrelaible
  - Error Control optional
  - Less overhead
  - Fast Transmission
  - No Flow Control & Congestion control
  - Examples of applications/protocols using UDP: DNS,RIP,DHCP etc.

DOWNLOADED FROM KTUASSIST.IN

Congestion Control & Quality of Service

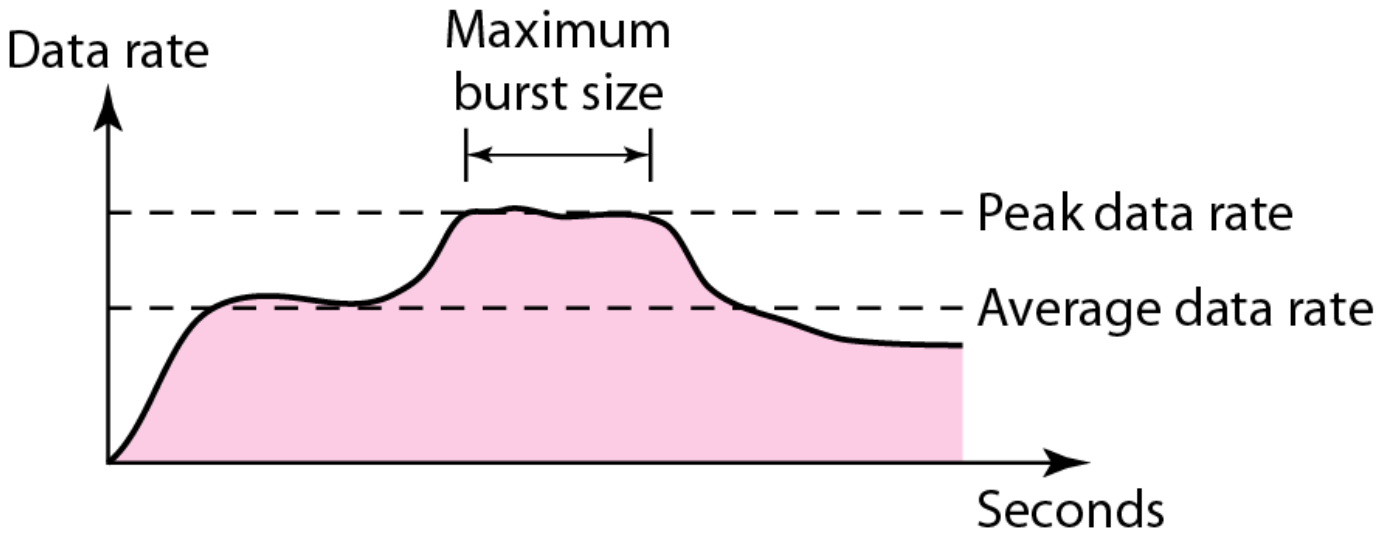
DOWNLOADED FROM KTUASSIST.IN

DATA TRAFFIC

- The main focus of congestion control and quality of service is data traffic.
- In congestion control we try to avoid traffic congestion.
- In quality of service, we try to create an appropriate environment for the traffic.
- So, before talking about congestion control and quality of service, we discuss the data traffic itself.

DOWNLOADED FROM KTUASSIST.IN

Traffic Descriptors



DOWNLOADED FROM KTUASSIST.IN

Traffic Descriptors

- Traffic descriptors are qualitative values that represent a data flow
  - Average Data Rate: is the number of bits sent during a period of time, divided by the number of seconds in that period. It indicates the average bandwidth needed by the traffic.
  - Peak Data Rate
  - Maximum Burst Size

DOWNLOADED FROM KTUASSIST.IN

Traffic Descriptors

- Traffic descriptors are qualitative values that represent a data flow
  - Average Data Rate
  - Peak Data Rate: defines the maximum data rate of the traffic. In the figure, it is the maximum y axis value. It is important because it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.
  - Maximum Burst Size

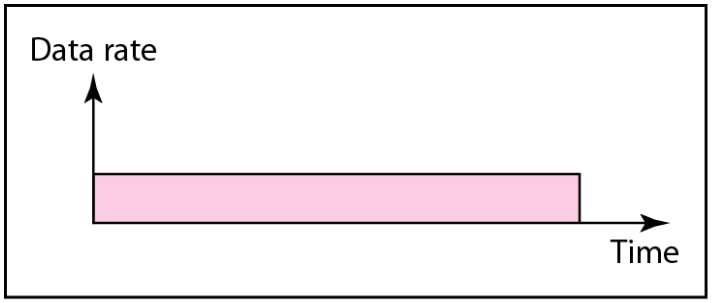
DOWNLOADED FROM KTUASSIST.IN

Traffic Descriptors

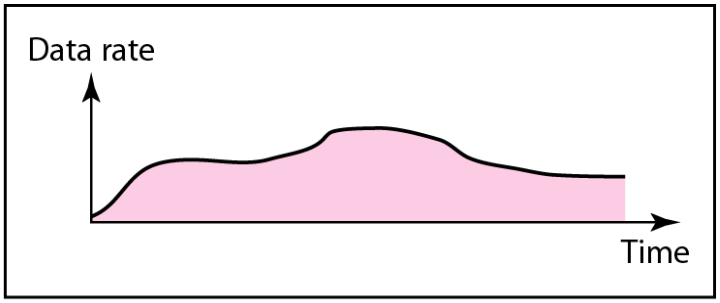
- Traffic descriptors are qualitative values that represent a data flow
  - Average Data Rate
  - Peak Data Rate
  - Maximum Burst Size: It normally refers to the maximum length of time the traffic is generated at the peak rate

DOWNLOADED FROM KTUASSIST.IN

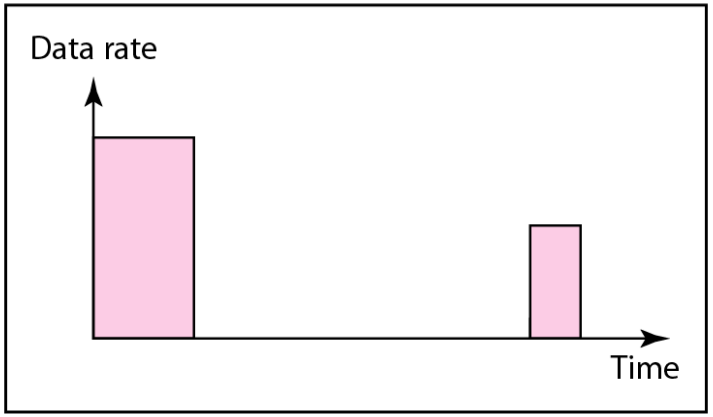
Three Traffic Profiles



a. Constant bit rate



b. Variable bit rate



c. Bursty

DOWNLOADED FROM KTUASSIST.IN

Three Traffic Profiles

- Constant bit-rate:
  - Fixed-rate
  - Data rate does not change.
  - Average and peak data rate are the same.
- Variable-bit rate
  - Rate of data flow changes in time, with the changes smooth instead of sudden and sharp
  - Average and peak data rate are different
  - Maximum burst size is usually small value.
- Bursty traffic
  - Data rate changes in a very short period of time.
  - Average and peak bit rates are very different in this type of flow.
  - Maximum burst size is significant
  - Most difficult type of traffic to handle because the profile is very unpredictable.
  - One of the main causes of congestion.

DOWNLOADED FROM KTUASSIST.IN

CONGESTION

- Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle.
- Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

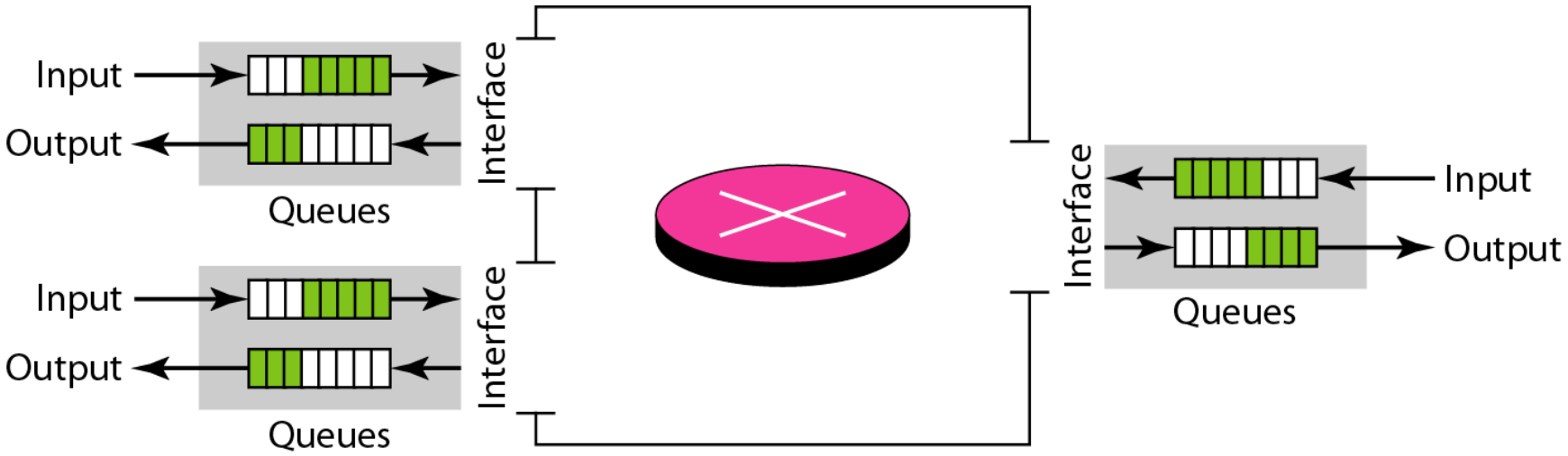
DOWNLOADED FROM KTUASSIST.IN

Queues in a Router

- Congestion in a network occurs because routers and switches have queues-buffers that hold packets before and after processing.
- A router, for example, has an input queue and an output queue for each interface.
- When a packet arrives at the incoming interface, it undergoes three steps before departing:
  - The packet is put at the end of the input queue
  - The processing module remove the packet from the queue once it reaches the front of the queue and uses its routing table to find the route
  - The packet is put in the appropriate output queue and waits its turn to be sent
- Two issues: if the rate packet arrival is higher than the packet processing rate, the input queues become longer and longer
- Second, if the packet departure rate is less than the packet processing rate, the output queues become longer and longer

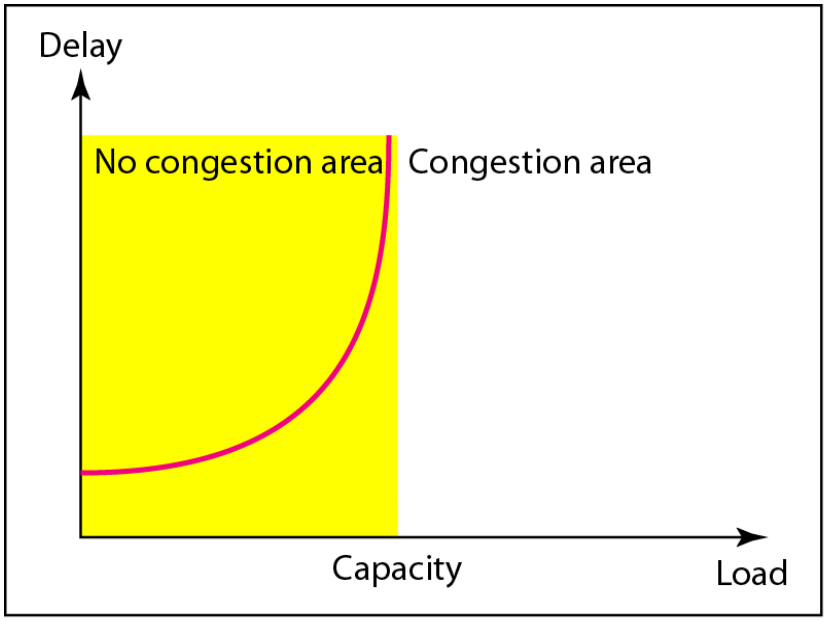
DOWNLOADED FROM KTUASSIST.IN

Queues in a Router

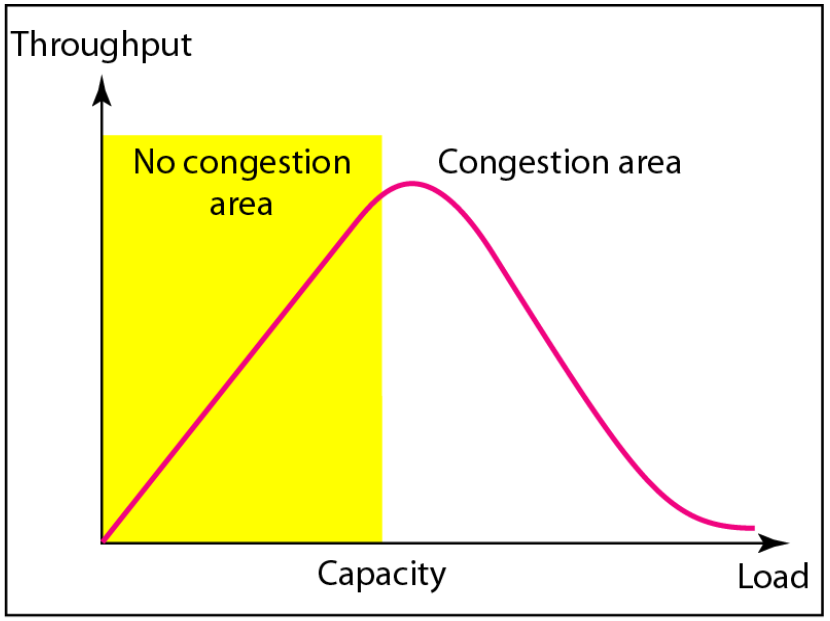


DOWNLOADED FROM KTUASSIST.IN

Network Performance: Packet Delay and Throughput as functions of load



a. Delay as a function of load



b. Throughput as a function of load

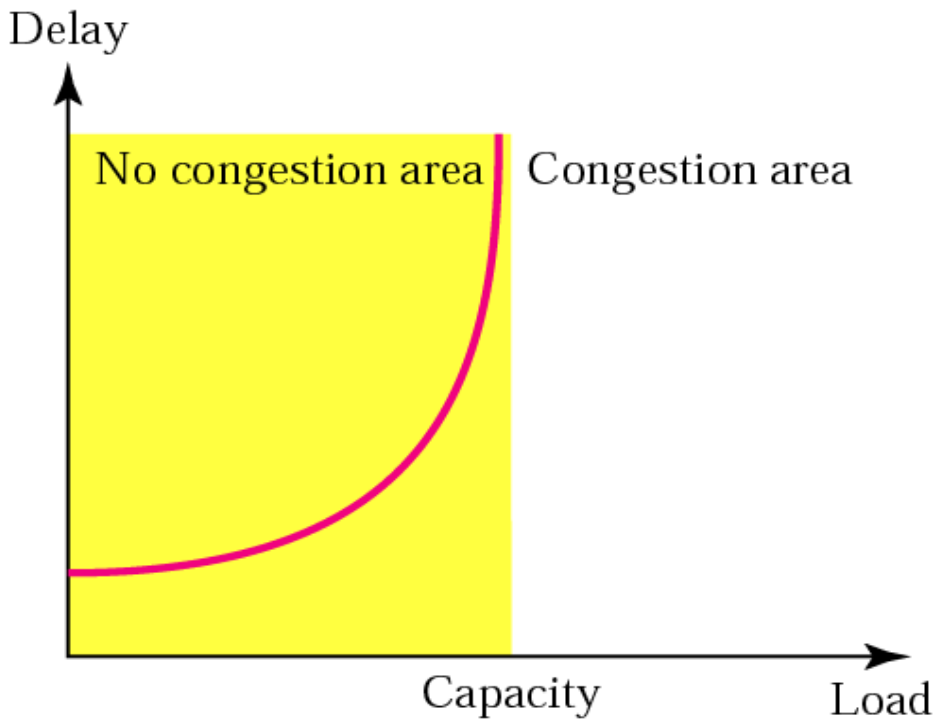
DOWNLOADED FROM KTUASSIST.IN

Delay versus Load

- When load is much less than capacity, the delay is at minimum. Minimum delay is due to propagation delay and processing delay.
- When load reaches the network capacity, the delay increases sharply due to addition of waiting time in the queues.
- Delay has negative effect on the load and consequently the congestion. When a packet is delayed, the source, not receiving the acknowledgement, retransmits the packet, which makes the delay, and the congestion, worse.

DOWNLOADED FROM KTUASSIST.IN

Delay versus Load



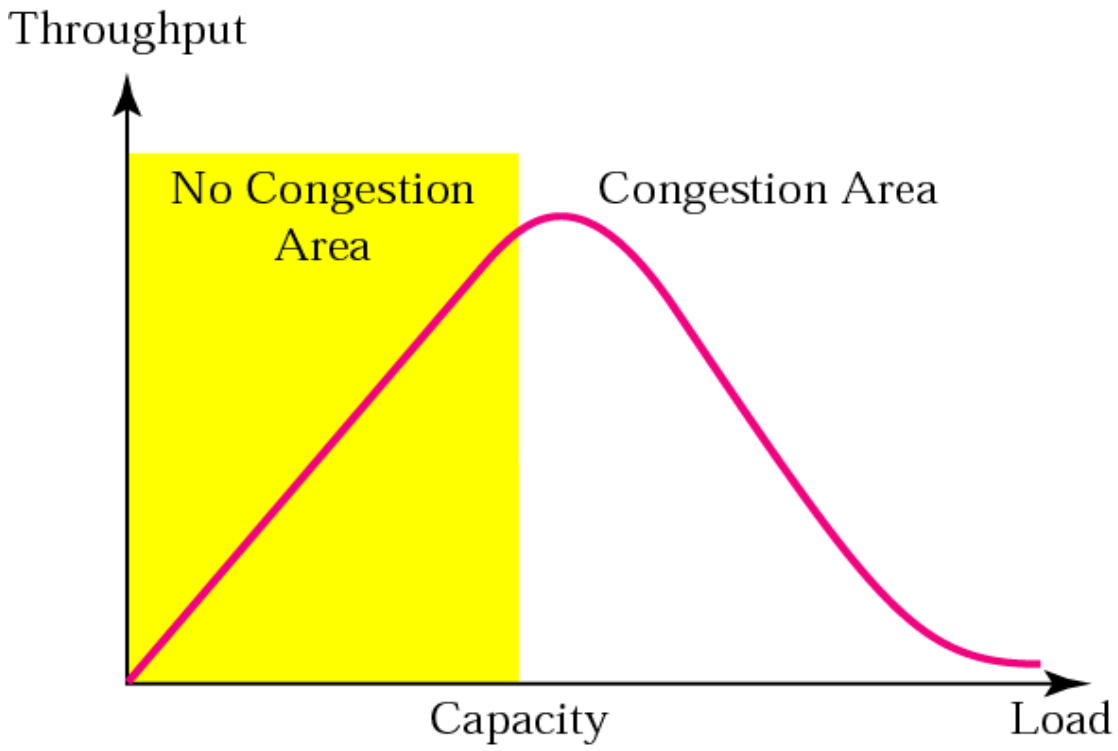
DOWNLOADED FROM KTUASSIST.IN

Performance:
Throughput vs Network load

- We can define throughput in a network as the number of packets passing through the network in a unit of time.
- When the load is below the capacity of the network, the throughput increases proportionally with the load.
- The throughput declines sharply after the load reaches to its capacity due to discarding of packets by routers.
- When the load exceeds the capacity, the queues become full and routers have to discard some packets.
- Discarding packets does not reduce the number of packets in the network because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destination.

DOWNLOADED FROM KTUASSIST.IN

Performance:
Throughput vs Network load



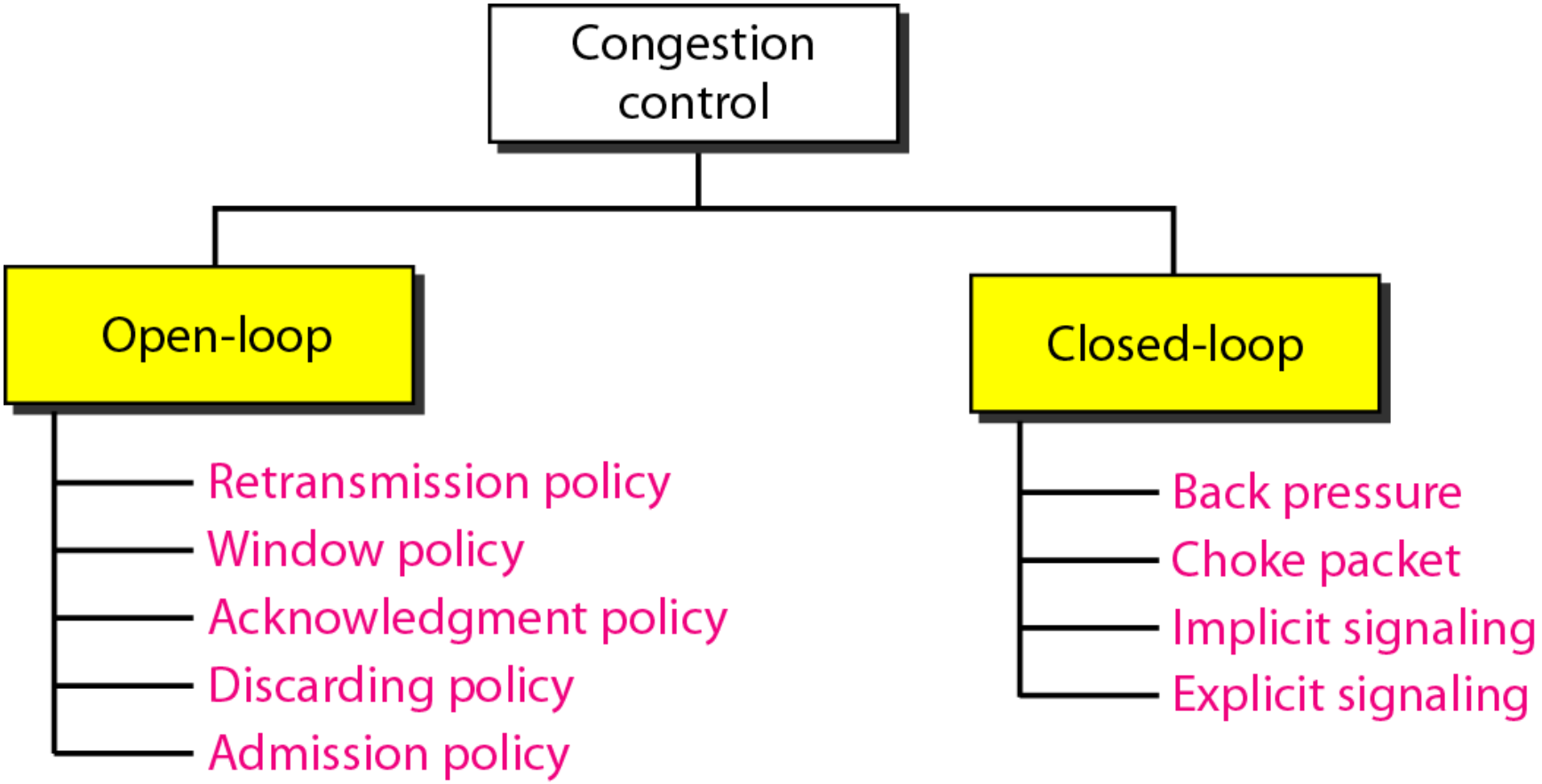
DOWNLOADED FROM KTUASSIST.IN

CONGESTION CONTROL

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.
- In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal).

DOWNLOADED FROM KTUASSIST.IN

Congestion Control Categories



DOWNLOADED FROM KTUASSIST.IN

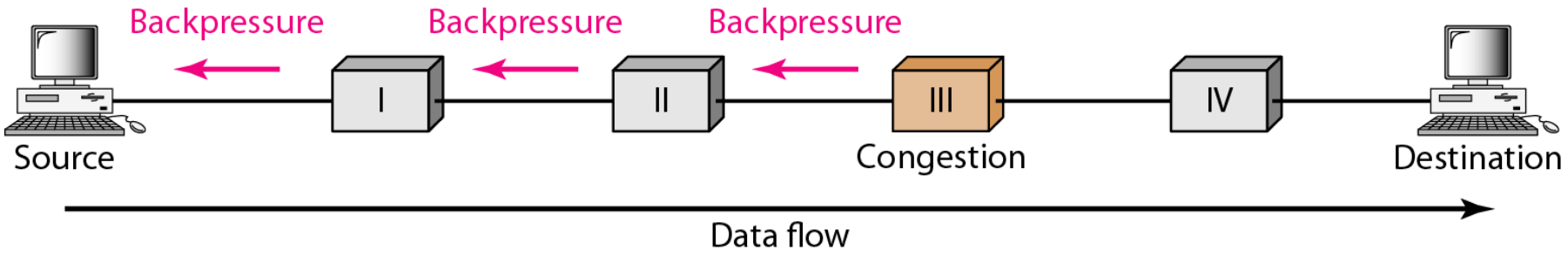
Open-loop congestion control [Prevention]

- Policies are applied to prevent congestion before it happens.
- Congestion control is handled by either the source or the destination.
  - Retransmission policy: to optimize efficiency and reduce congestion set proper retransmission policy and timers.
  - Windows policy: Type of window at sender may also affect congestion. Selective repeat is better than Go-Back-N.
  - Acknowledgement policy: Policy set by receiver may also affect congestion. If receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
  - Discard policy: Discard less sensitive packets [in audio transmission] at routers.
  - Admission policy: Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion

DOWNLOADED FROM KTUASSIST.IN

Closed-loop congestion control [Removal]

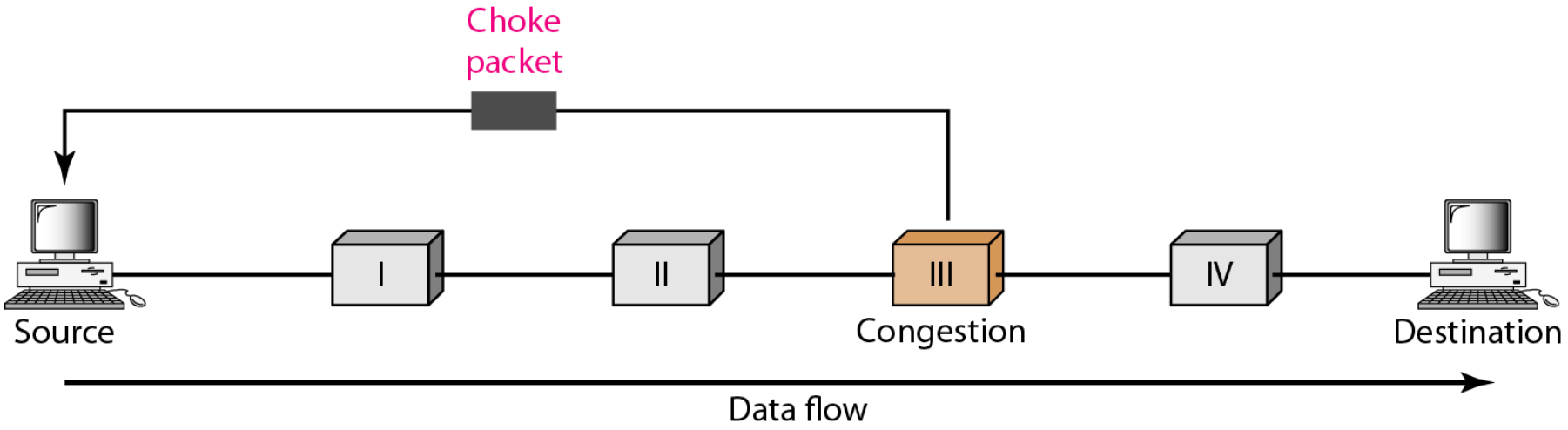
- **Back Pressure**: When a router is congested, it can inform the previous upstream router to reduce the rate of outgoing packets. The action can be recursive all the way to the router before the source.



DOWNLOADED FROM KTUASSIST.IN

Closed-loop congestion control [Removal]

- Choke Packet: A packet sent by a router to the source to inform it of congestion. This type of control is similar to ICMP's source quench packet.



DOWNLOADED FROM KTUASSIST.IN

Closed-loop congestion control [Removal]

- Implicit signaling: There is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms.
- For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

DOWNLOADED FROM KTUASSIST.IN

Closed-loop congestion control [Removal]

- Explicit Signaling:
- The node that experiences congestion can explicitly send a signal to the source or destination.
- The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data.
  - Backward Signaling: Bit can be set in a packet moving in the direction opposite to the congestion; indicate the source.
  - Forward Signaling: Bit can be set in a packet moving in the direction of the congestion; indicate the destination.

DOWNLOADED FROM KTUASSIST.IN

Congestion Control in TCP

- Packet from a sender may pass through several routers before reaching its final destination.
- Router has a buffer that stores the incoming packets, processes them, and forwards them.
- If a router receives packets faster than it can process, congestion might occur and some packets could be dropped.
- When a packet does not reach the destination, no acknowledgement is sent for it.
- The sender has no choice but to retransmit the lost packet. This may create more congestion and more dropping of packets, which means more retransmission and more congestion.
- A point may then be reached in which the whole system collapses and no more data can be sent. TCP therefore needs to find some way to avoid this situation.
- If the network cannot deliver the data as fast as they are created by the sender, it needs to tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window in TCP.
- If the cause of the lost segment is congestion, retransmission of the segment does not remove the cause – it aggravates it.

DOWNLOADED FROM KTUASSIST.IN

Congestion Window

- In TCP, sender's window size is determined not only by the receiver but also by congestion in the network.

Actual window size = minimum (rwnd size, congestion window size)

DOWNLOADED FROM KTUASSIST.IN

Congestion Policy in TCP

- TCPs general policy for handling congestion is based on three phases:
  - Slow start: Exponential Increase
  - Congestion Avoidance: Additive Increase
  - Congestion Detection: Multiplicative Decrease

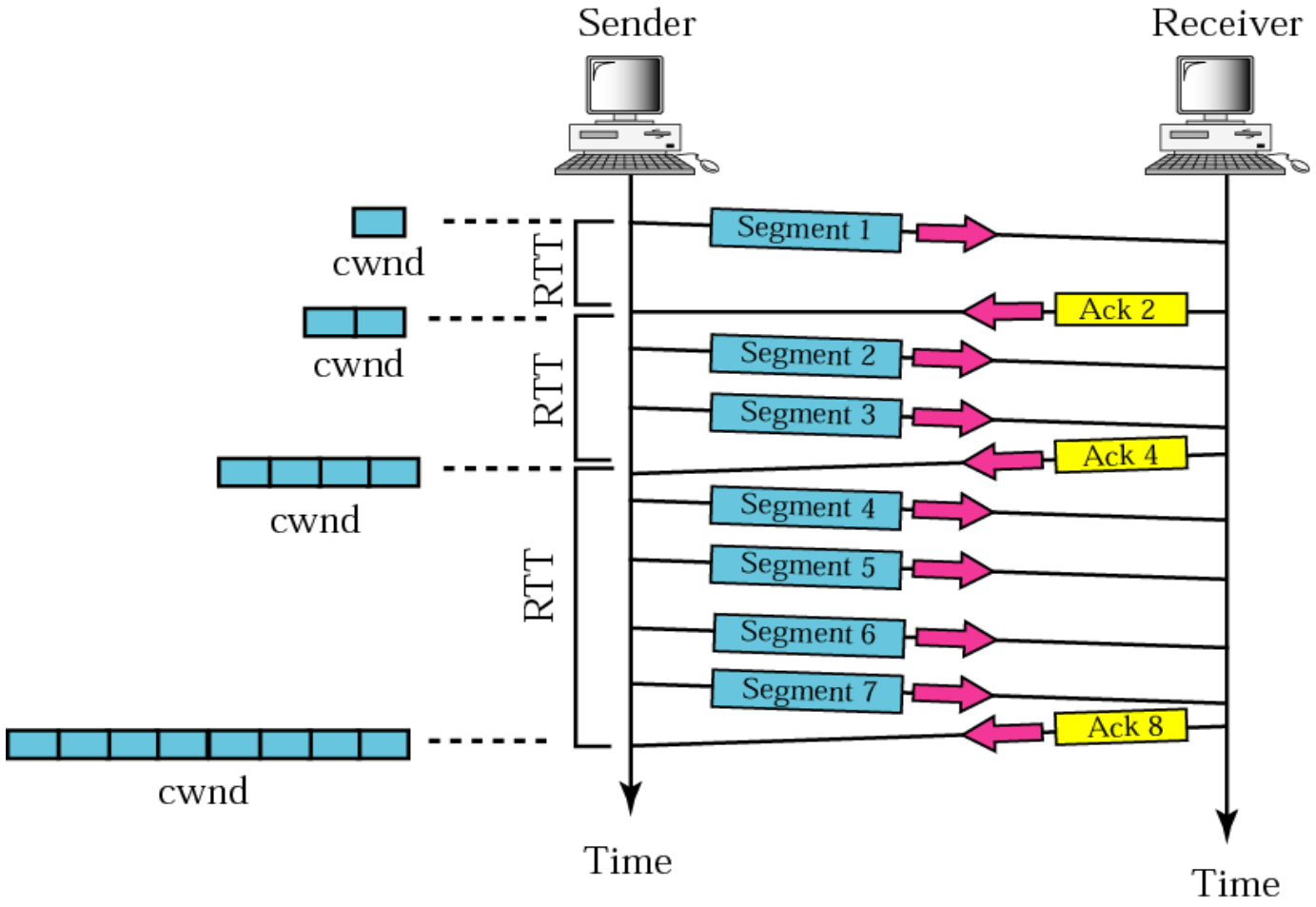
DOWNLOADED FROM KTUASSIST.IN

Slow Start

- At start of a connection, TCP sets the congestion window to one.
- For each segment that is ACKed, TCP increases the size of the congestion window by one maximum segment size until it reaches a threshold → increases exponentially. [Called as slow start, which is a misleading name]
- Sender sends one segment, receives one ACK, increases the size to two segments, sends two segments, receives ACKs for two segments, increases the size to four segments, sends four segments, receives ACK for four segments and so on.

DOWNLOADED FROM KTUASSIST.IN

Slow Start



DOWNLOADED FROM KTUASSIST.IN

Slow Start

- In the slow start algorithm, the size of the congestion window increases exponentially until it reaches a threshold

Start → cwnd = 1

After 1 RTT → cwnd = 1 x 2 = 2 → 2^1

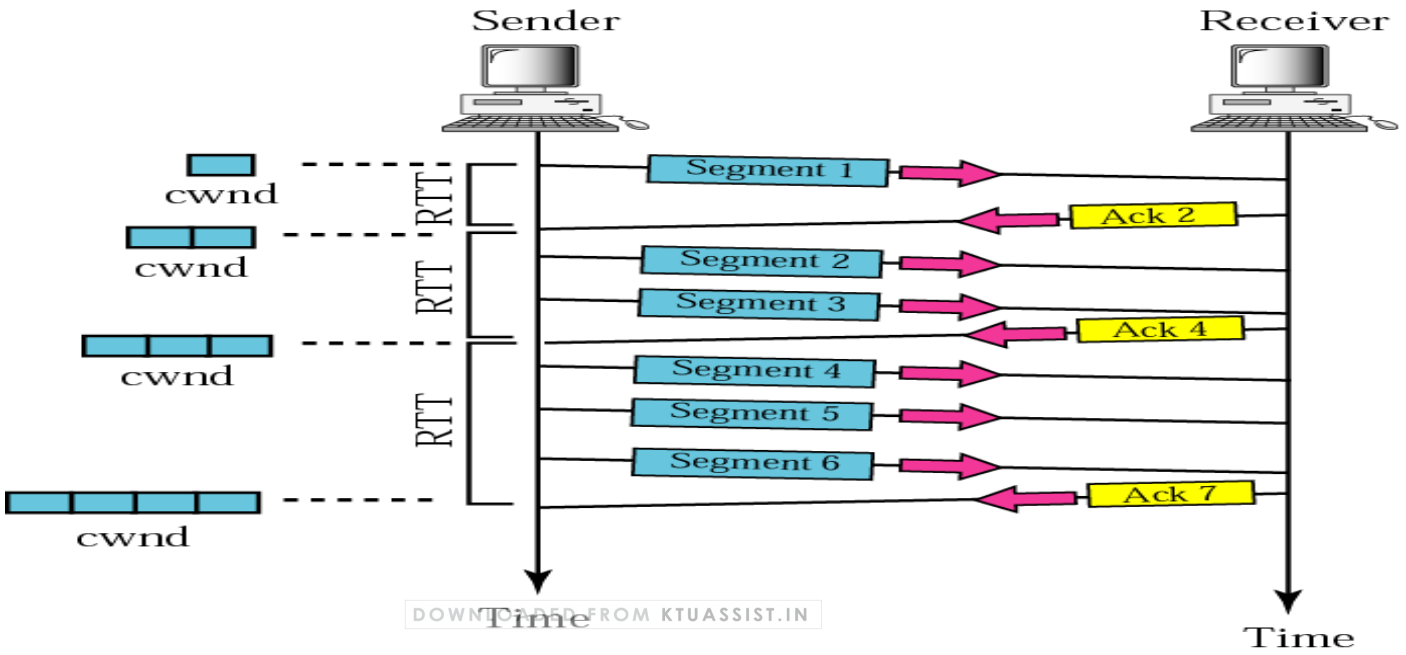
After 2 RTT → cwnd = 2 x 2 = 4 → 2^2

After 3 RTT → cwnd = 4 x 2 = 8 → 2^3

DOWNLOADED FROM KTUASSIST.IN

Congestion Avoidance: Additive Increase

- Congestion avoidance: additive increase
  - When the size of the congestion window reaches the slow start threshold, in the congestion avoidance algorithm, the size of the congestion window increases additively until congestion is detected



DOWNLOADED FROM KTUASSIST.IN

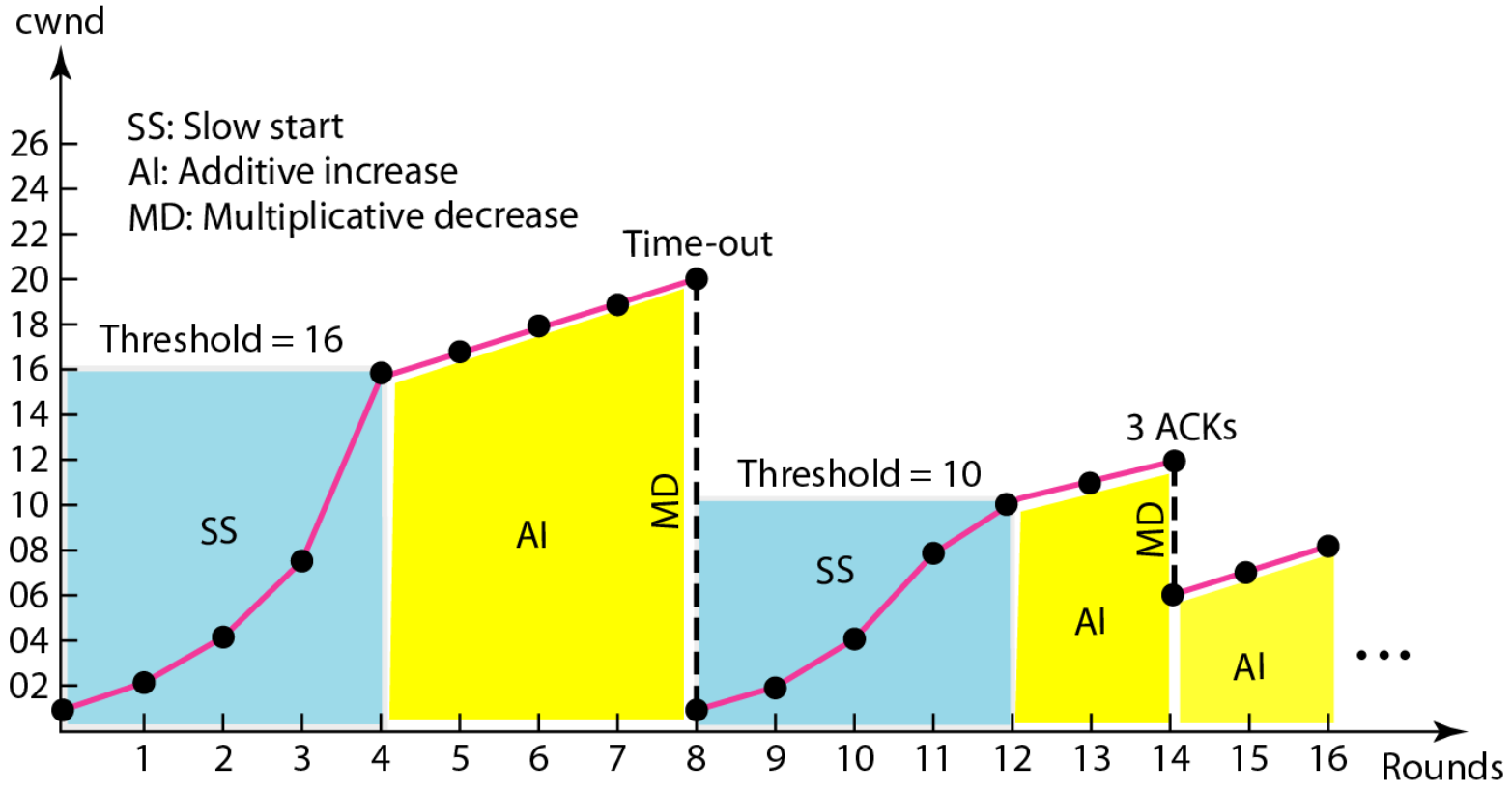
Congestion Detection: Multiplicative Decrease

- If congestion occurs, the congestion window size must be decreased.
- If the sender does not receive an acknowledgement for a segment before its retransmission timer has matured, it assumes that there is congestion.
- If a time-out occurs, the threshold must be set to one-half of the last congestion window size, and the congestion window size should start from 1 again. In other words, the sender returns to the slow start phase.
- Note that the threshold is reduced to one-half of the current congestion window size each time a time-out occurs. This means that the threshold is reduced exponentially (multiplicative decrease).

DOWNLOADED FROM KTUASSIST.IN

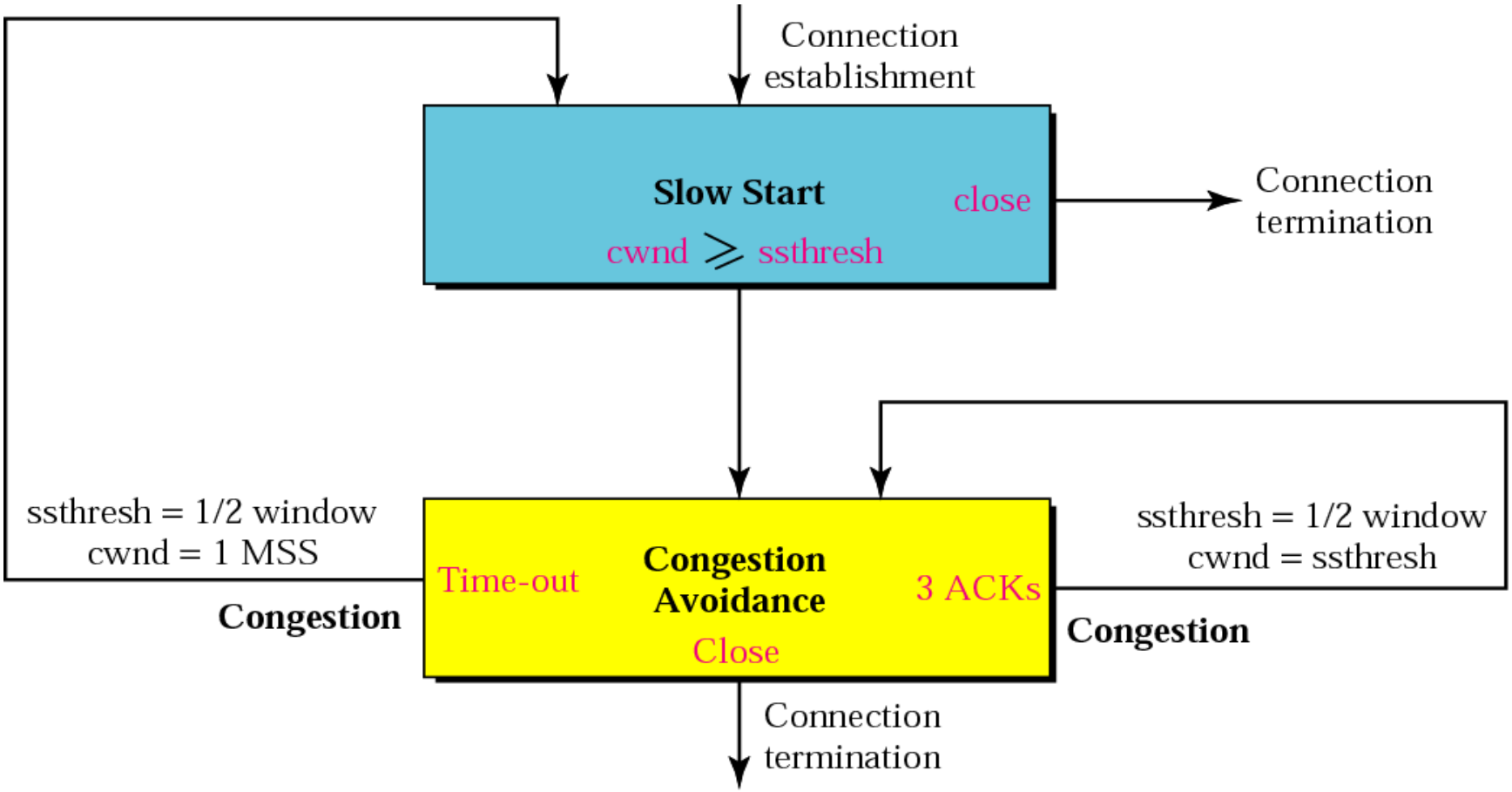
Congestion Detection: Multiplicative Decrease

- If detection is by time-out, a new slow start phase starts
- If detection is by three ACKs, a new congestion avoidance phase starts



DOWNLOADED FROM KTUASSIST.IN

Congestion Detection: Multiplicative Decrease



DOWNLOADED FROM KTUASSIST.IN

Quality of Service

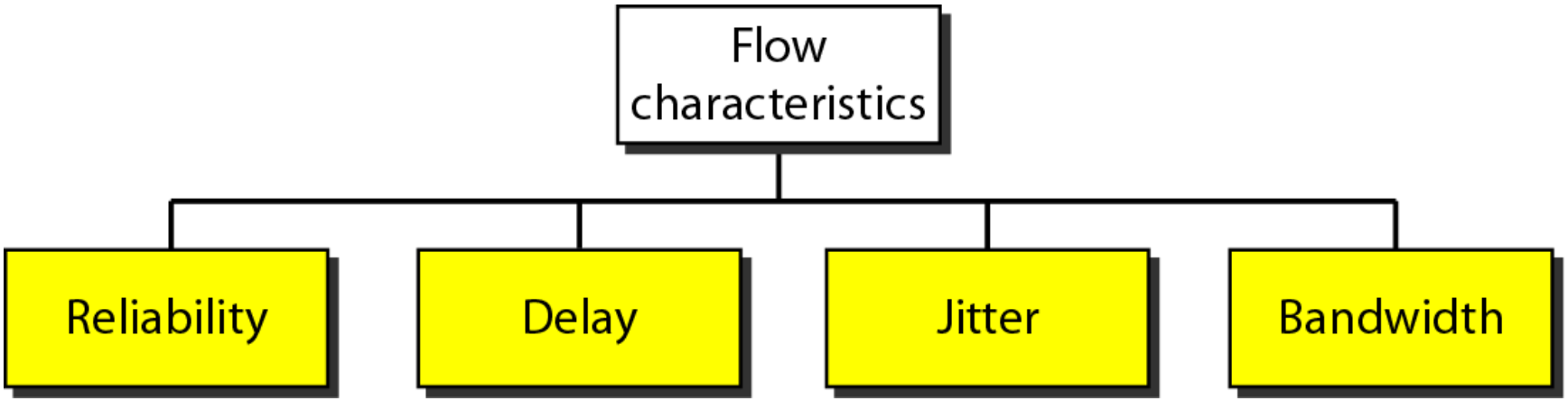
DOWNLOADED FROM KTUASSIST.IN

Quality of Service

- In Quality of Service, we try to create an appropriate environment for the traffic
- Basically traffic is the flow of data
- We will start by discussing some characteristics of the flow of data such as Reliability, Delay, Jitter and Bandwidth and then will discuss various techniques to improve the QoS

DOWNLOADED FROM KTUASSIST.IN

Flow Characteristics



DOWNLOADED FROM KTUASSIST.IN

Quality of Service

- Reliability: Lack of reliability means losing a packet or acknowledgement, which entails retransmission. Different application programs need different levels of reliability.
- Delay: Source-to-destination delay. Delay tolerance varies between applications.
- Jitter: Variation in delay for packets belonging to the same flow. Real-time audio and video applications cannot tolerate high jitter.
- Bandwidth: bits per second

DOWNLOADED FROM KTUASSIST.IN

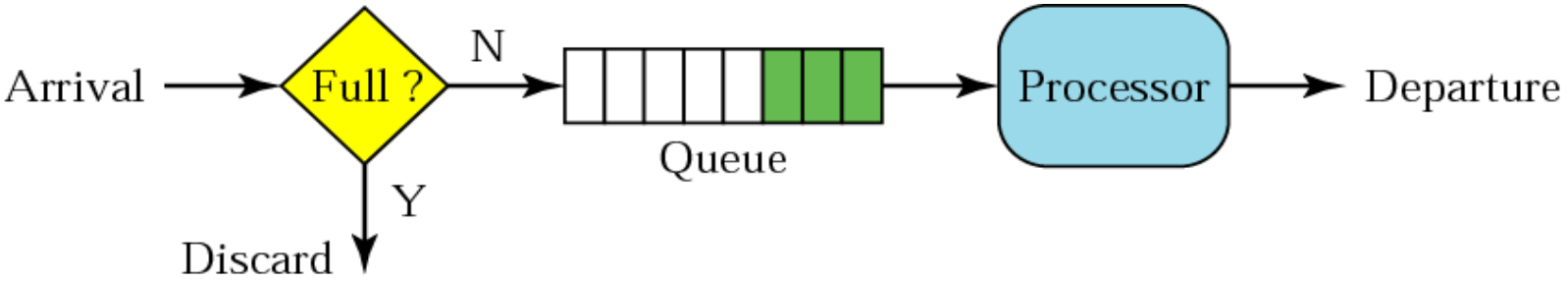
TECHNIQUES TO IMPROVE QoS

- Scheduling
  - FIFO Queuing
  - Priority Queuing
  - Weighted Fair Queuing
- Traffic Shaping
  - Leaky Bucket
  - Token Bucket
  - Combination of Leaky Bucket and Token Bucket.
- Resource Reservations
- Admission Control

DOWNLOADED FROM KTUASSIST.IN

Scheduling

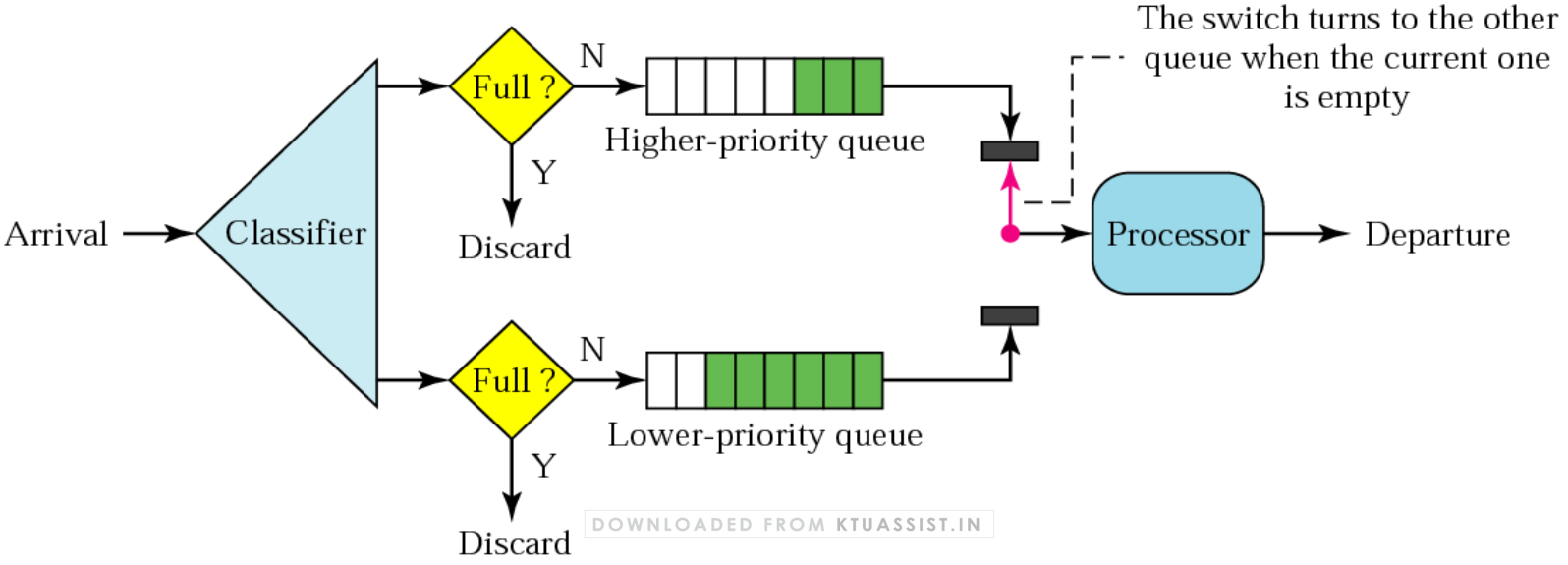
- The method of processing the flows. A good scheduling technique treats the different flows in a fair and appropriate manner.
- Three Types of Scheduling Algorithms
- FIFO Queuing:
  - First-in first-out queuing
  - Packets wait in a buffer (queue) until the node (router or switch) is ready to process them.
  - If average arrival rate is higher than average processing rate, the queue will fill up and new packets will be discarded.



DOWNLOADED FROM KTUASSIST.IN

Scheduling: Priority Queuing

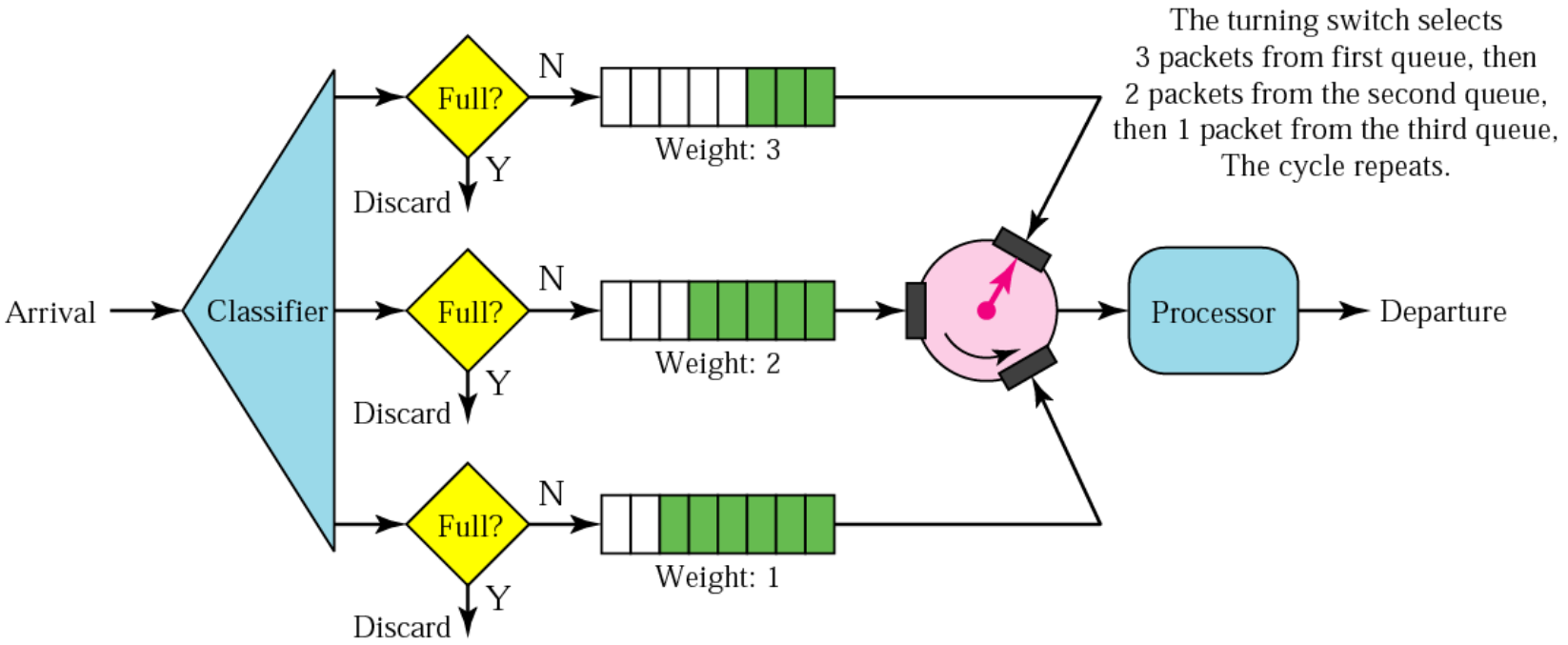
- Packets are first assigned to a priority class.
- Each priority class has its own queue.
- Packets in highest-priority queue are processed first. Packets in lowest-priority queue are processed last.
- System does not stop serving a queue until it is empty.
- Good for multimedia traffic.
- Starvation is possible: If there is a continuous flow in a high-priority queue, the packets in lower-priority queues will never have a chance to be processed.



DOWNLOADED FROM KTUASSIST.IN

Scheduling: Weighted Fair Queuing

- Packets are assigned to different classes and admitted to different queues.
- System processes packets in each queue in round-robin fashion with the number of packets selected from each queue based on the corresponding weight.



DOWNLOADED FROM KTUASSIST.IN

QoS: Traffic Shaping

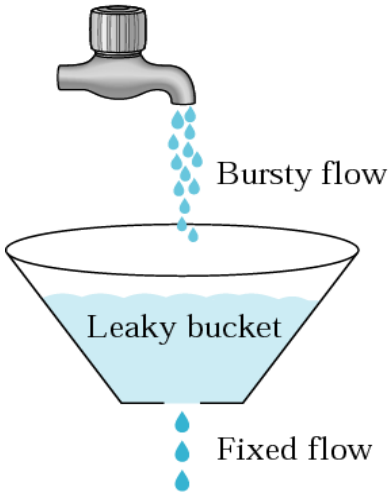
- Traffic shaping: Mechanism to control the amount and rate of the traffic sent to the network.

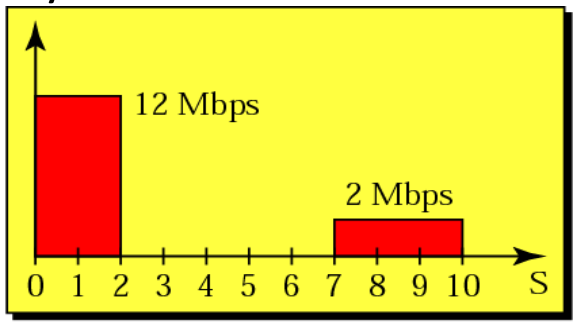
- Two Techniques for Traffic Shaping
  1. Leaky Bucket
  2. Token Bucket

DOWNLOADED FROM KTUASSIST.IN

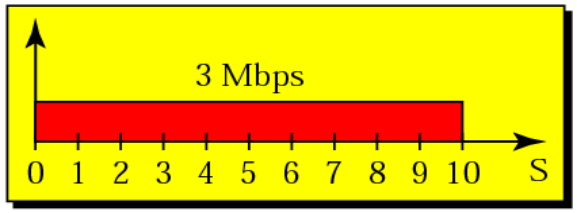
Traffic Shaping: Leaky Bucket

- Leaky bucket
  - Input rate varies; Output rate is fixed.
  - Using FIFO queue, if traffic consists of fixed-size packets, the process removes a fixed number of packets from the queue at each tick of the clock. If traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.





Bursty data

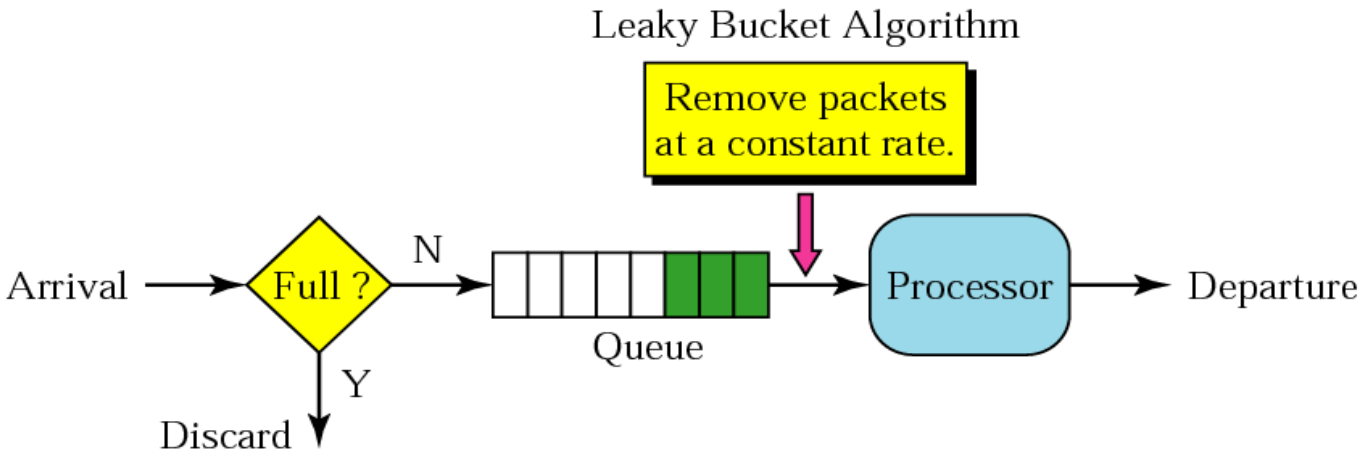


Fixed-rate data

DOWNLOADED FROM KTUASSIST.IN

Leaky Bucket Implementation

- LB algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if bucket is full.



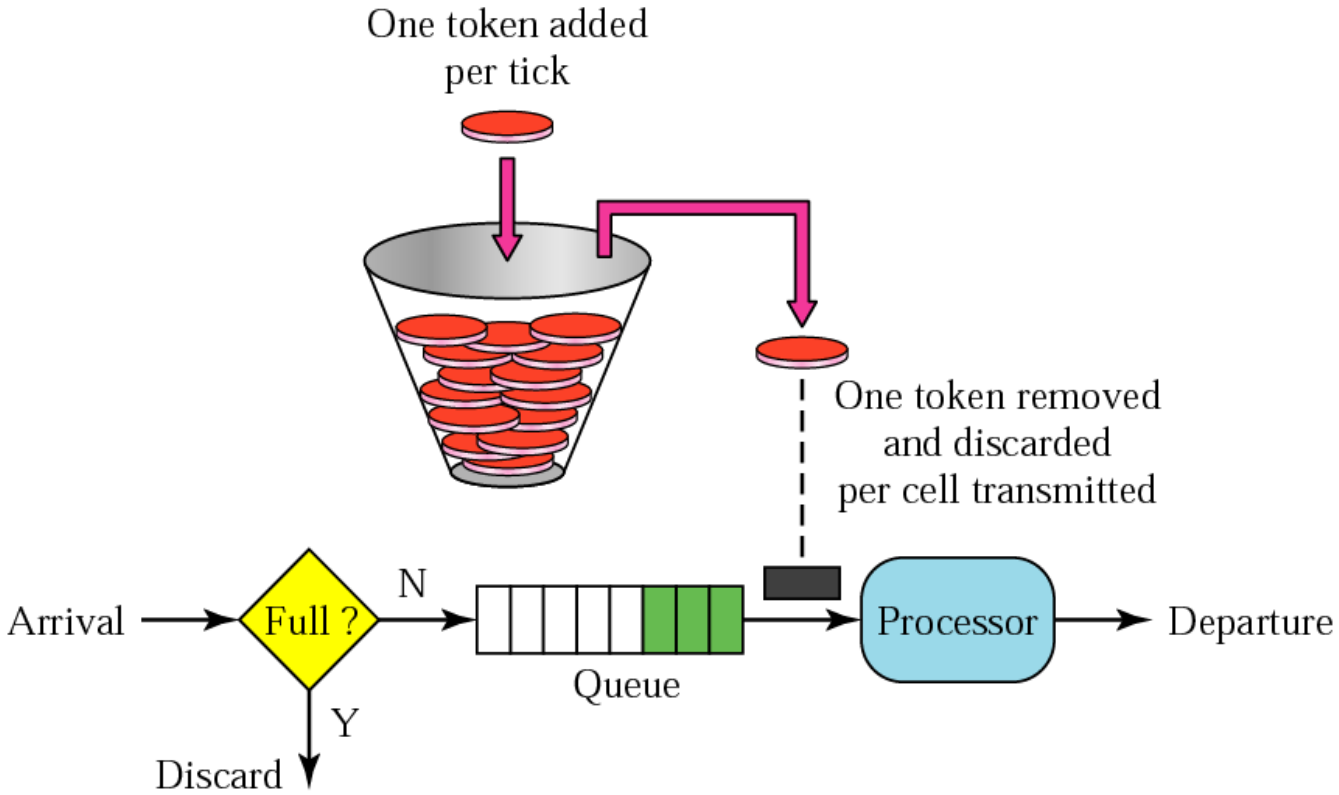
DOWNLOADED FROM KTUASSIST.IN

Traffic Shaping: Token Bucket

- Leaky bucket does not credit an idle host.
- If a host is not sending for a while, bucket becomes empty.
- The idle time of a host is not considered in leaky bucket.
- In token bucket, idle hosts accumulate credit for the future in the form of tokens.
- The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1.
- Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.

DOWNLOADED FROM KTUASSIST.IN

Traffic Shaping: Token Bucket



DOWNLOADED FROM KTUASSIST.IN

QoS: Resource Reservation

- Resource Reservation:
  - A Flow of data needs resources such as a buffer, bandwidth, CPU time, and so on.
  - The quality of service is improved if these resources are reserved beforehand.
- Admission Control:
  - It refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications.
  - Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.

DOWNLOADED FROM KTUASSIST.IN

Application Layer

DOWNLOADED FROM KTUASSIST.IN

Application Layer

- The application layer enables the user to access the network
- It provides user interfaces and support for services such as electronic mail, file access and transfer, access to system resources ,surfing the world wide web, and network management

DOWNLOADED FROM KTUASSIST.IN

DNS
(Domain Name System)

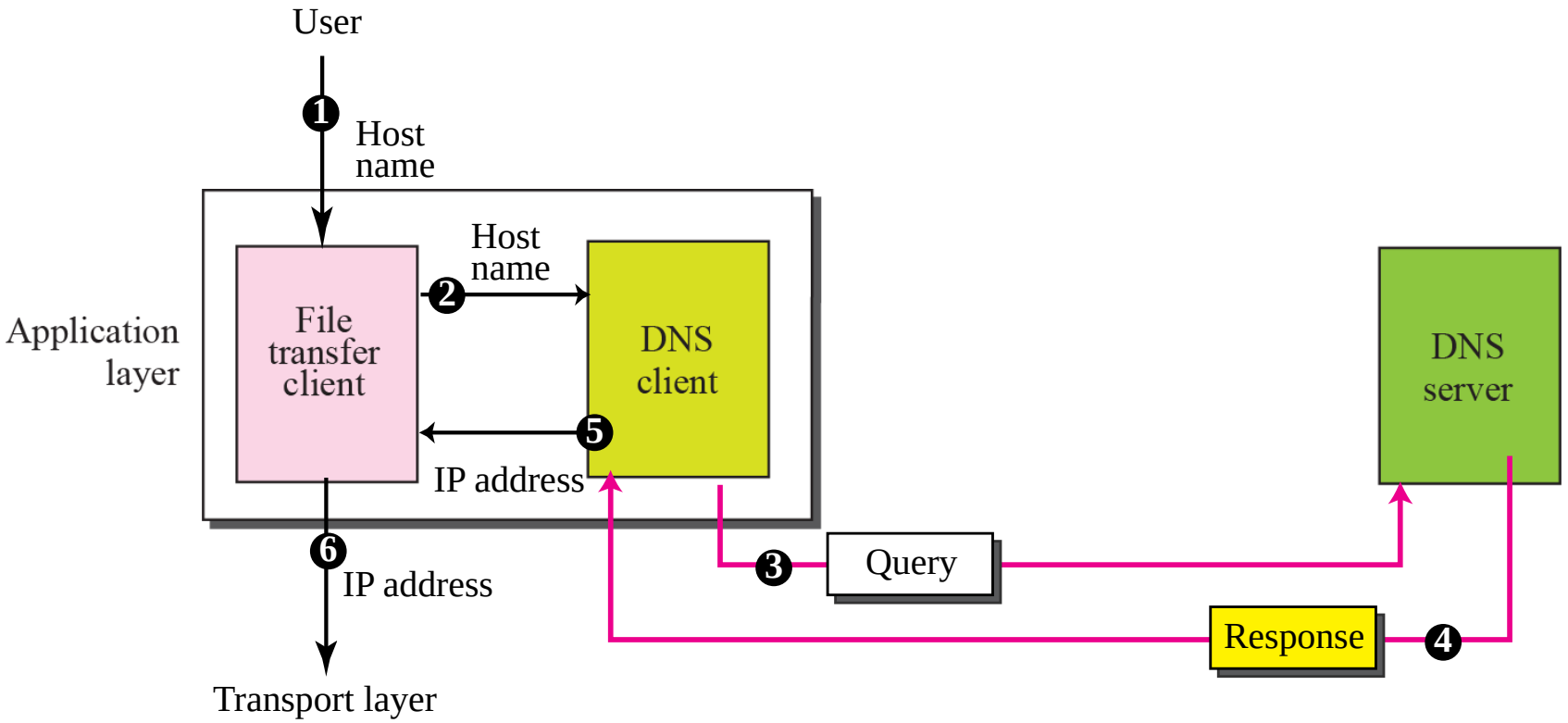
DOWNLOADED FROM KTUASSIST.IN

DNS

- Why DNS is Needed?
  - To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet.
  - However, people prefer to use names instead of numeric addresses.
  - Therefore, we need a system that can map a name to an address or an address to a name.

DOWNLOADED FROM KTUASSIST.IN

Working of DNS



DOWNLOADED FROM KTUASSIST.IN

NAME SPACE

- To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- In other words, the names must be unique because the addresses are unique.
- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

DOWNLOADED FROM KTUASSIST.IN

Flat Name Space

- In this, a name is assigned to an address.
- A Name in this space is a sequence of characters without structure
- The main disadvantage of a flat name space is that it cannot be used in a large system such as Internet because it must be centrally controlled to avoid ambiguity and duplication

DOWNLOADED FROM KTUASSIST.IN

Hierarchical Name Space

- In this, each name is made of several parts.
- The first part can define the nature of the organization…the second part can define the name of an organization…and the third part can define departments in the organization.
- A central authority can assign the part of the name that defines the nature of the organization and the name of the organization
- The responsibility of the rest of the name can be given to the organization

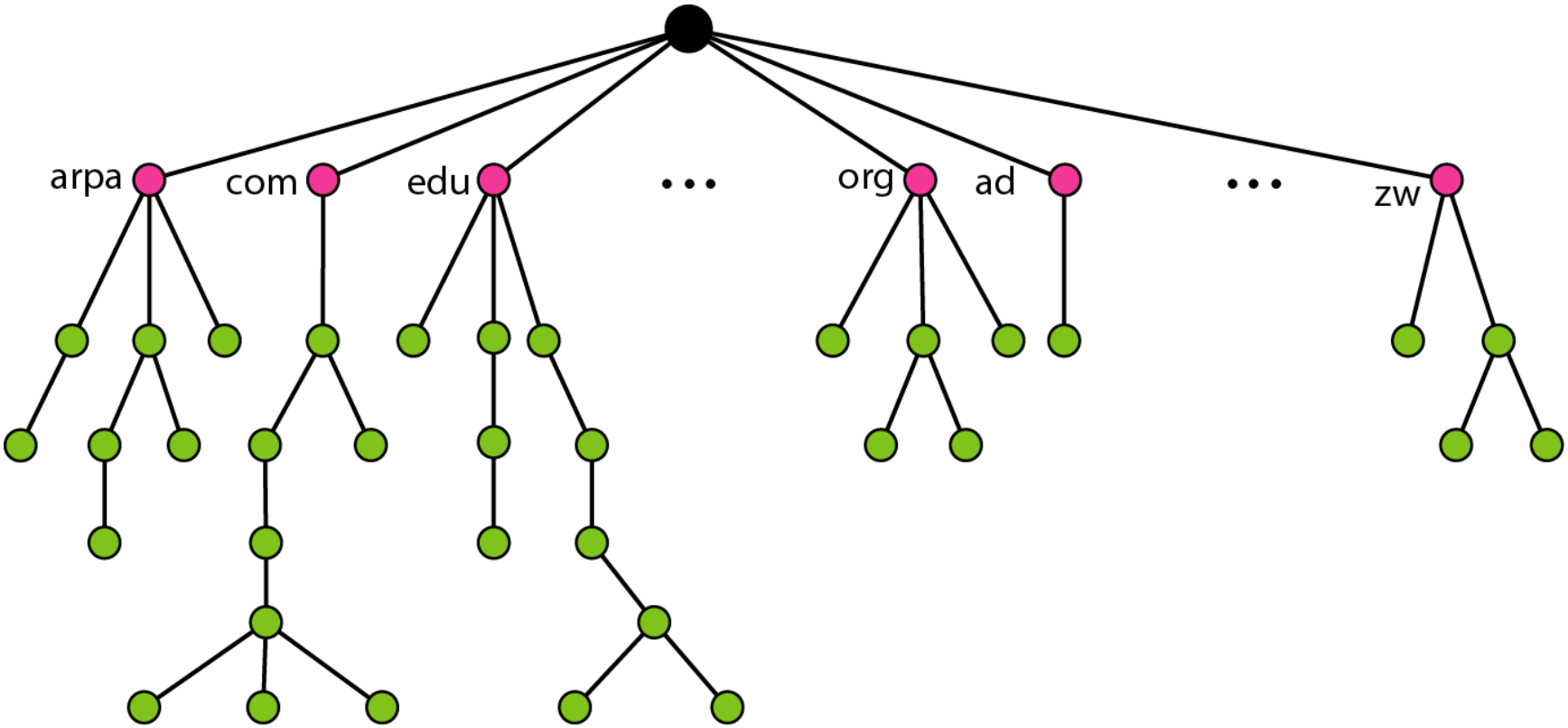
DOWNLOADED FROM KTUASSIST.IN

DOMAIN NAME SPACE

- It is designed to have a hierarchical name space.
- In this design the names are defined in an inverted-tree structure with the root at the top.
- The tree can have only 128 levels: level 0 (root) to level 127.
  - Label: Each node in a tree has a label, which is a string(63 characters maximum)
  - Root Label: NULL or empty string.DNS requires that children of a node have different labels to ensure uniqueness of domain names
  - Domain Name: A full domain name is a sequence of labels separated by dots(.)Domain names are always read from the node up to to the root

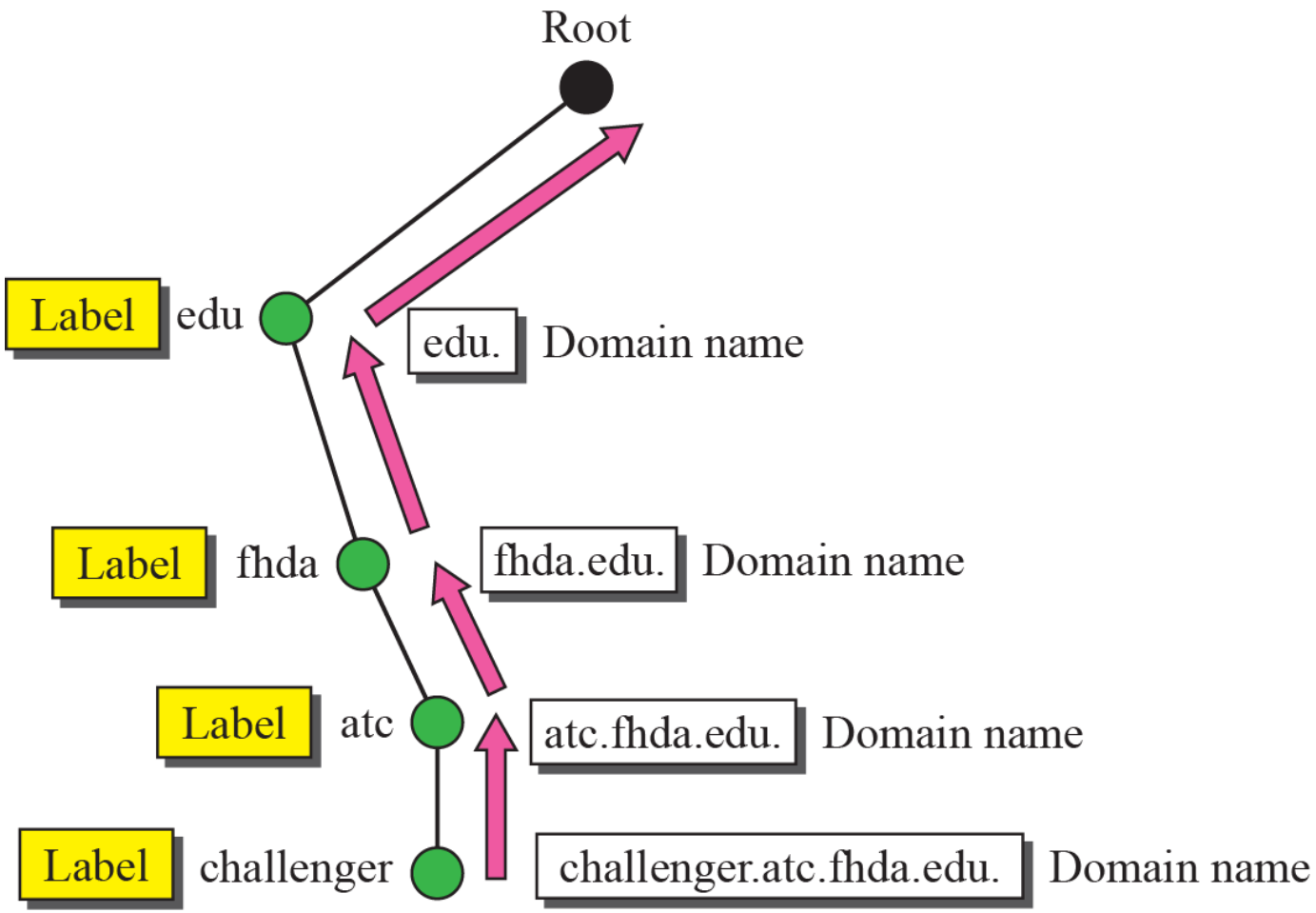
DOWNLOADED FROM KTUASSIST.IN

DOMAIN NAME SPACE



DOWNLOADED FROM KTUASSIST.IN

Domain names and labels



DOWNLOADED FROM KTUASSIST.IN

FQDN & PQDN

FQDN

- Fully Qualified Domain Name
- In this a label is terminated by NULL string
- FQDN: Domain name that contains full name of a host
- Eg: challenger.atc.fhda.edu

PQDN

- Partially Qualified Domain Name
- In this a label is not terminated by NULL string
- PQDN: Starts from Node,but doesn't reach root
- Eg: challenger.atc.fhda.edu

FQDN

challenger.atc.fhda.edu.
cs.hmme.com.
www.funny.int.

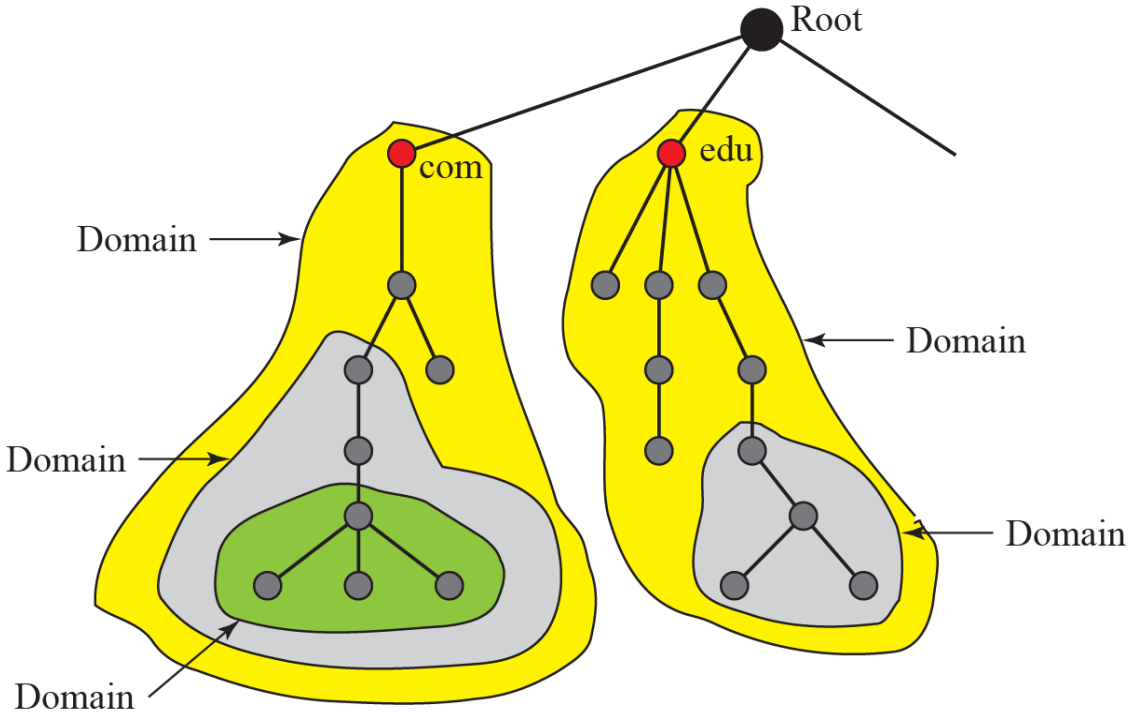
PQDN

challenger.atc.fhda.edu
cs.hmme
www

DOWNLOADED FROM KTUASSIST.IN

Domain

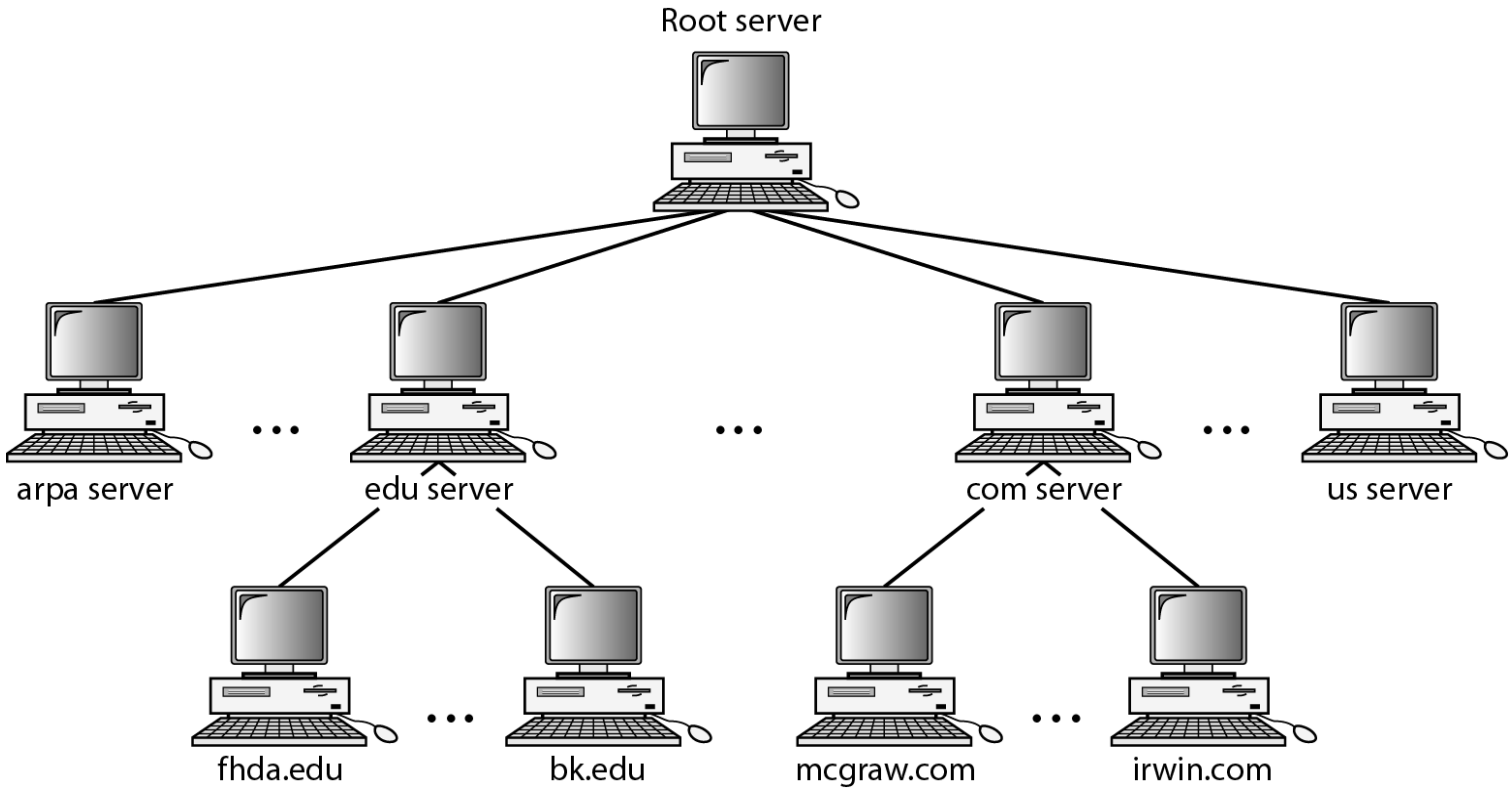
- A domain is a subtree of the domain space.
- The name of the domain is the name of the node at the top of the subtree.
- Note that a domain may itself be divided into domains(subdomains)



DOWNLOADED FROM KTUASSIST.IN

DISTRIBUTION OF NAME SPACE

- The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information.

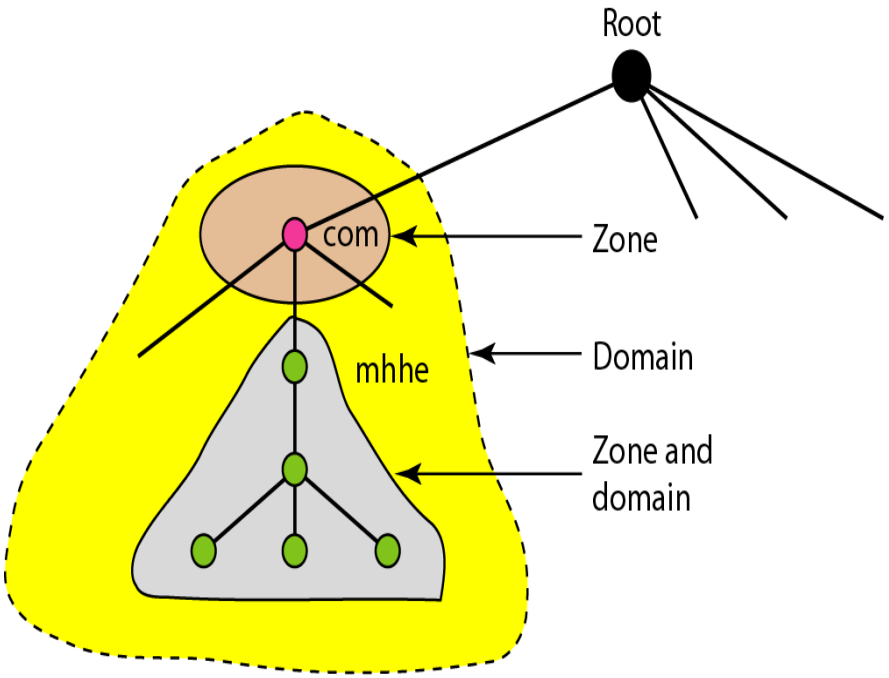


DOWNLOADED FROM KTUASSIST.IN

Hierarchy of Name Servers

Zone

- Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers.
- What a server is responsible for or has authority over is called a zone.
- The server makes a database called a zone file and keeps all the information for every node under that domain.



DOWNLOADED FROM KTUASSIST.IN

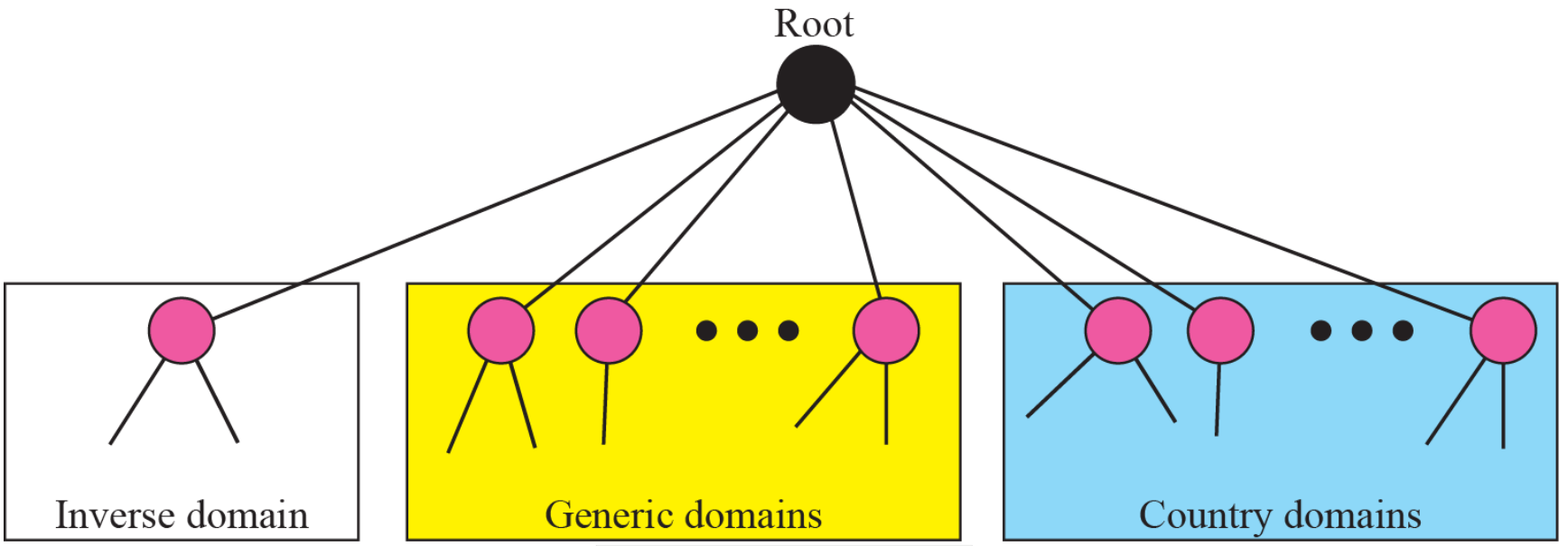
Primary Server and Secondary Server

- A primary server is a server that stores a file about the zone for which it is an authority.
- It is responsible for creating, maintaining, and updating the zone file.
- A primary server loads all information from the disk file; the secondary server loads all information from the primary server.
- When the secondary downloads information from the primary, it is called zone transfer.

DOWNLOADED FROM KTUASSIST.IN

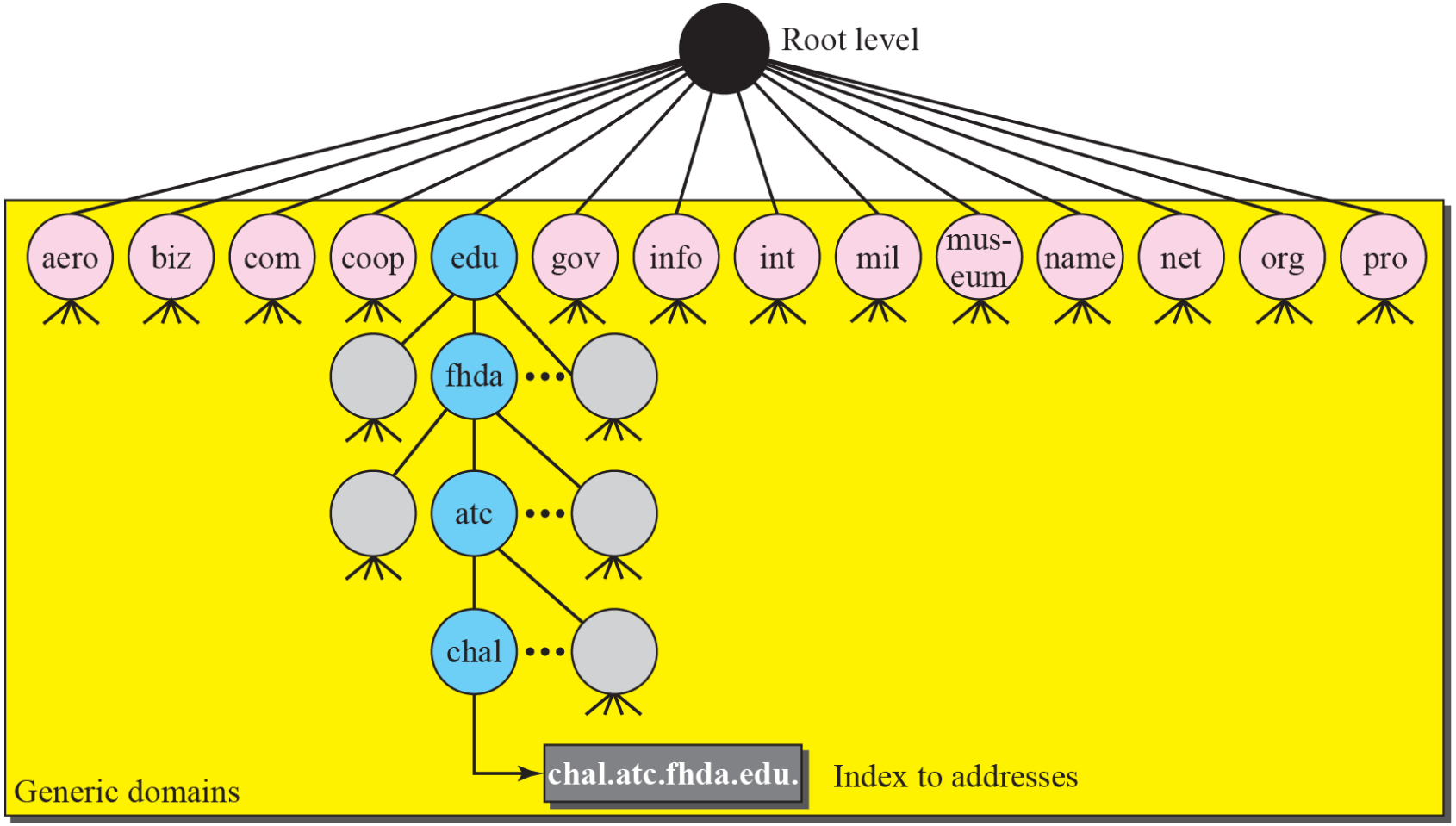
DNS IN THE INTERNET

- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain



DOWNLOADED FROM KTUASSIST.IN

DNS IN THE INTERNET



DOWNLOADED FROM KTUASSIST.IN

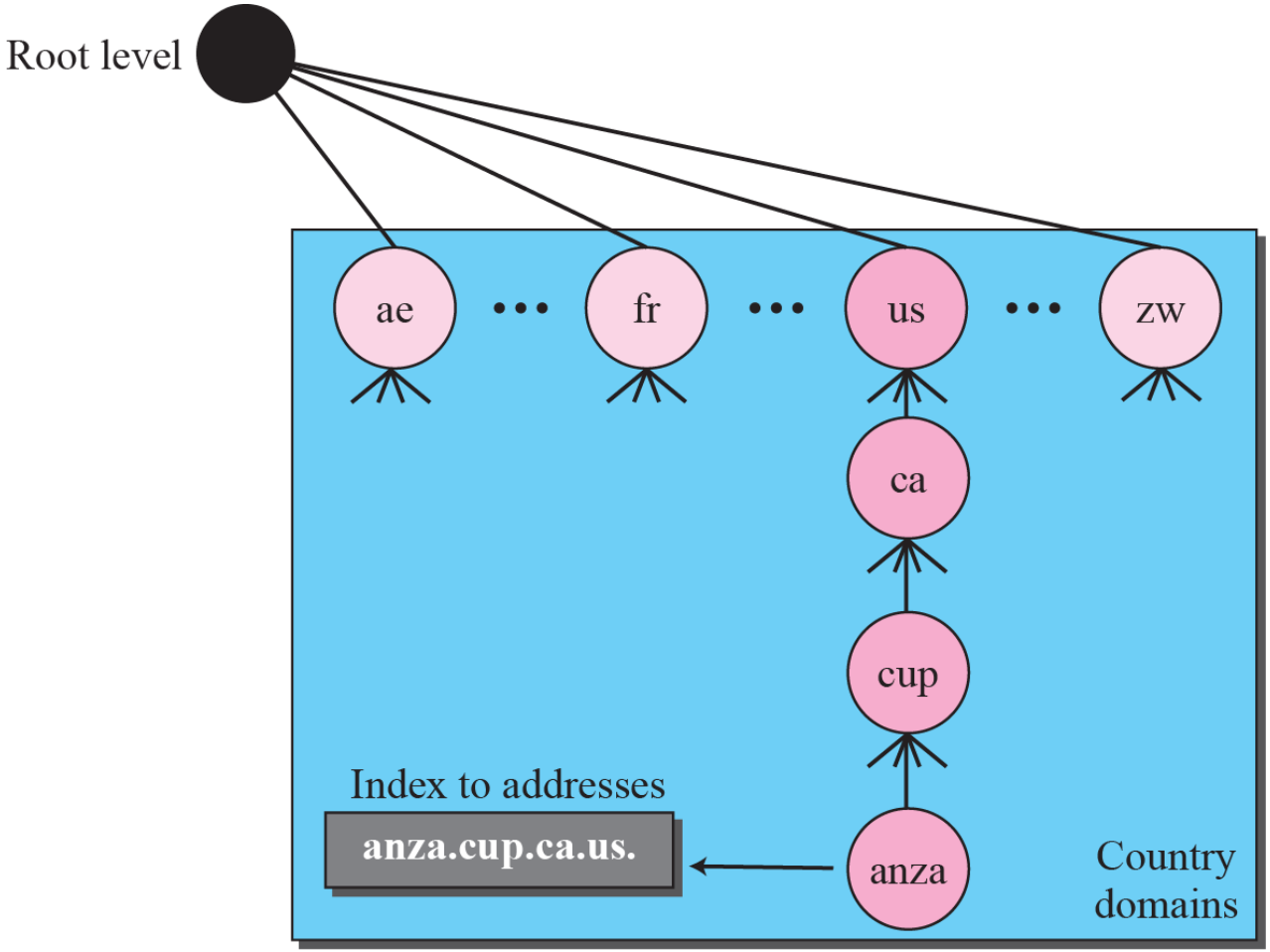
DNS IN THE INTERNET

Table 19.1 *Generic domain labels*

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

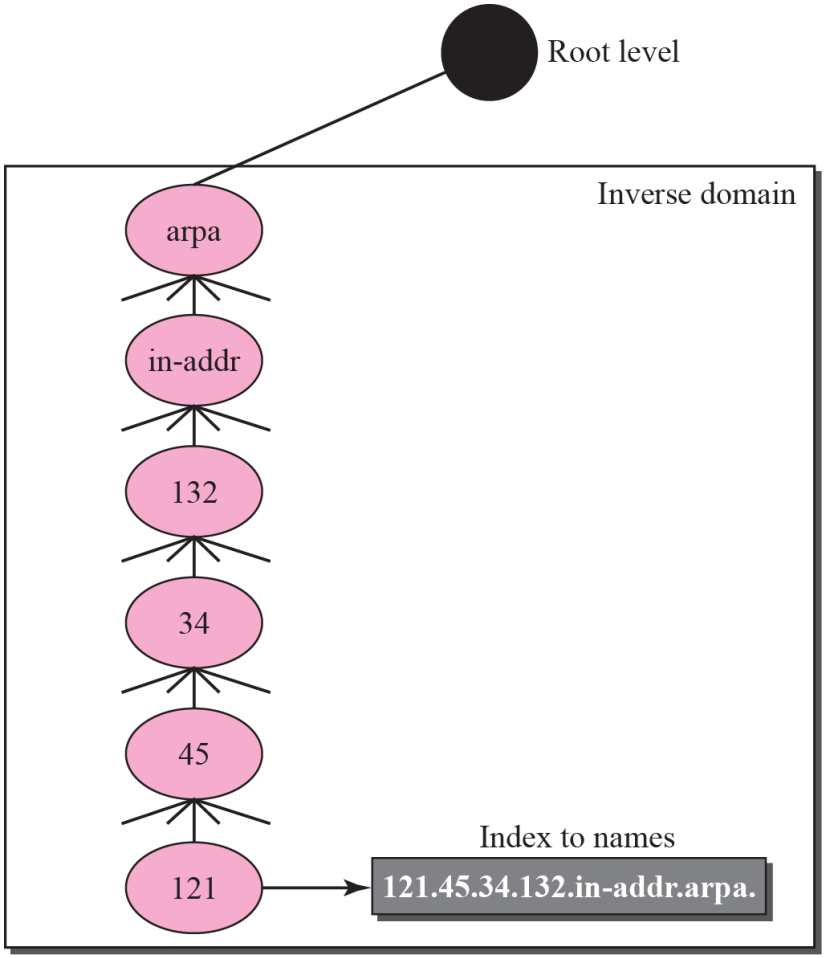
DOWNLOADED FROM KTUASSIST.IN

Country Domains



DOWNLOADED FROM KTUASSIST.IN

Inverse Domain



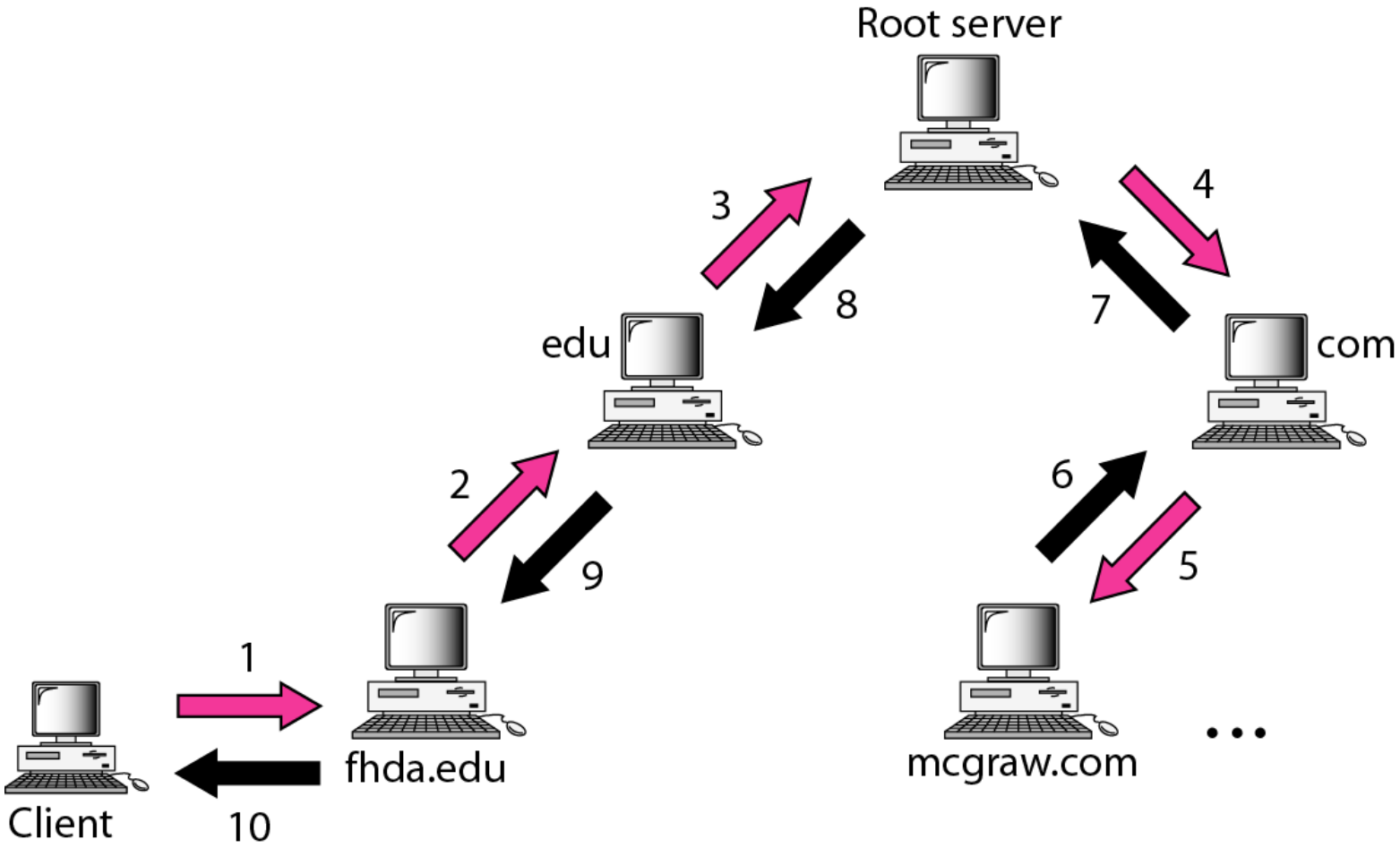
DOWNLOADED FROM KTUASSIST.IN

RESOLUTION

- Mapping a name to an address or an address to a name is called name-address resolution.

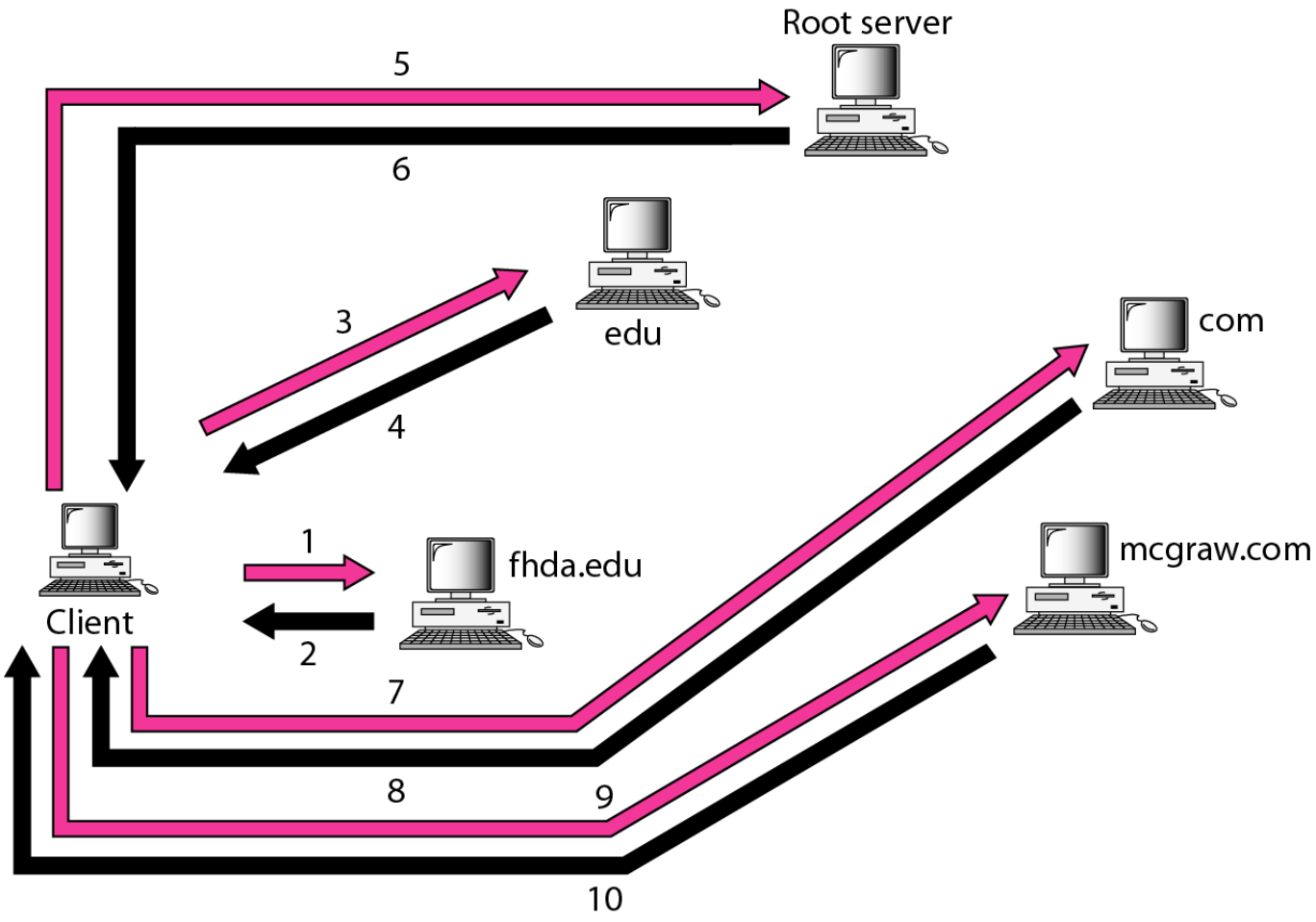
DOWNLOADED FROM KTUASSIST.IN

Recursive Resolution



DOWNLOADED FROM KTUASSIST.IN

Iterative Resolution



DOWNLOADED FROM KTUASSIST.IN

Module 6

Introduction to information system security, common attacks

Security at Application Layer (E-MAIL, PGP and S/MIME).

Security at Transport Layer (SSL and TLS).

Security at Network Layer (IPSec).

Defence and counter measures: Firewalls and their types. DMZ, Limitations of firewalls, Intrusion Detection Systems -Host based, Network based, and Hybrid IDSs

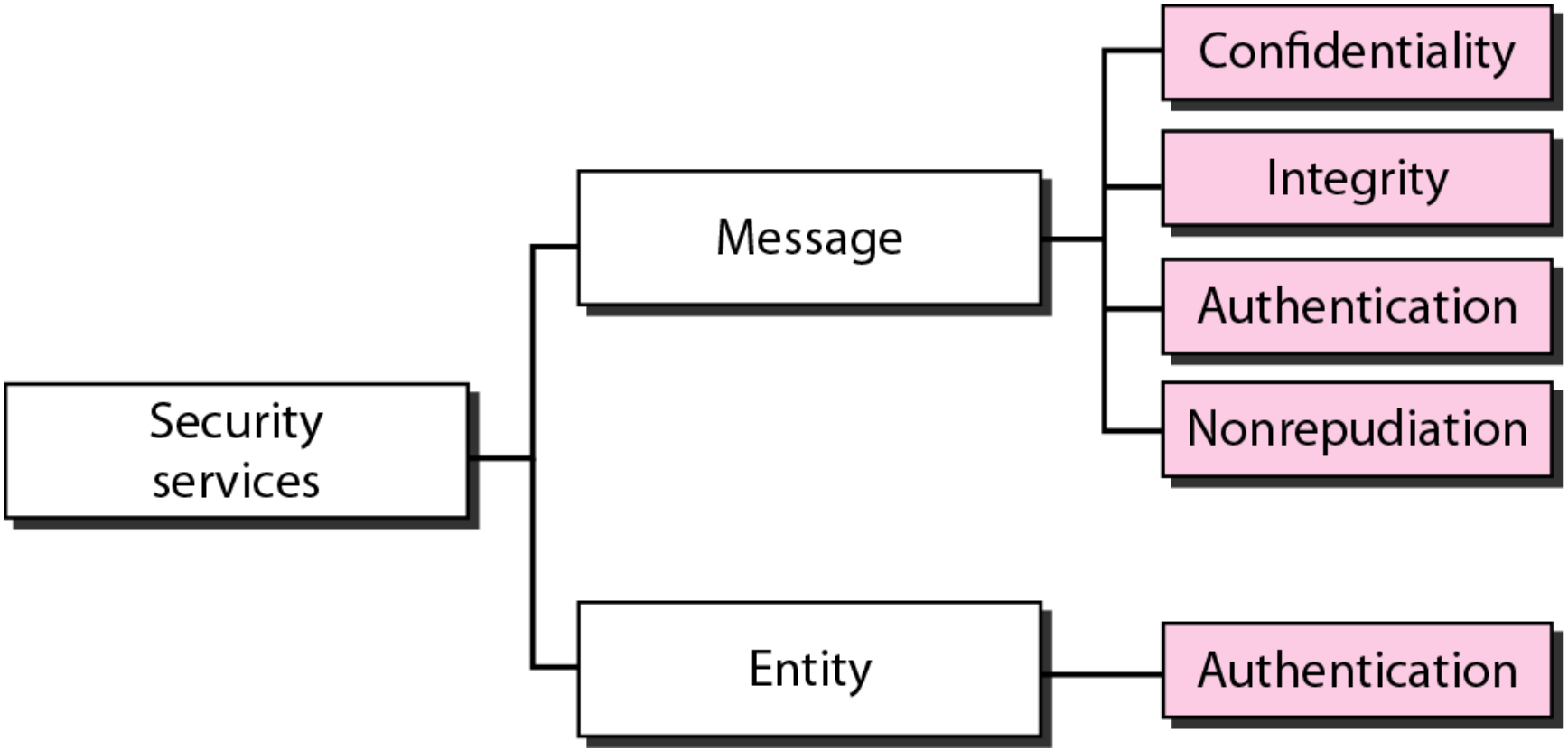
DOWNLOADED FROM KTUASSIST.IN

SECURITY SERVICES

- Network security can provide five services.
  - Four of these services are related to the message exchanged using the network.
  - The fifth service provides entity authentication or identification.

DOWNLOADED FROM KTUASSIST.IN

SECURITY SERVICES



DOWNLOADED FROM KTUASSIST.IN

MESSAGE CONFIDENTIALITY

- Message confidentiality or privacy means hiding information from unauthorized access.
- The transmitted message must make sense to only the intended receiver.

DOWNLOADED FROM KTUASSIST.IN

MESSAGE INTEGRITY

- preventing information from unauthorized modification
- Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission.

DOWNLOADED FROM KTUASSIST.IN

MESSAGE AUTHENTICATION

- In message authentication the receiver needs to be sure of the senders identity and that an imposter has not sent the message.

DOWNLOADED FROM KTUASSIST.IN

MESSAGE NONREPUDIATION

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact did send.
- For example when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION

- In entity authentication the entity or user is verified prior to access to the system resources.
- For example ,a student who needs to access her college resources needs to be authenticated during the logging process.

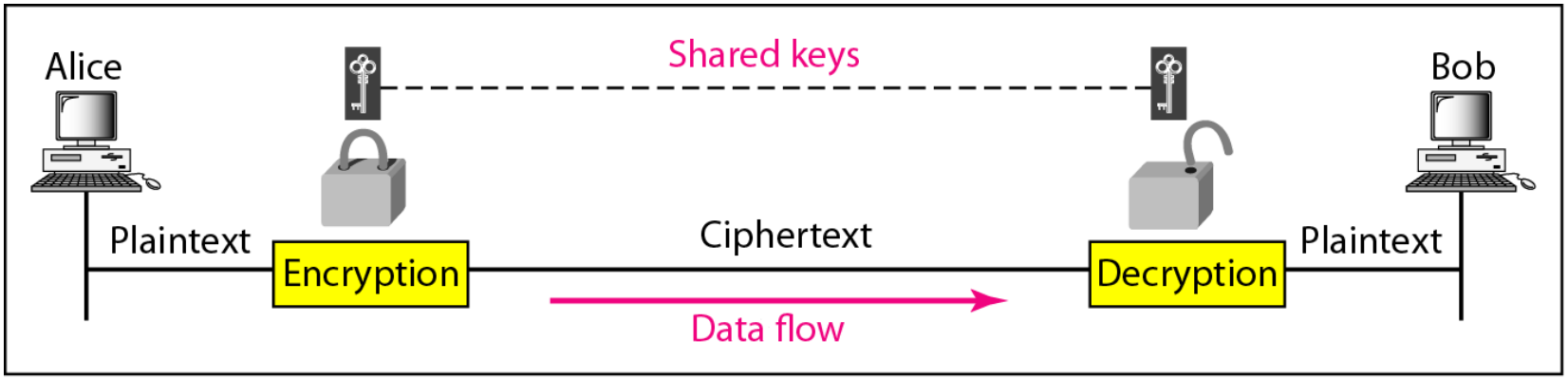
DOWNLOADED FROM KTUASSIST.IN

MESSAGE CONFIDENTIALITY

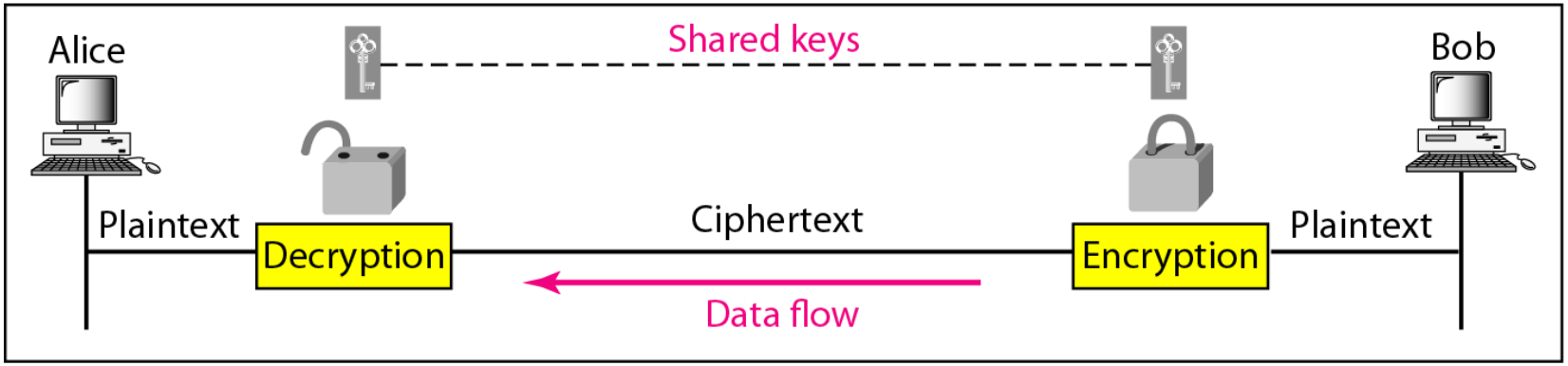
- To achieve message confidentiality or privacy, the message must be encrypted at the sender site and decrypted at the receiver site.
- Two types of Cryptographic techniques are
  - Symmetric-key cryptography
  - Asymmetric-key cryptography.

DOWNLOADED FROM KTUASSIST.IN

Confidentiality with Symmetric-Key Cryptography



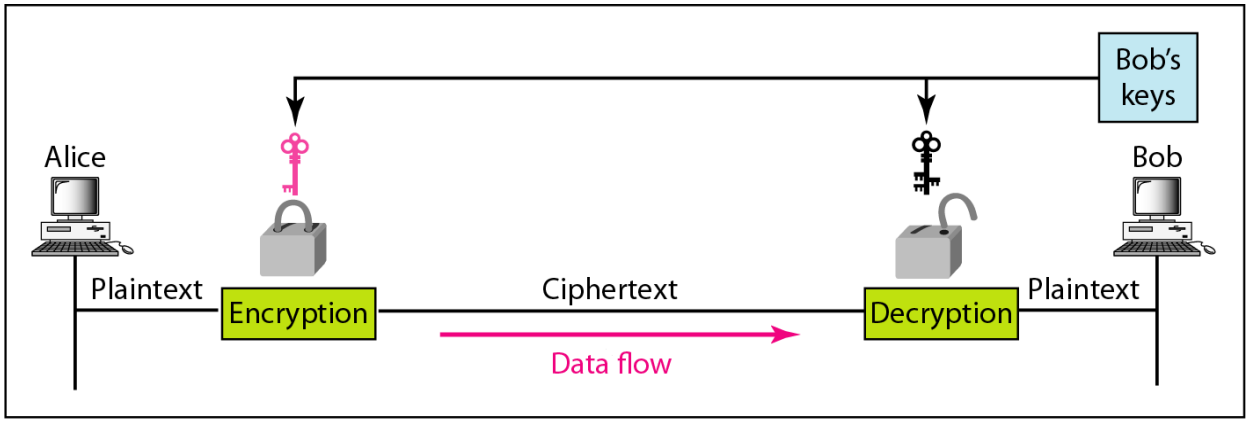
a. A shared secret key can be used in Alice-Bob communication



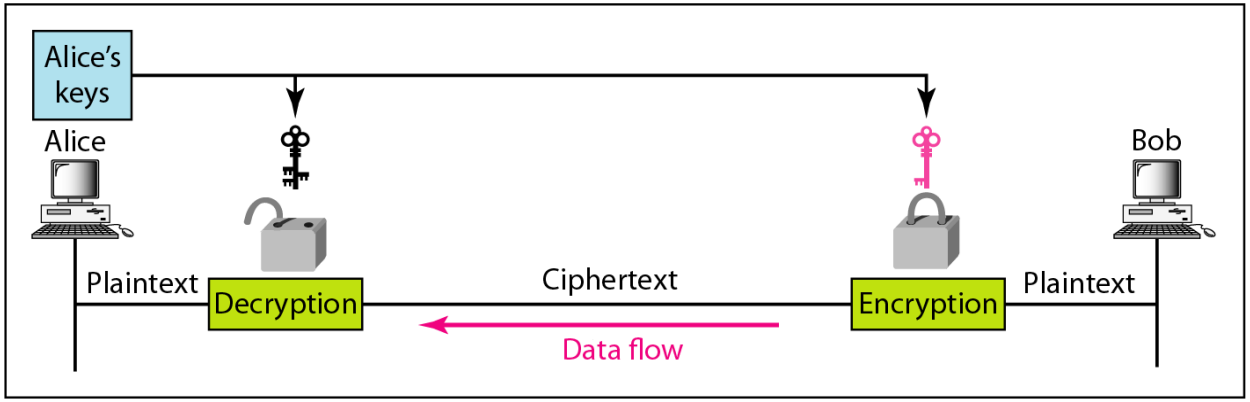
b. A different shared secret key is recommended in Bob-Alice communication

DOWNLOADED FROM KTUASSIST.IN

Confidentiality with Asymmetric-Key Cryptography



a. Bob's keys are used in Alice-Bob communication



b. Alice's keys are used in Bob-Alice communication

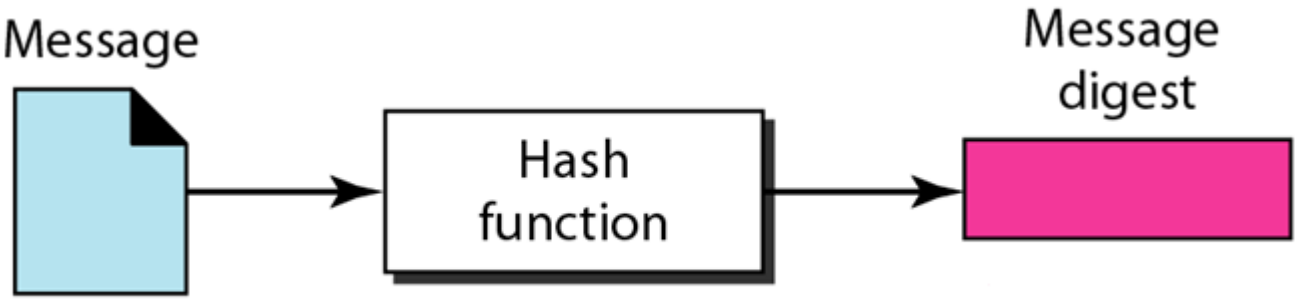
DOWNLOADED FROM KTUASSIST.IN

MESSAGE INTEGRITY

- Encryption and decryption provide secrecy, or confidentiality, but not integrity. However, on occasion we may not even need secrecy, but instead must have integrity.

DOWNLOADED FROM KTUASSIST.IN

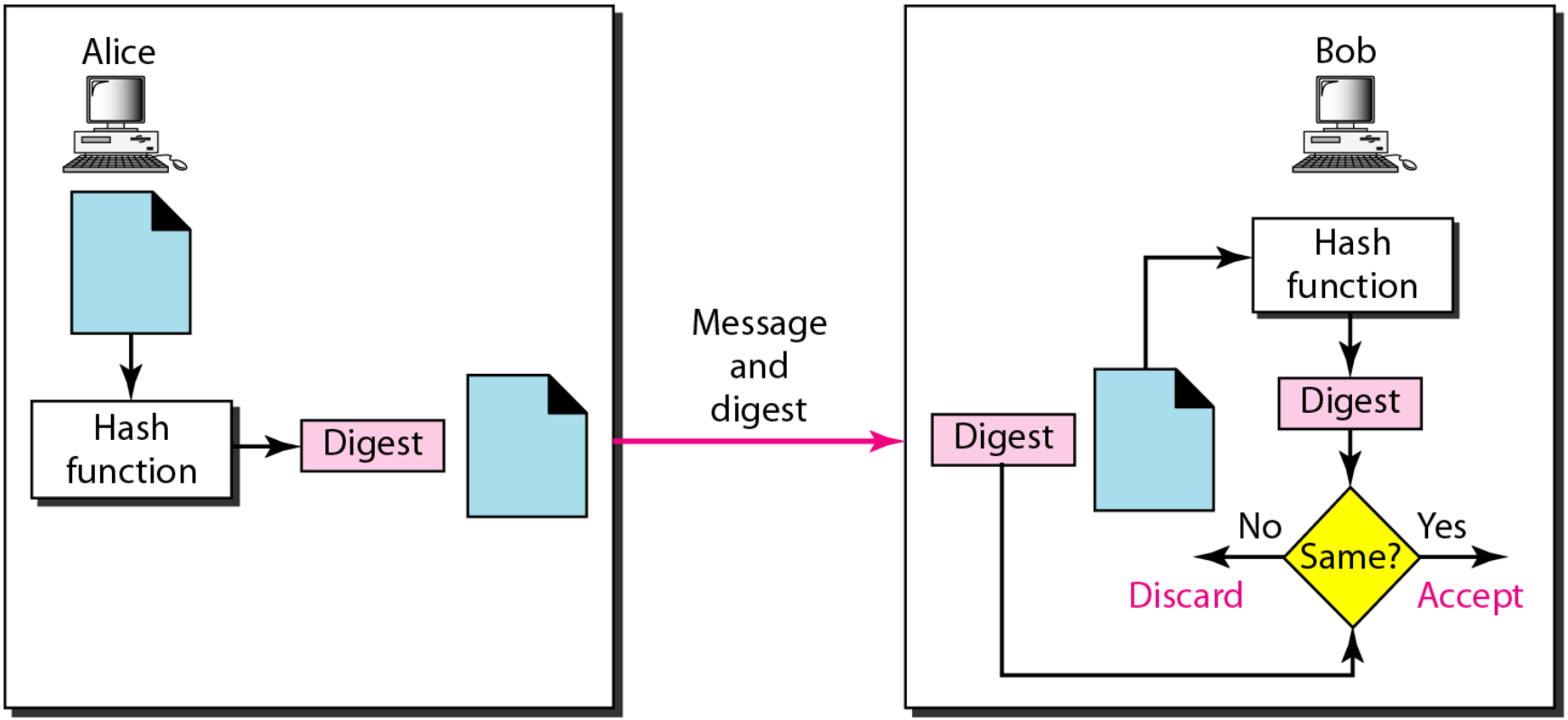
MESSAGE INTEGRITY



The message digest needs to be kept secret.

DOWNLOADED FROM KTUASSIST.IN

MESSAGE INTEGRITY - checking



DOWNLOADED FROM KTUASSIST.IN

Criteria of a Hash Function

- Collision Resistance
  - It ensures that we cannot find two messages that hash to the same digest
- One-wayness
  - Means that we must not be able to recreate the message from the digest

SHA-1 hash algorithms create an N-bit message digest out of a message of 512-bit blocks.
SHA-1 has a message digest of 160 bits (5 words of 32 bits).

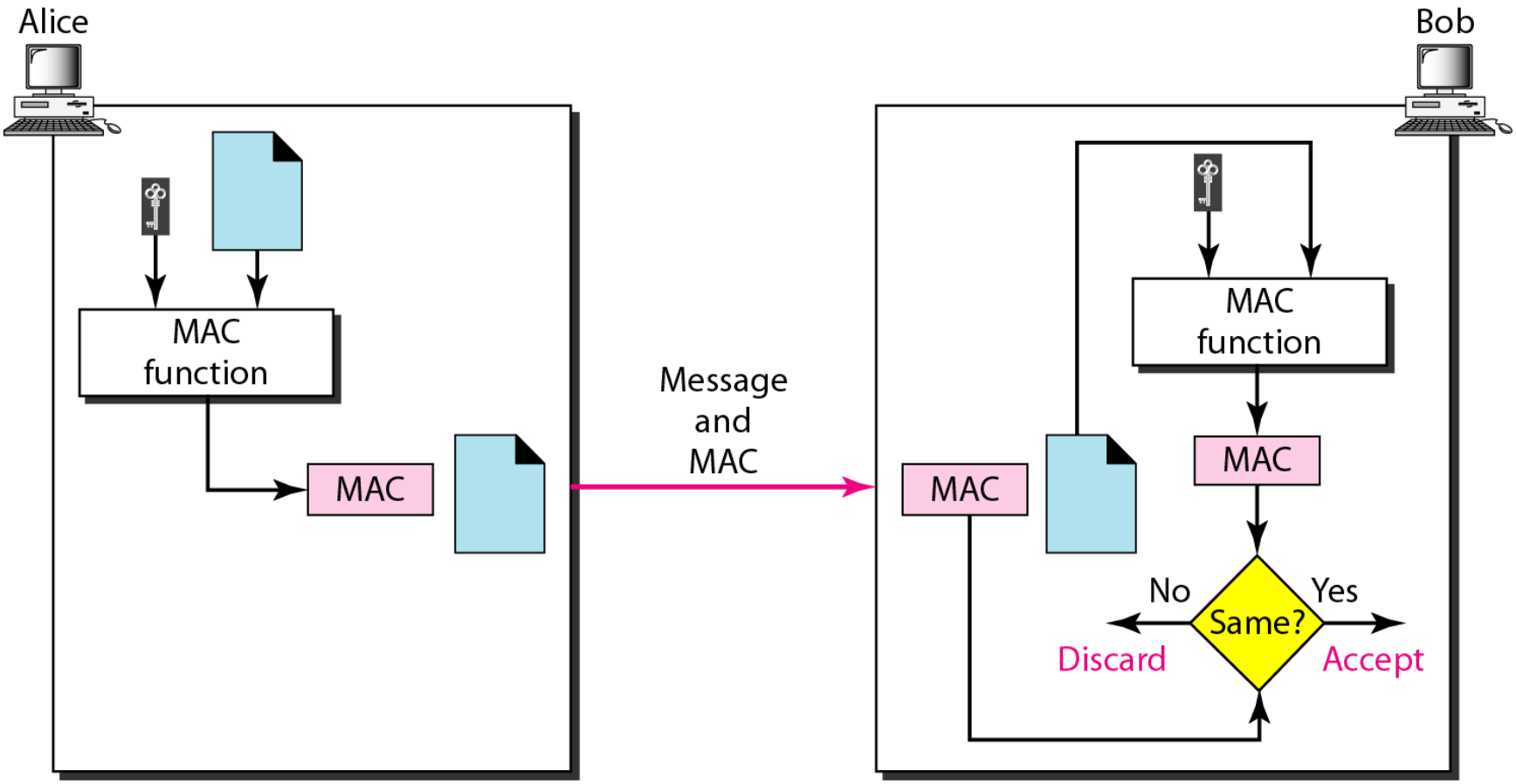
DOWNLOADED FROM KTUASSIST.IN

MESSAGE AUTHENTICATION

- A hash function per se cannot provide authentication. The digest created by a hash function can detect any modification in the message, but not authentication.
- Two approaches
  - Message Authentication Code(MAC) created using symmetric keyed hash function(MAC function)
  - Digital Signature

DOWNLOADED FROM KTUASSIST.IN

MAC



DOWNLOADED FROM KTUASSIST.IN

DIGITAL SIGNATURE

- When Alice sends a message to Bob, Bob needs to check the authenticity of the sender; he needs to be sure that the message comes from Alice and not Eve.
- Bob can ask Alice to sign the message electronically. In other words, an electronic signature can prove the authenticity of Alice as the sender of the message.
- We refer to this type of signature as a digital signature.

DOWNLOADED FROM KTUASSIST.IN

DIGITAL SIGNATURE

- Digital signature is a type of method for authenticating digital information analogous to ordinary physical signatures on paper.
- Implemented using public-key cryptography.
- Private Key – Used for making Digital Signature.
- Public Key – Used to verify the Digital Signature

DOWNLOADED FROM KTUASSIST.IN

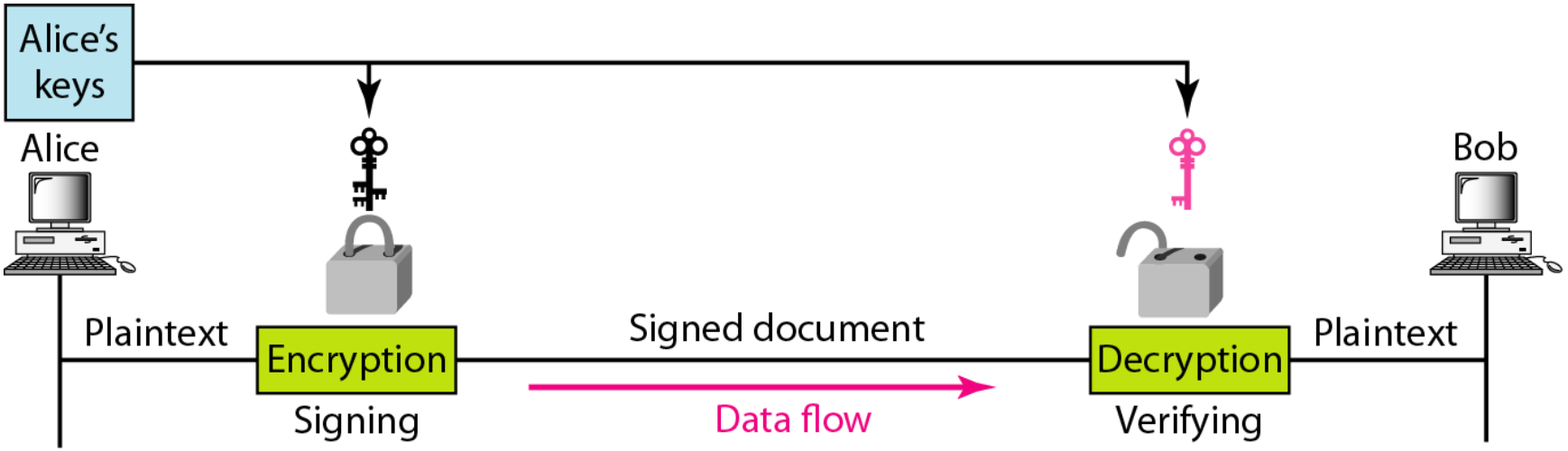
Two Choices

1. Signing the whole document/message.

2. Signing the digest (miniature version of document).

DOWNLOADED FROM KTUASSIST.IN

Signing the message itself in digital signature



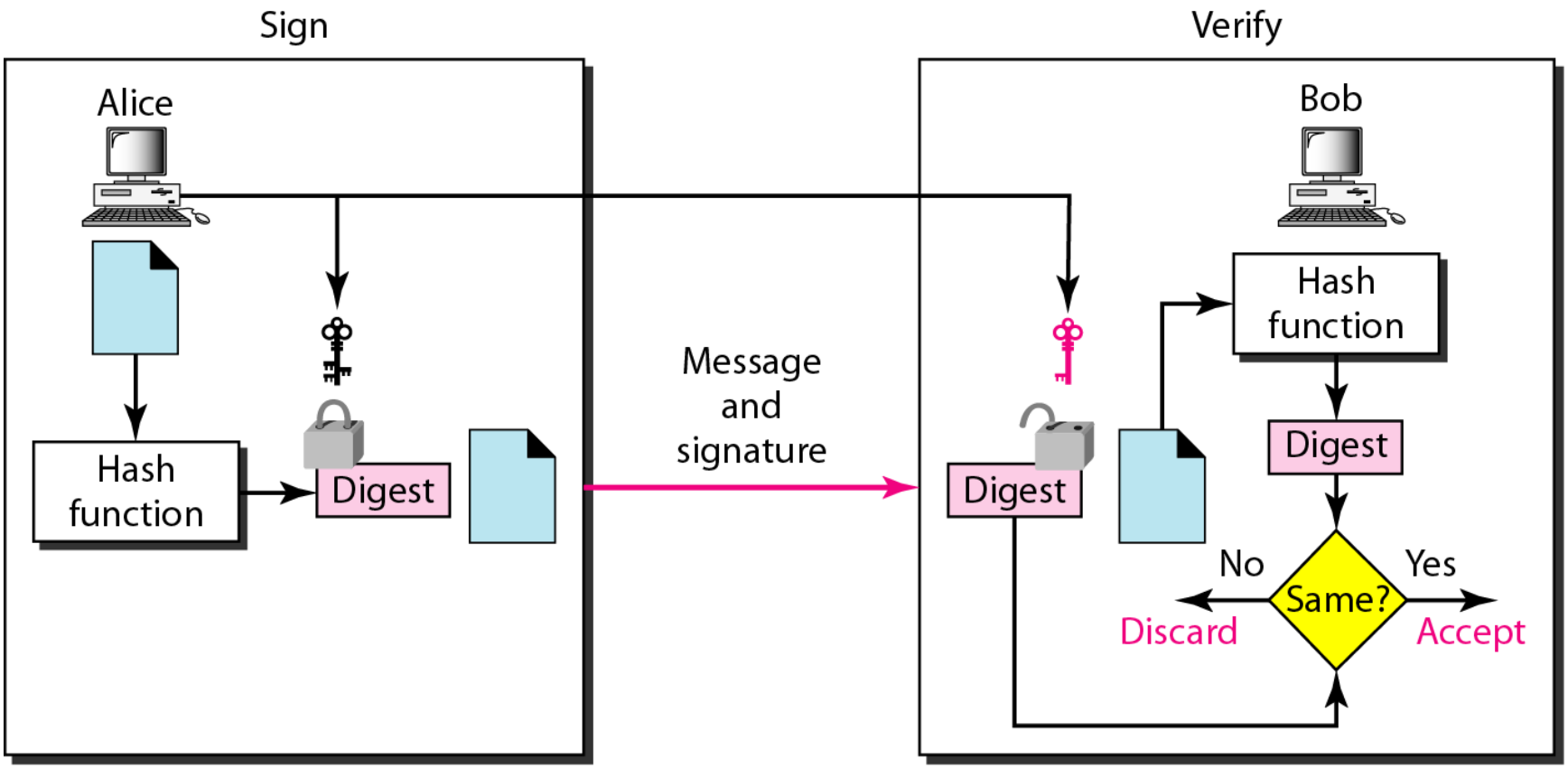
DOWNLOADED FROM KTUASSIST.IN

Signing the message itself in digital signature

- Public key encryption can be used to sign a document.
- The sender uses her private key to encrypt(sign)the message just as a person uses her signature to sign a paper document.
- The receiver on the other hand uses the public key of the sender to decrypt the message just as a person verifies

DOWNLOADED FROM KTUASSIST.IN

Signing the digest in a digital signature



DOWNLOADED FROM KTUASSIST.IN

Signing the digest in a digital signature

- Public key encryption is efficient if the message is short.
- Using a public key to sign the entire message is very inefficient if the message is very long.
- The solution is to let the sender sign a digest of the document instead of the whole document.
- The sender creates a miniature version of the document and sign it the receiver then checks the signature on the miniature

DOWNLOADED FROM KTUASSIST.IN

Signing the digest in a digital signature

- After the digest has been created it is encrypted using the senders private key.
- The encrypted digest is attached to the original message and sent to the receiver

DOWNLOADED FROM KTUASSIST.IN

Signing the digest in a digital signature

- The receiver receives the original message and the encrypted digest and separates the two.
- The receiver applies the same hash function to the message to create a second digest.
- The receiver also decrypts the received digest using the public key of the sender.
- If the two digests are the same all three aspects of security – Authentication, Non repudiation, integrity- are preserved.

DOWNLOADED FROM KTUASSIST.IN

MESSAGE NONREPUDIATION

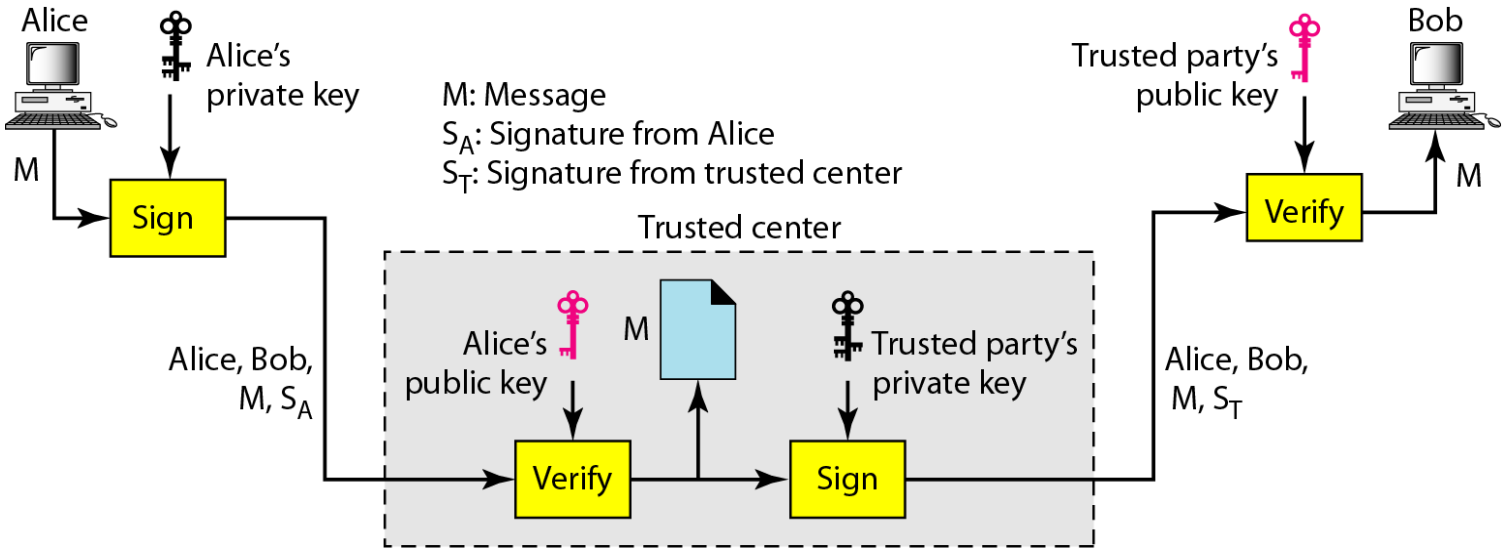


Figure: Using a trusted center for nonrepudiation

DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION

- Entity authentication is a technique designed to let one party prove the identity of another party.
- An entity can be a person, a process, a client, or a server.
- The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier

DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION

- In entity authentication, the claimant must identify herself to the verifier.
- This can be done with one of the three kinds of witnesses: something known, something possessed, or something inherent
  - Something known: examples are password, PIN, secret key etc
  - Something possessed: Examples are a passport, drivers license, credit card etc.
  - Something inherent: Examples are fingerprint, voice, facial characteristics, retinal pattern etc.

DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION

- We will discuss entity authentication by two methods
  - Passwords
  - Challenge-Response

DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION – using Passwords

- A password is used when a user needs to access a system to use the systems resources
- Each user has a user id and password
- We can divide this scheme into two separate groups:
  - Fixed password
  - One time password

DOWNLOADED FROM KTUASSIST.IN

Fixed Password

- In this group, the password is fixed; the same password is used over and over for every access
- This approach is subject to several attacks:
  - Eavesdropping
  - Stealing a password
  - Accessing password file
  - Guessing

DOWNLOADED FROM KTUASSIST.IN

One-time Password

- In this type of scheme, a password is used only once.
- It is called he one time password

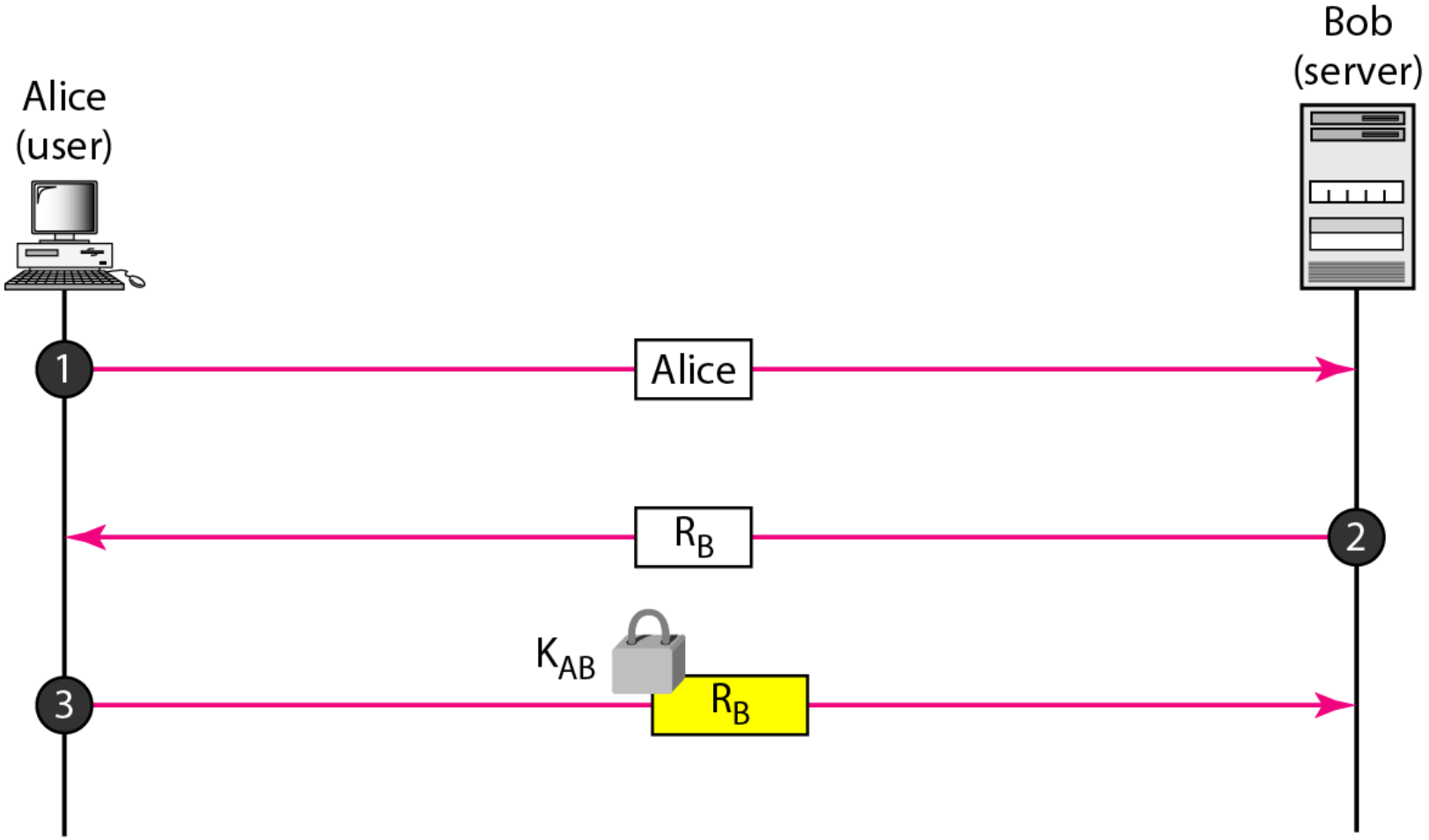
DOWNLOADED FROM KTUASSIST.IN

ENTITY AUTHENTICATION – Challenge-Response

- In challenge-response authentication, the claimant proves that she knows a secret without revealing it.

DOWNLOADED FROM KTUASSIST.IN

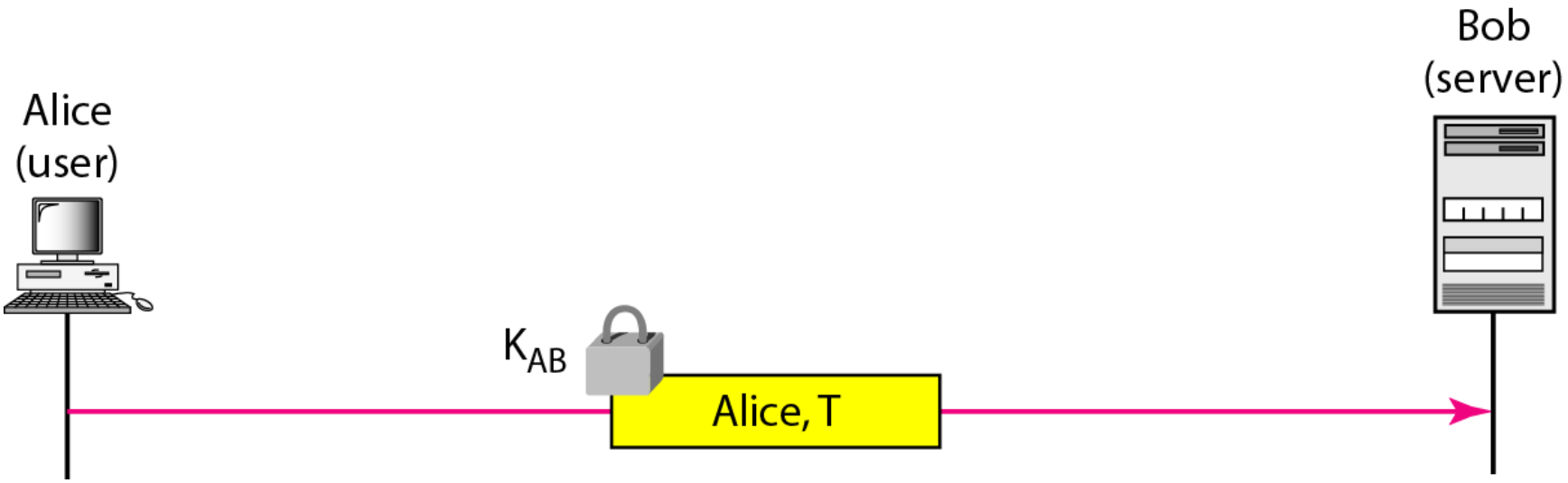
Challenge-Response: Using a Symmetric-Key Cipher



The challenge is a time-varying value sent by the verifier;
the response is the result of a function applied on the challenge.

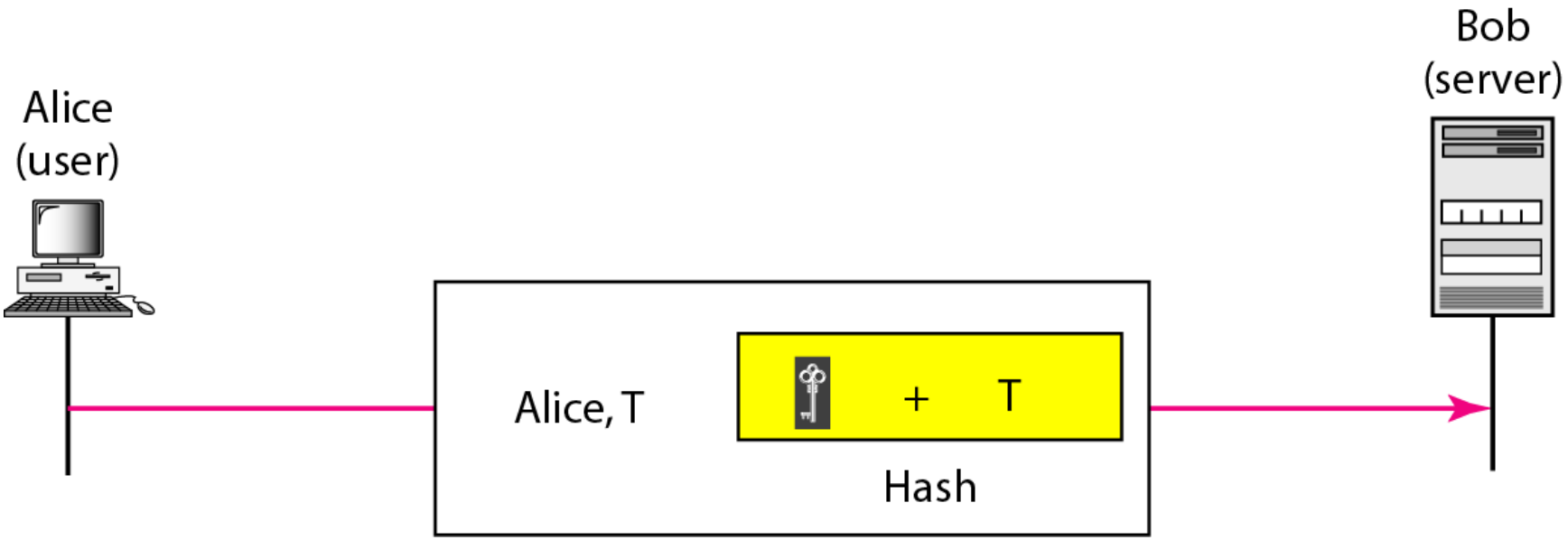
DOWNLOADED FROM KTUASSIST.IN

Challenge-response authentication using a timestamp



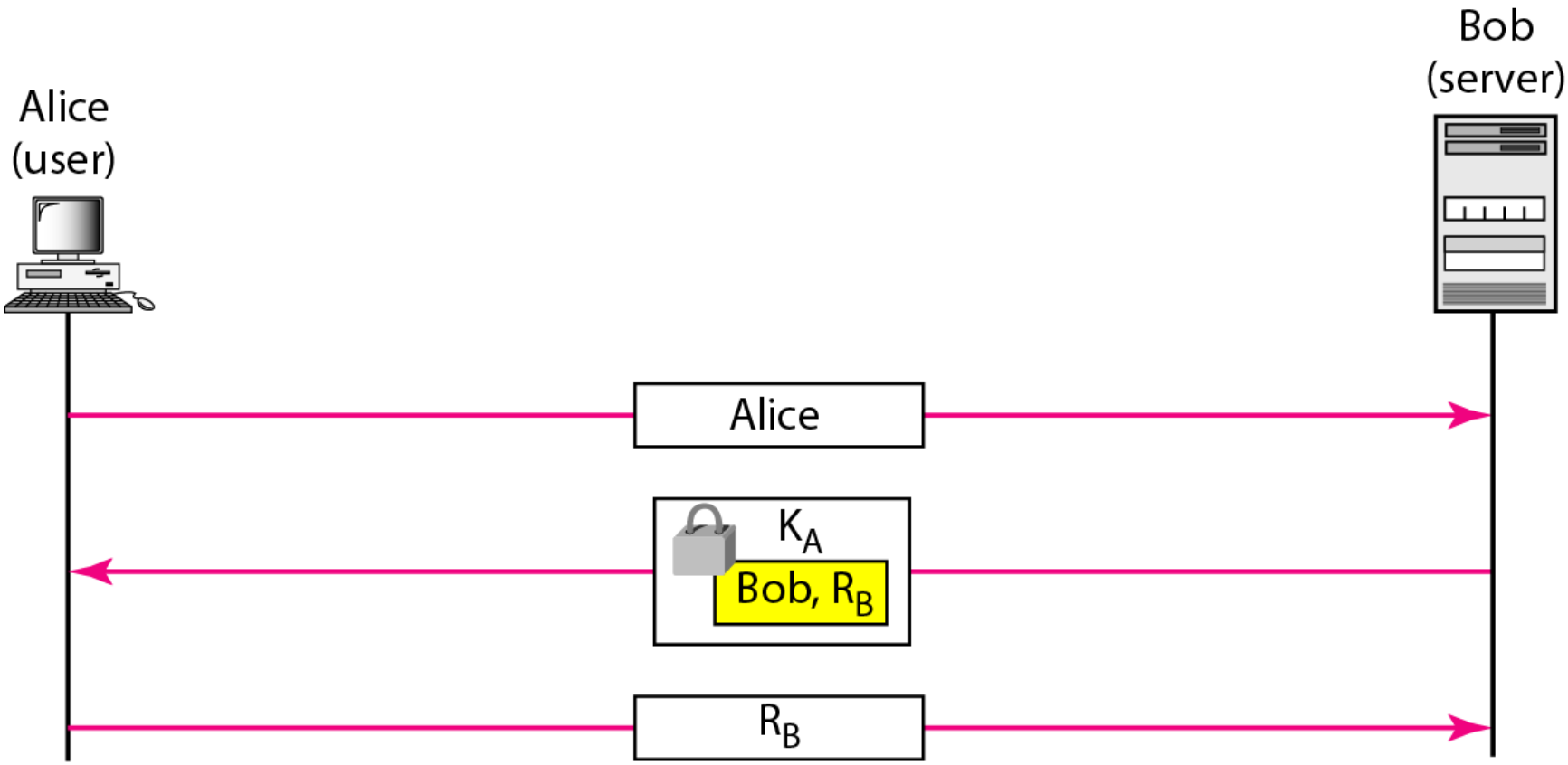
DOWNLOADED FROM KTUASSIST.IN

Challenge-response authentication using a keyed-hash function



DOWNLOADED FROM KTUASSIST.IN

Authentication, asymmetric-key



DOWNLOADED FROM KTUASSIST.IN

Security Attacks

- Any action that compromises the security of an information owned by an organization

DOWNLOADED FROM KTUASSIST.IN

Security Attacks

- Any action that compromises the security of an information owned by an organization
- Classification
  - Passive
  - Active

DOWNLOADED FROM KTUASSIST.IN

Security Attacks

- Any action that compromises the security of an information owned by an organization
- Classification
  - Passive – here the attackers goal is just obtain information that is being transmitted. So passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions
  - Active

DOWNLOADED FROM KTUASSIST.IN

Security Attacks

- Any action that compromises the security of an information owned by an organization
- Classification
  - Passive – here the attackers goal is just obtain information that is being transmitted. So passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions
  - Active – involves some modification of the data stream.

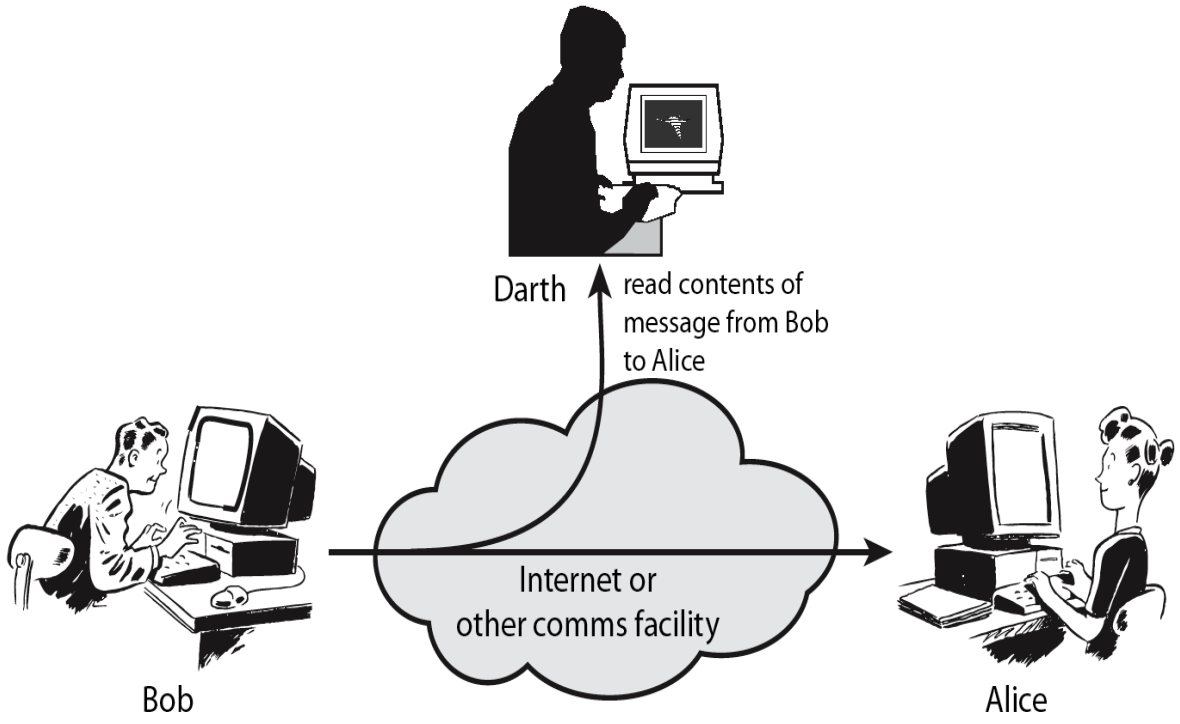
DOWNLOADED FROM KTUASSIST.IN

Passive Attacks

- Release of message contents(Snooping): refers to unauthorized access or interception of information

DOWNLOADED FROM KTUASSIST.IN

Release of message contents(Snooping)



DOWNLOADED FROM KTUASSIST.IN

Passive Attacks

- Release of message contents(Snooping): refers to unauthorized access or interception of information
- To prevent snooping, the data can be made nonintelligible to the intercepter by using encryption

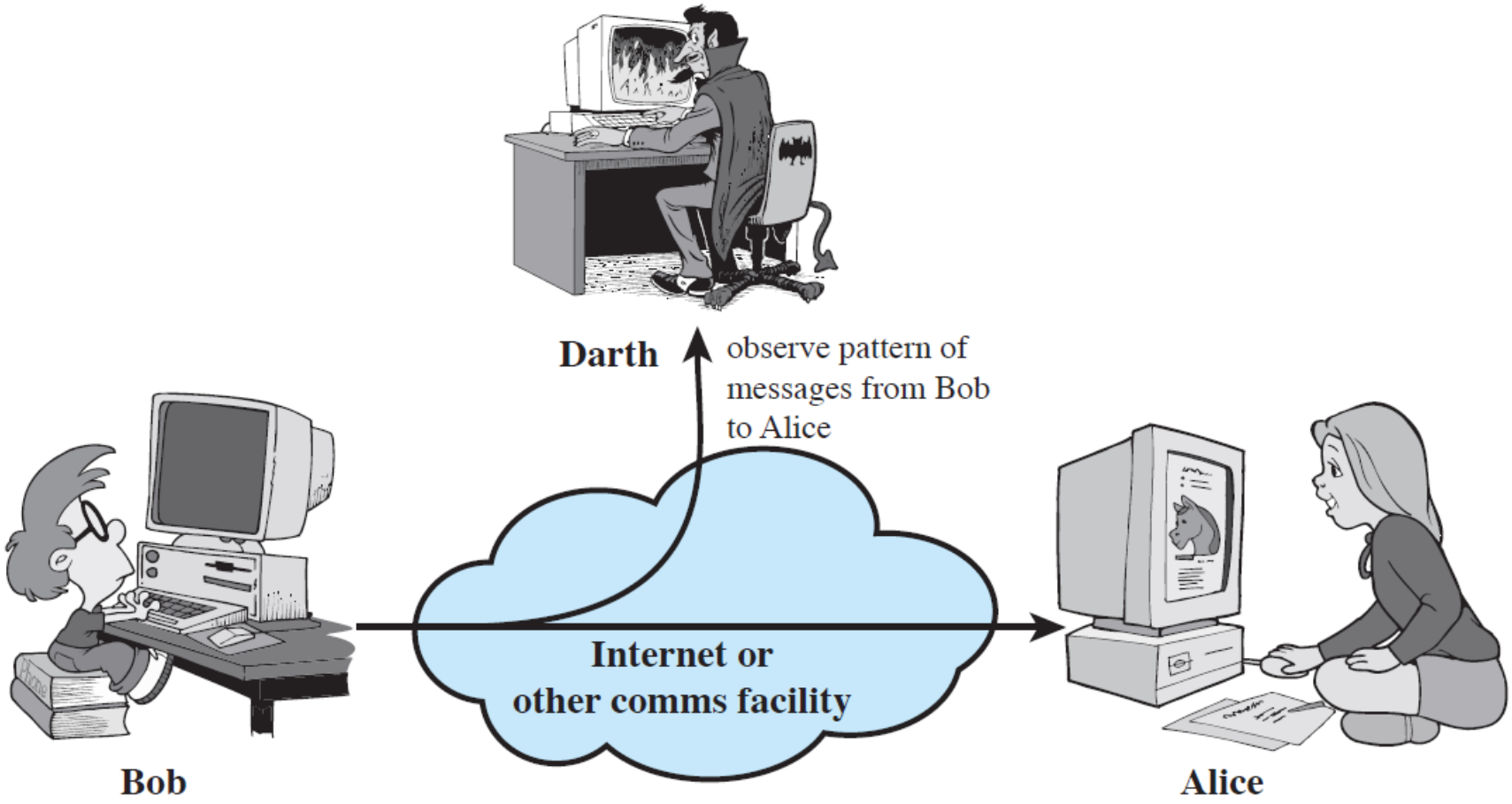
DOWNLOADED FROM KTUASSIST.IN

Passive Attacks

- Traffic analysis: Although encryption of data make it nonintelligible for the intercepter, he can obtain some other type of information by monitoring online traffic
- For example, he can find the identity such as email address of the sender and receiver
- Or he can collect pairs of requests and responses that might be useful in guessing the nature of the communication that was taking place.

DOWNLOADED FROM KTUASSIST.IN

Traffic analysis



DOWNLOADED FROM KTUASSIST.IN

Passive Attacks

- Passive attacks do not affect system resources
  - Eavesdropping, monitoring
- Two types of passive attacks
  - Release of message contents
  - Traffic analysis
- Passive attacks are very difficult to detect
  - Message transmission apparently normal
    - No alteration of the data
  - Emphasis on prevention rather than detection
    - By means of encryption

DOWNLOADED FROM KTUASSIST.IN

Active Attacks

- Four categories:
  - Modification of messages
  - Masquerade
  - Replay
  - Denial of Service

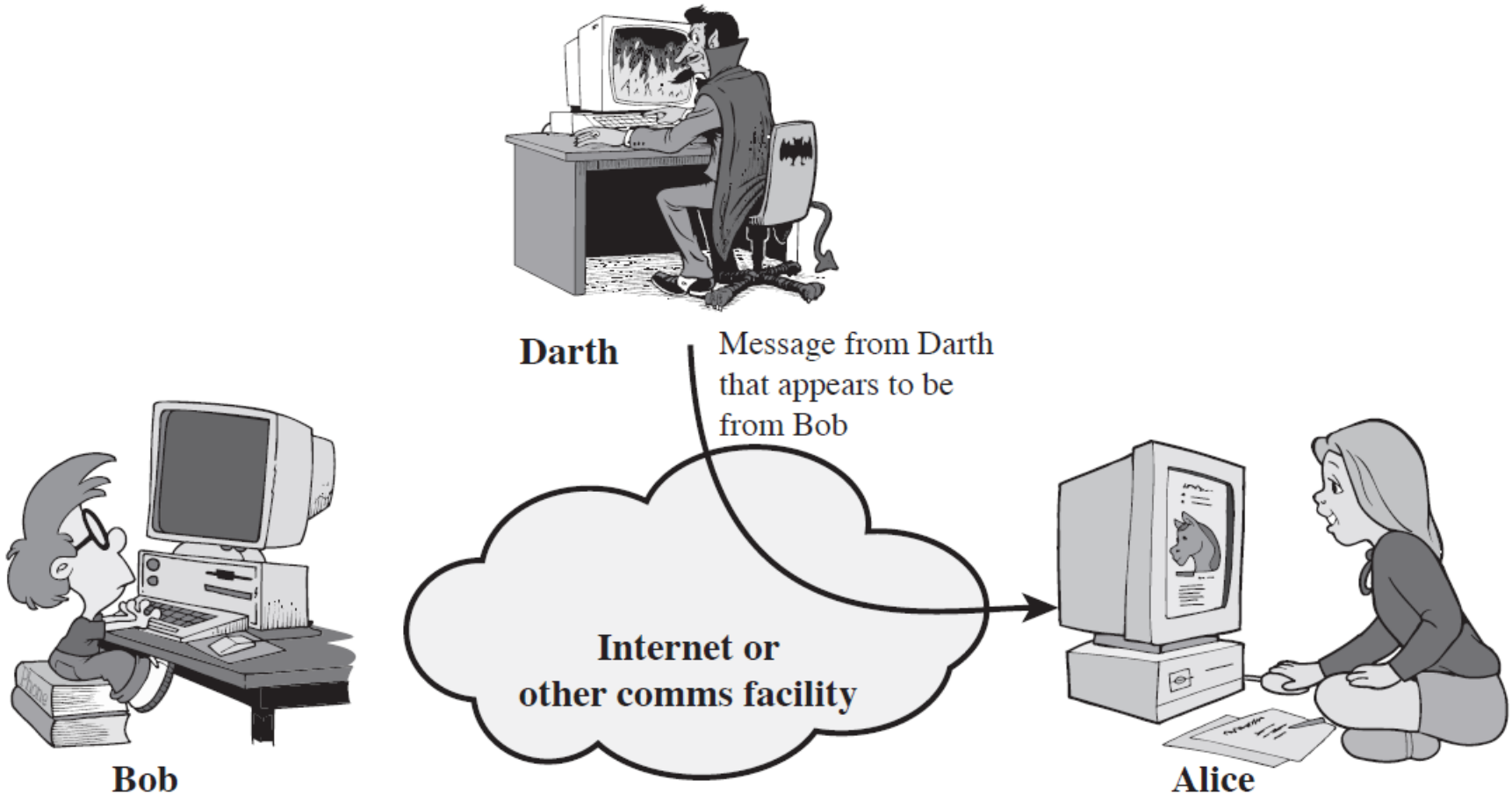
DOWNLOADED FROM KTUASSIST.IN

Modification of Messages

- means that some portion of the message is altered, or that message is delayed or reordered to produce an unauthorized effect.
- Ex: ‘allow John to read confidential file accounts’ is modified to mean ‘allow Brown to read confidential file accounts’

DOWNLOADED FROM KTUASSIST.IN

Masquerade



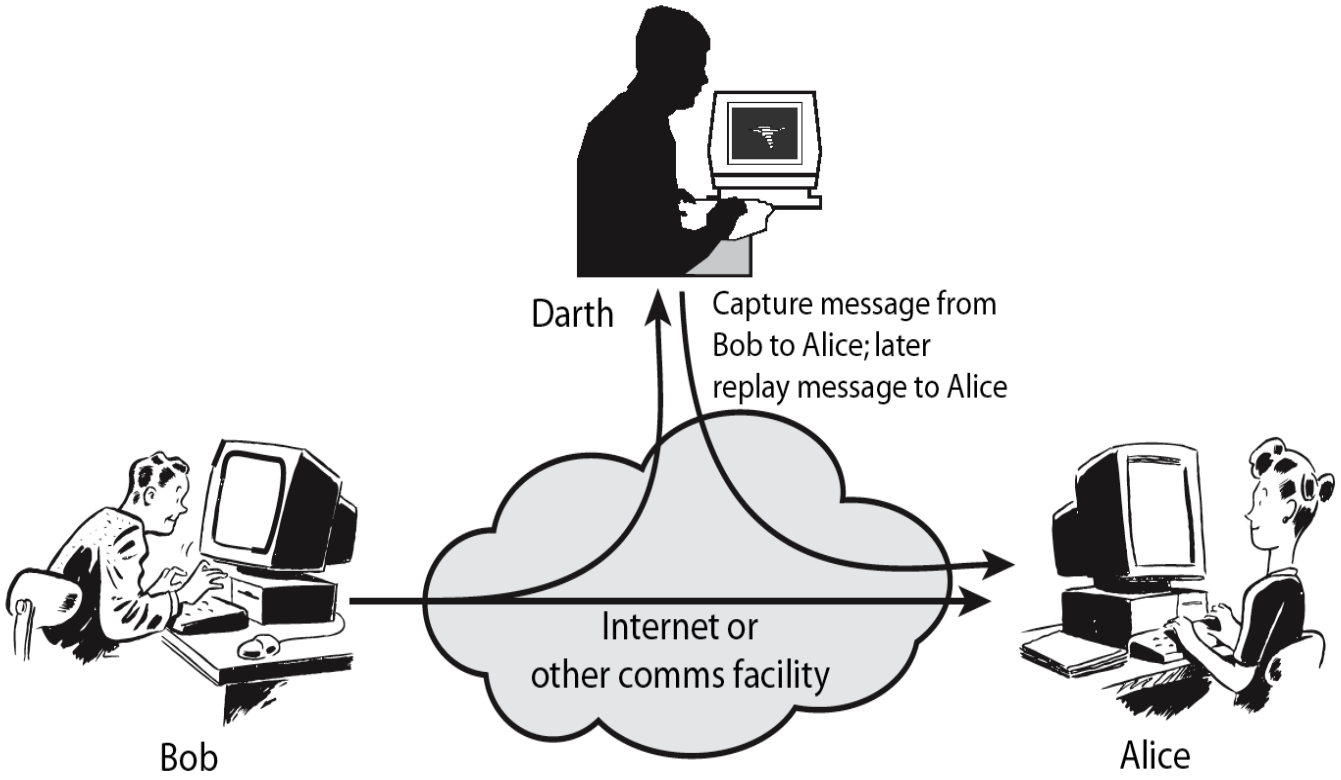
DOWNLOADED FROM KTUASSIST.IN

Masquerade

- Masquerading takes place when the attacker pretends to be a different entity.
- Ex: an attacker might steal the bank card and PIN of a bank customer and pretends that he is that customer
- Ex: a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

DOWNLOADED FROM KTUASSIST.IN

Replay



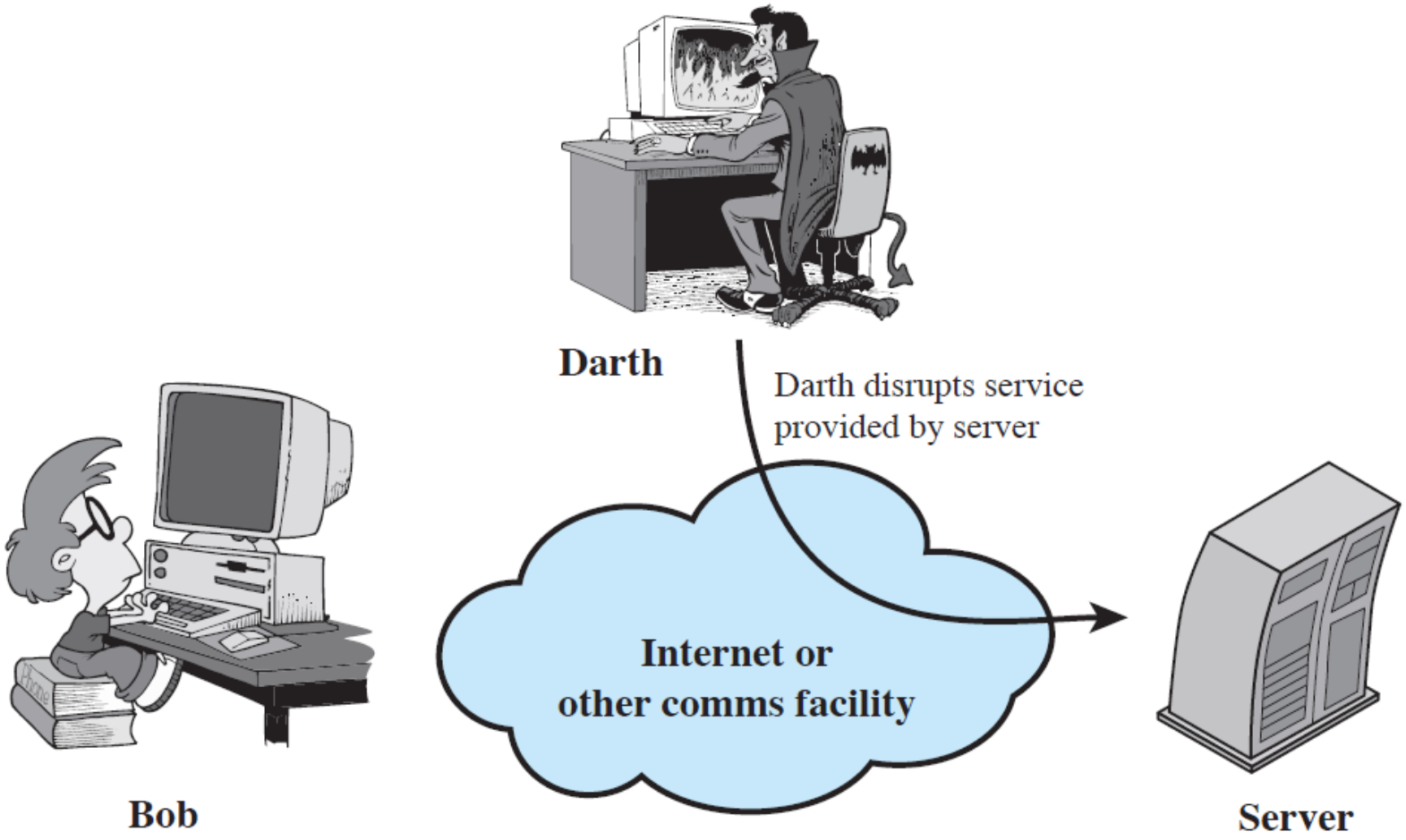
DOWNLOADED FROM KTUASSIST.IN

Replay

- The attacker obtains a copy of the message sent by a user and later tries to replay it.
- Ex: a person sends a request to her bank to ask for payment to the attacker. The attacker intercepts the message and sends it again to receive another payment from the bank.

DOWNLOADED FROM KTUASSIST.IN

Denial of Service(DoS)



DOWNLOADED FROM KTUASSIST.IN

Denial of Service(DoS)

- It may slow down or totally interrupt the service of a system.

DOWNLOADED FROM KTUASSIST.IN

Active Attacks

- Active attacks try to alter system resources or affect their operation
  - Modification of data, or creation of false data
- Four categories
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service: preventing normal use
    - A specific target or entire network
- Difficult to prevent
  - The goal is to detect and recover

DOWNLOADED FROM KTUASSIST.IN

IPSecurity (IPSec)

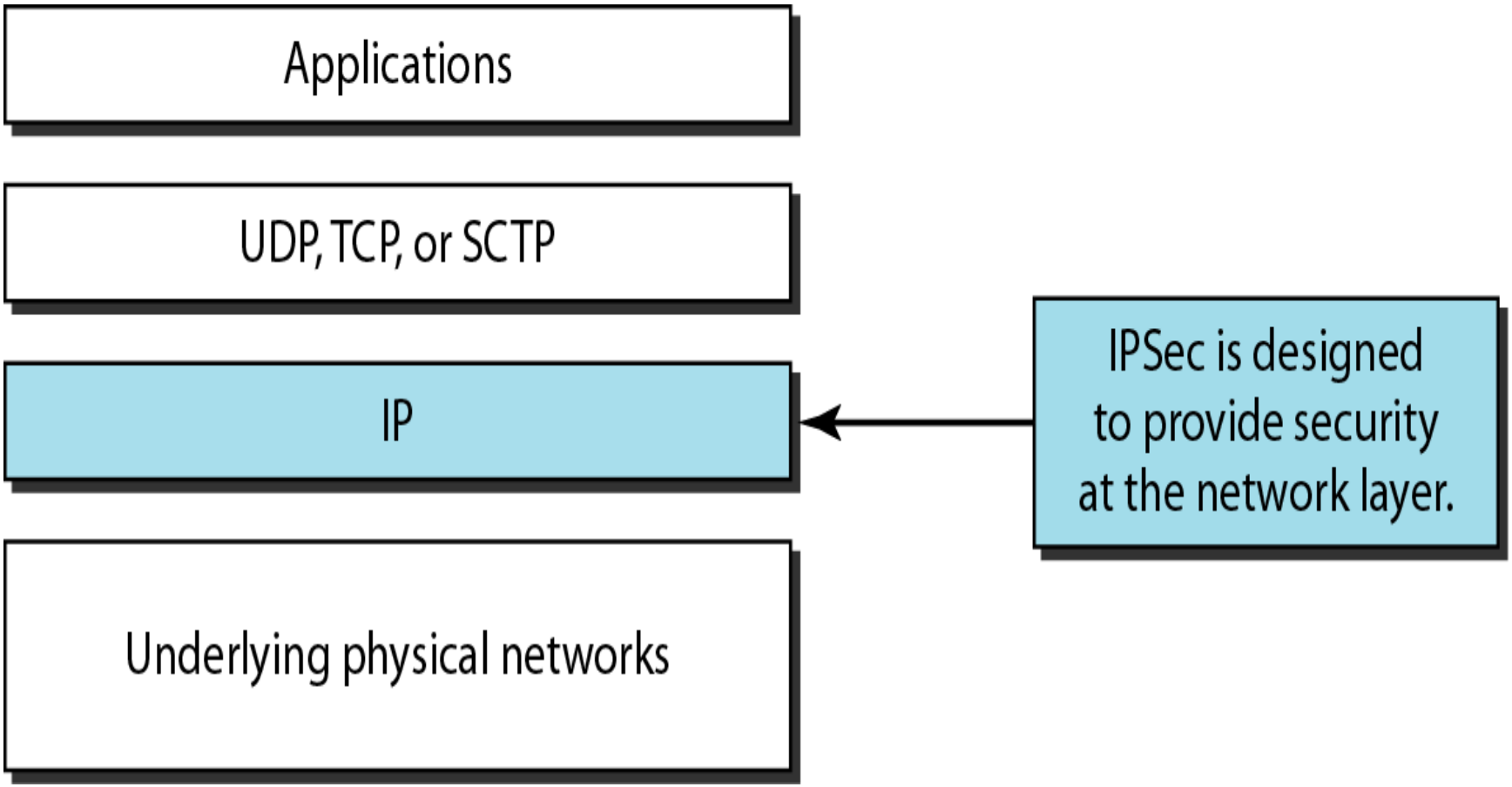
DOWNLOADED FROM KTUASSIST.IN

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. helps to create authenticated and confidential packets for the IP layer

DOWNLOADED FROM KTUASSIST.IN

TCP/IP Protocol suite and IPSec



DOWNLOADED FROM KTUASSIST.IN

Two Modes

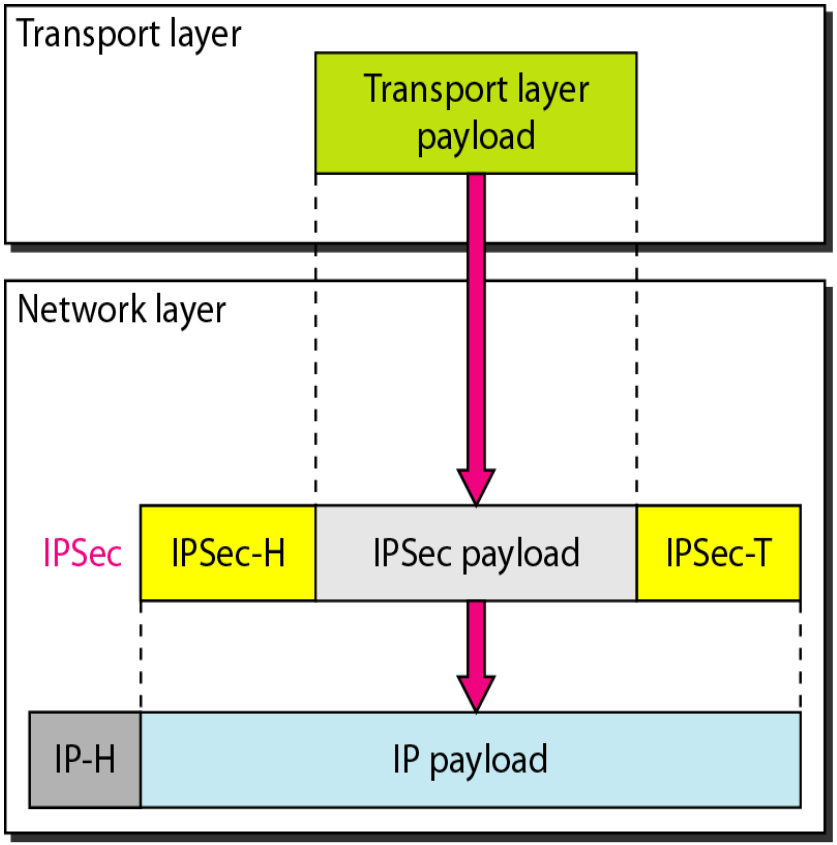
IPSec operates in one of two different modes

-Transport Mode

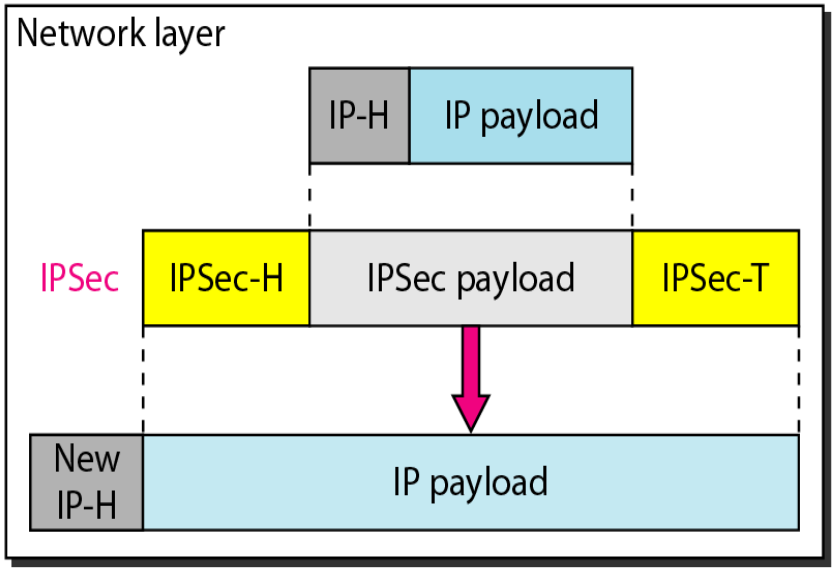
-Tunnel Mode

DOWNLOADED FROM KTUASSIST.IN

Transport mode and Tunnel modes of IPSec Protocol



a. Transport mode



b. Tunnel mode

DOWNLOADED FROM KTUASSIST.IN

Transport Mode

- In the transport mode IPSec protects what is delivered from the transport layer to the network layer.
- IPSec in the transport mode does not protect the IP header, it only protects the information coming from the transport layer

DOWNLOADED FROM KTUASSIST.IN

Tunnel Mode

- The tunnel mode IPSec protects the entire IP packet ,it takes an IP packet including the header applies IP security methods to the entire packet and then add a new IP header.
- The tunnel mode is normally used between two routers ,between a host and a router or between a router and a host.

DOWNLOADED FROM KTUASSIST.IN

Two Security Protocol

IPSec defines two protocols

-Authentication Header Protocol(AH)

-Encapsulating Security Payload Protocol(ESP)

to provide authentication and /or encryption for packets at the IP level

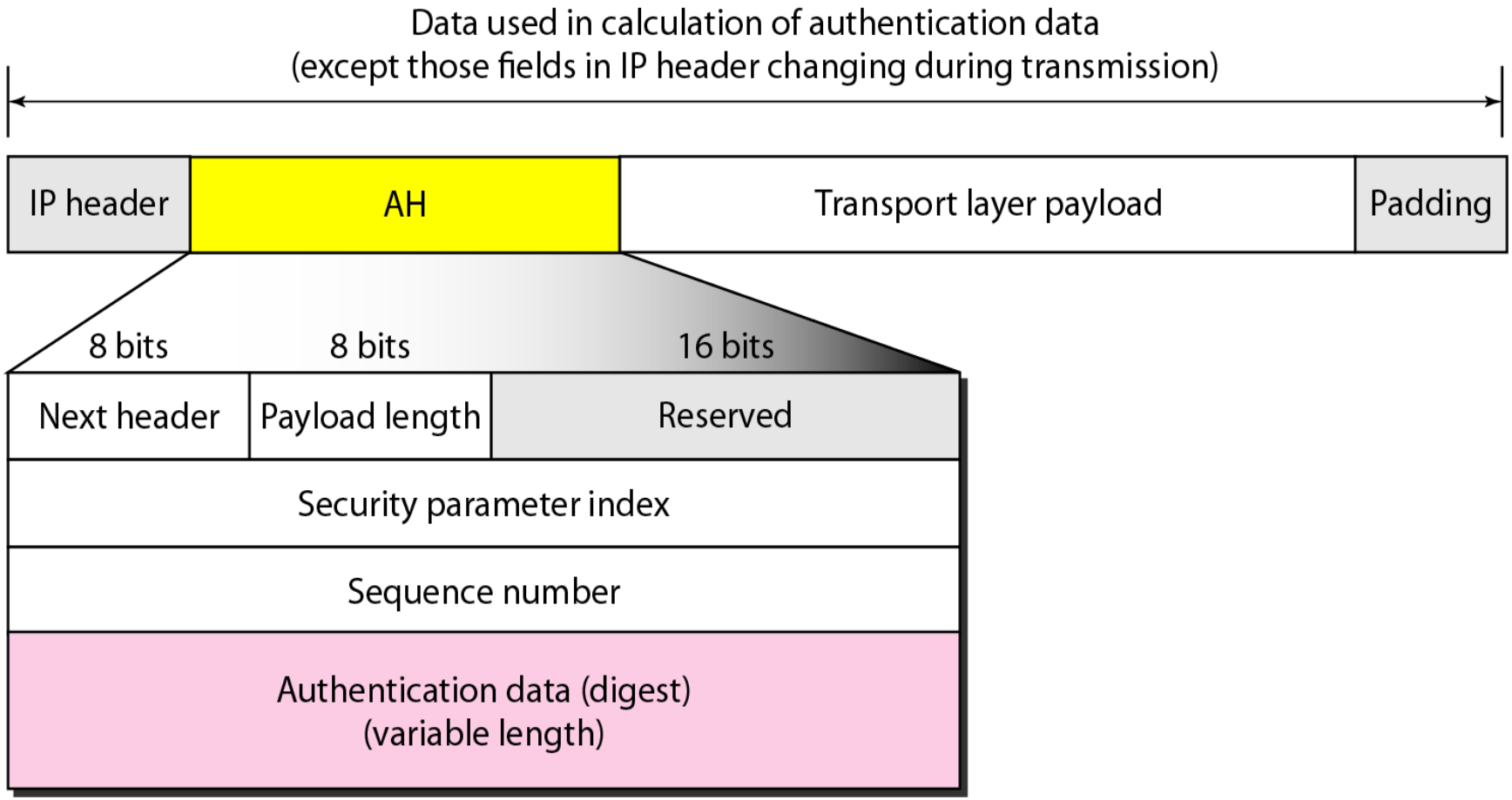
DOWNLOADED FROM KTUASSIST.IN

Authentication Header Protocol

- Authentication Header Protocol is designed to authenticate the source host.
- The AH is then placed to the appropriate location based on the mode.
- Figure shows the position of the authentication header in the transport mode

DOWNLOADED FROM KTUASSIST.IN

Authentication Header (AH) Protocol in Transport Mode



DOWNLOADED FROM KTUASSIST.IN

AH Protocol in Transport Mode

Next header-The 8 bit next header field defines the type of payload carried by the IP datagram(Such as TCP,UDP,ICMP or OSPF)It has the same function as the protocol field in the IP header before encapsulation.

DOWNLOADED FROM KTUASSIST.IN

AH Protocol in Transport Mode

Payload length (8 bit)-It defines the length of the authentication header

Security parameter index-The 32 bit security parameter index field plays the role of a virtual circuit identifier and is the same for all packets sent during a connection called a security association.

(Example-when Alice and Bob agree upon a set of security parameters between them, they have established a logical connection between themselves which is called security association.)

DOWNLOADED FROM KTUASSIST.IN

AH Protocol in Transport Mode

Sequence number-32 bit sequence number provides ordering information for a sequence of data grams.

Authentication data-Authentication data field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit(eg: time-to-live)

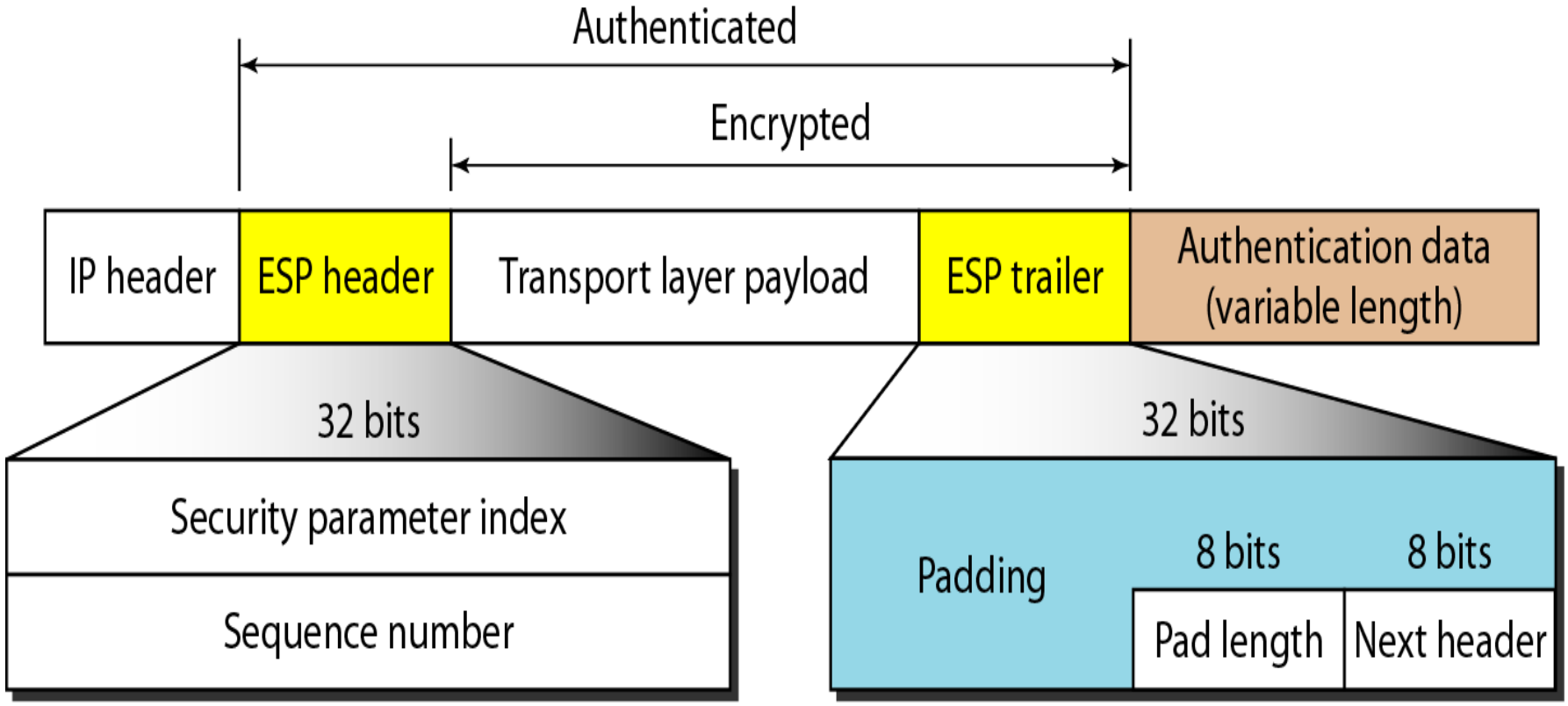
DOWNLOADED FROM KTUASSIST.IN

Encapsulating Security Payload Protocol (ESP)

- The AH protocol does not provide privacy, only source authentication and data integrity.
- IPSec later defined an alternative protocol that provides source authentication, integrity, and privacy called Encapsulating Security Payload (ESP).
- ESP adds a header and trailer.

DOWNLOADED FROM KTUASSIST.IN

Encapsulating Security Payload (ESP) Protocol in Transport Mode



DOWNLOADED FROM KTUASSIST.IN

ESP Protocol in Transport Mode

Padding-This variable length field (0-255 bytes) serves as padding.

Pad length-The 8 bit pad length field defines the number of padding bytes.

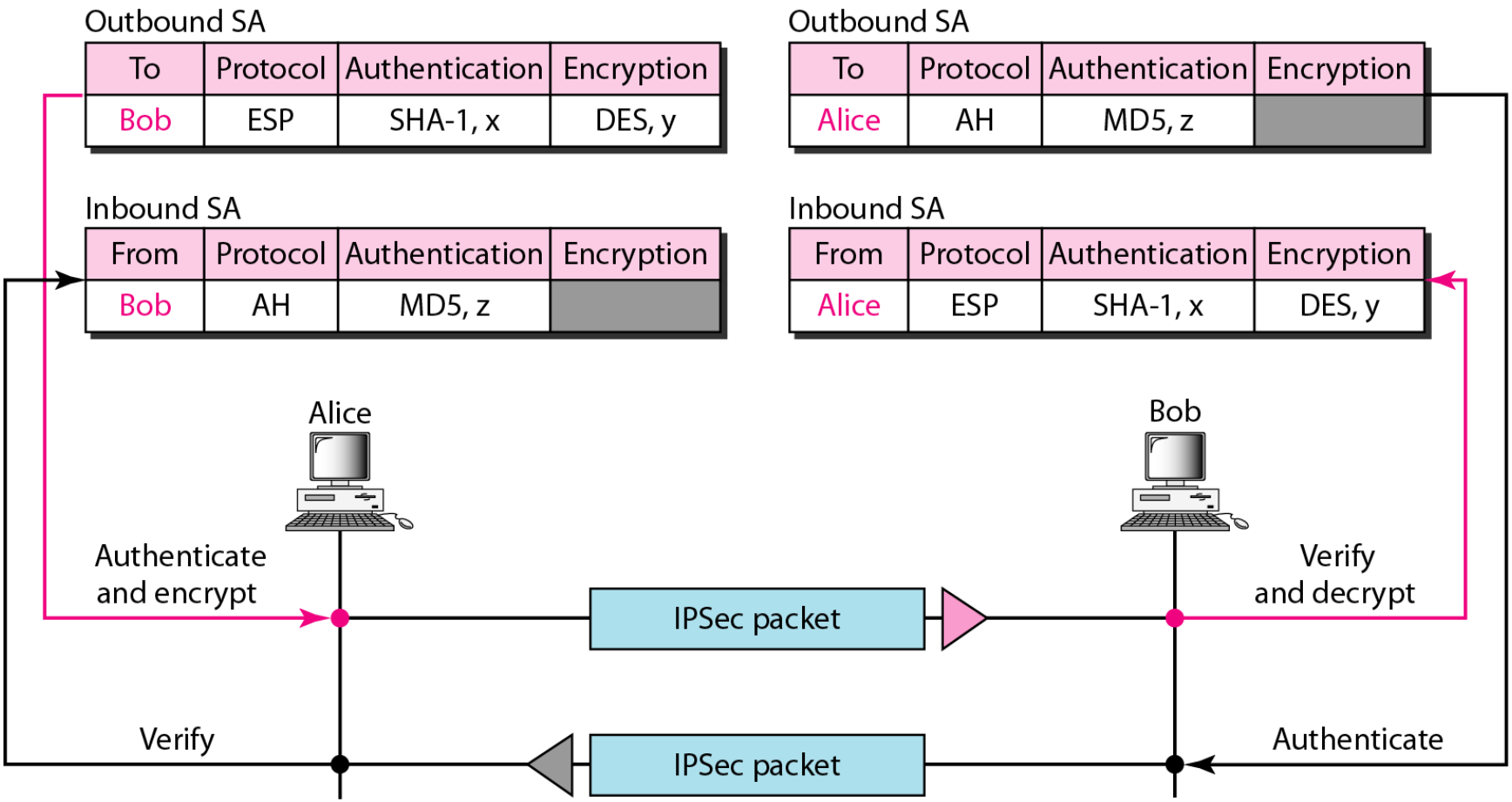
DOWNLOADED FROM KTUASSIST.IN

Security Association

- IPSec protocol requires a number of security measures has to be established between a sender and a particular receiver the first time the sender has a datagram to send to that receiver
- The establishment of this security measures is done via a mechanism called Security Association(SA)

DOWNLOADED FROM KTUASSIST.IN

Simple Inbound and Outbound Security Associations



DOWNLOADED FROM KTUASSIST.IN

Security Association

- Security Association Database(SADB): Sender and receiver has to maintain a security association for inbound and outbound communications with all people to whom they want to communicate. The database which contains this list of all SAs is called the SADB.
- Security Parameter Index: To distinguish one association from the other, each association is identified by a parameter called the security parameter index(SPI).

DOWNLOADED FROM KTUASSIST.IN

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

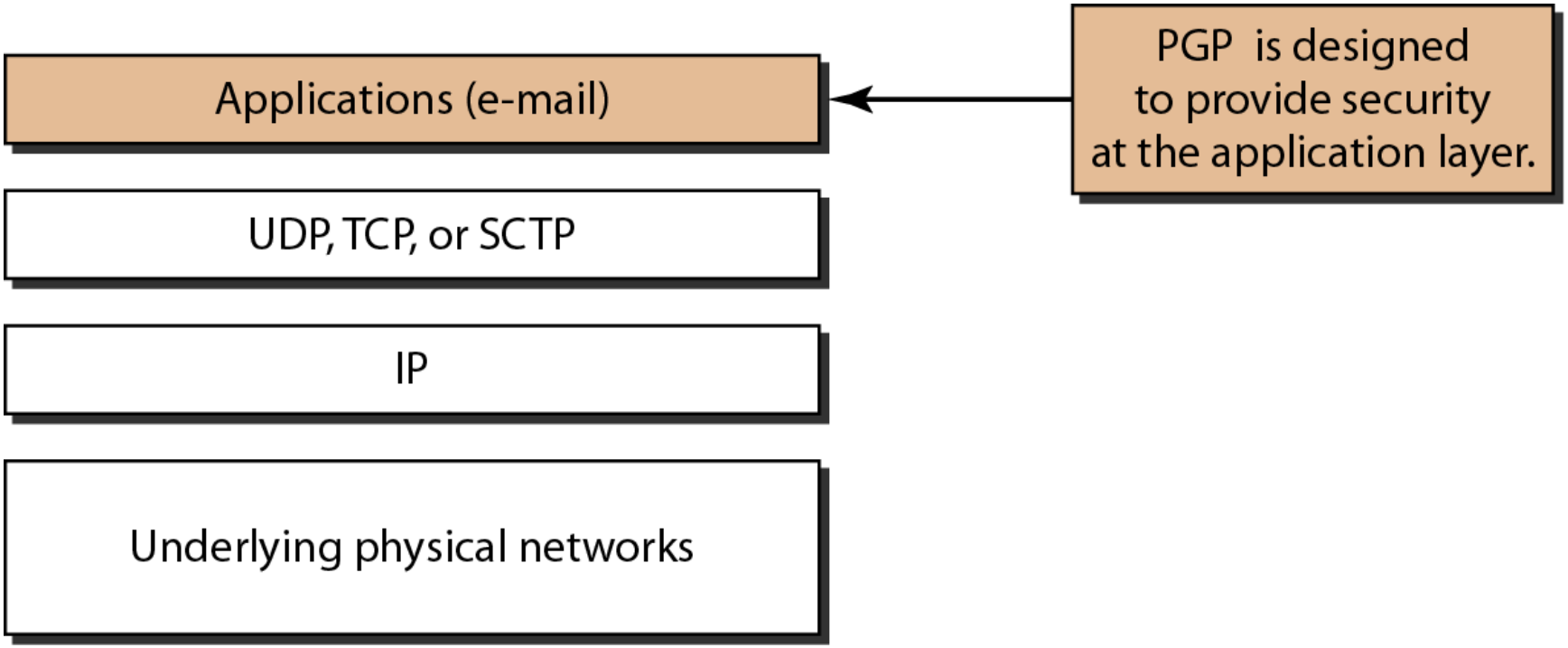
DOWNLOADED FROM KTUASSIST.IN

PGP(Pretty Good Privacy)

- 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.

DOWNLOADED FROM KTUASSIST.IN

Position of PGP in the TCP/IP protocol suite



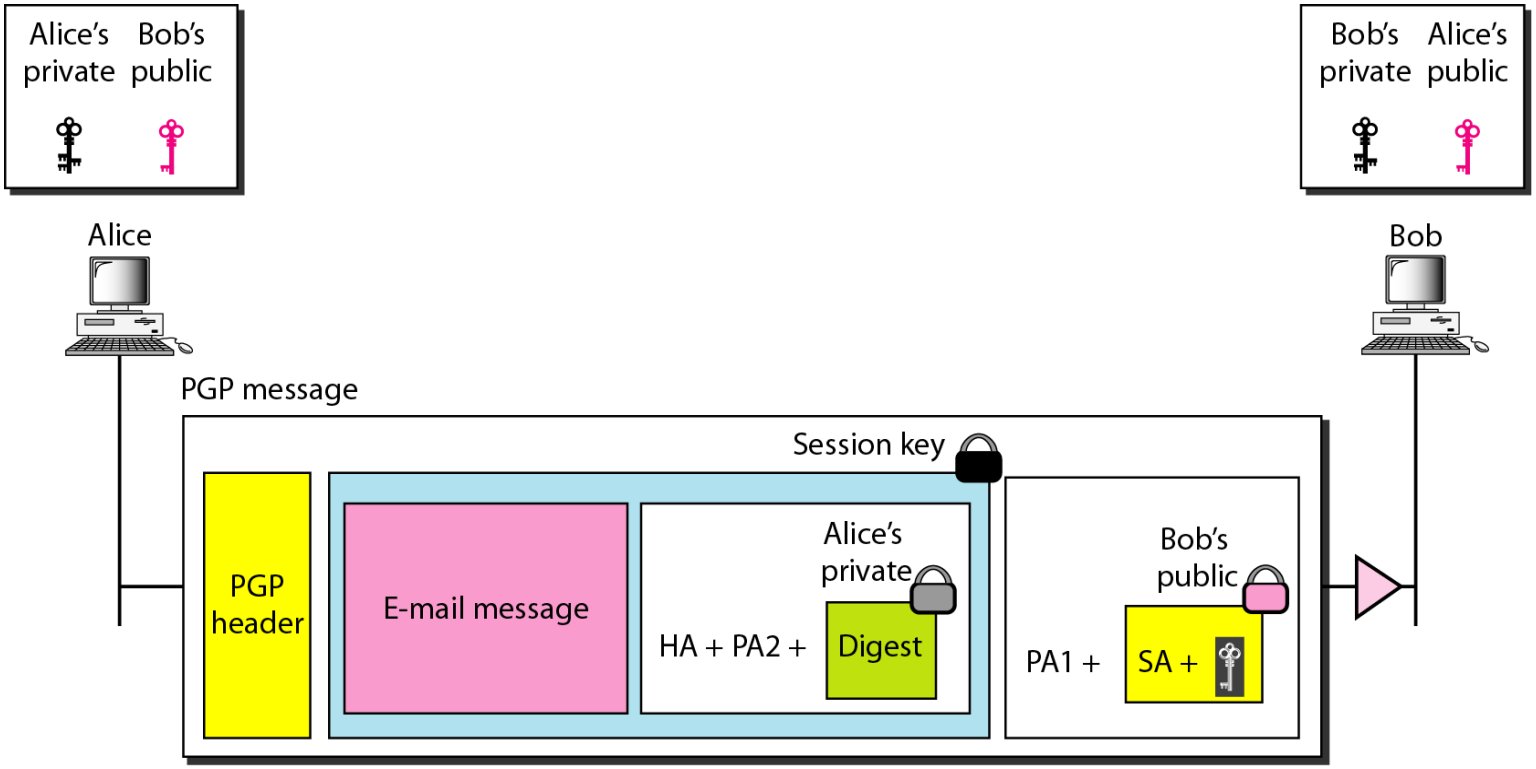
DOWNLOADED FROM KTUASSIST.IN

Security Parameters in PGP

- In PGP, the sender of the message needs to include the identifiers of the algorithms used in the message as well as the values of the keys.

DOWNLOADED FROM KTUASSIST.IN

A scenario in which an 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)

DOWNLOADED FROM KTUASSIST.IN

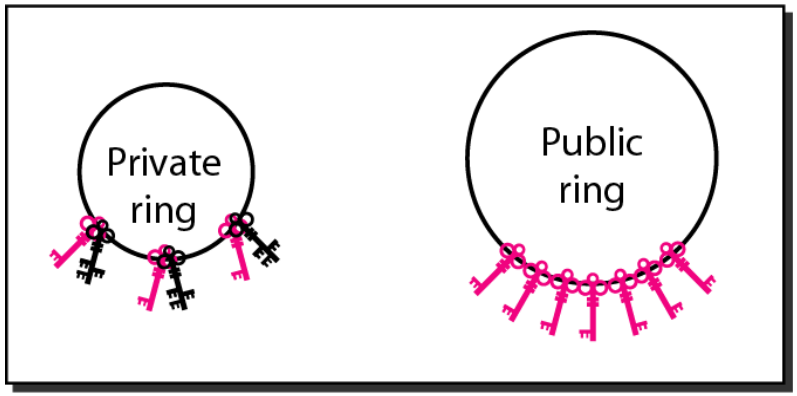
PGP Algorithms

Algorithm	*ID*	*Description*
Public key	1	RSA (encryption or signing)
	2	RSA (for encryption only)
	3	RSA (for signing only)
	17	DSS (for signing)
Hash algorithm	1	MD5
	2	SHA-1
	3	RIPE-MD
Encryption	0	No encryption
	1	IDEA
	2	Triple DES
	9	AES

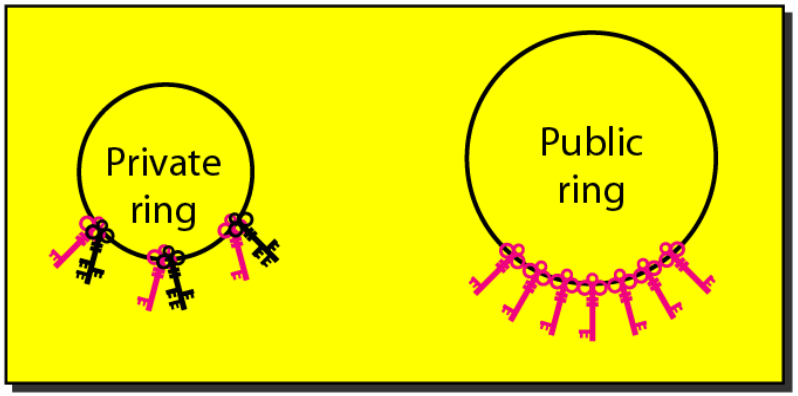
DOWNLOADED FROM KTUASSIST.IN

Key Rings in PGP

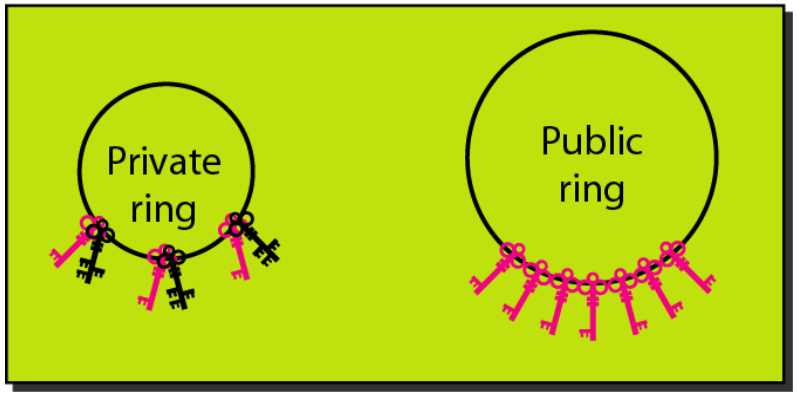
Alice's rings



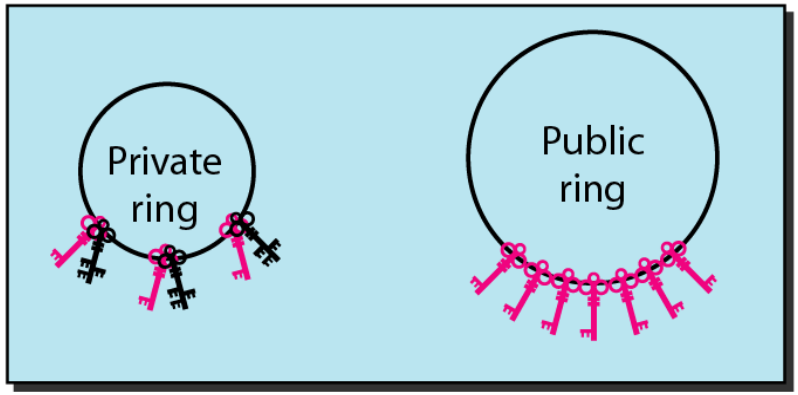
Bob's rings



Ted's rings



John's rings



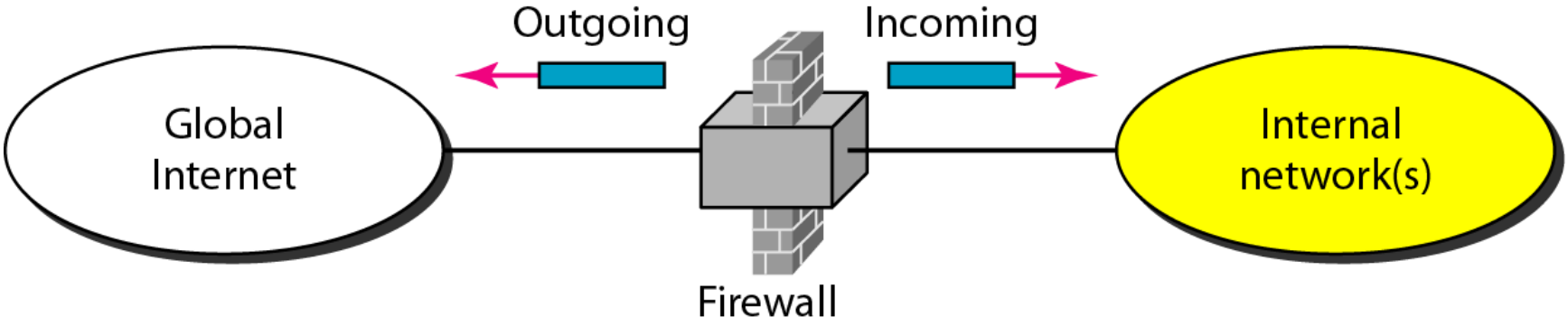
DOWNLOADED FROM KTUASSIST.IN

FIREWALLS

- All previous security measures cannot prevent Eve from sending a harmful message to a system.
- To control access to a system, we need firewalls.
- A firewall is a device installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (not forward) others.

DOWNLOADED FROM KTUASSIST.IN

Firewall



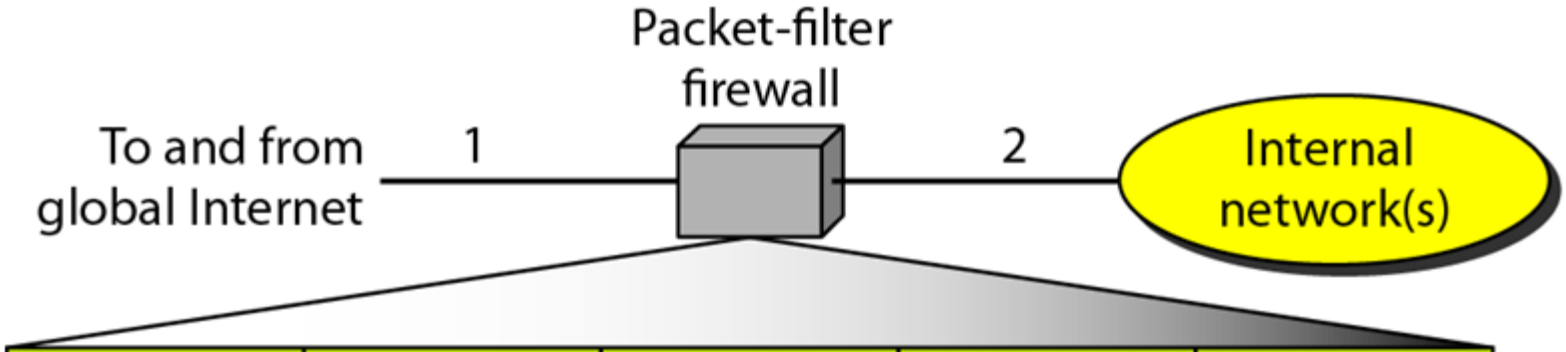
DOWNLOADED FROM KTUASSIST.IN

Classification

- A firewall is usually classified as
  - Packet-filter Firewall: A packet-filter firewall filters packets at the network or transport layer.
  - Proxy-based Firewall: A proxy firewall filters packets at the application layer.

DOWNLOADED FROM KTUASSIST.IN

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

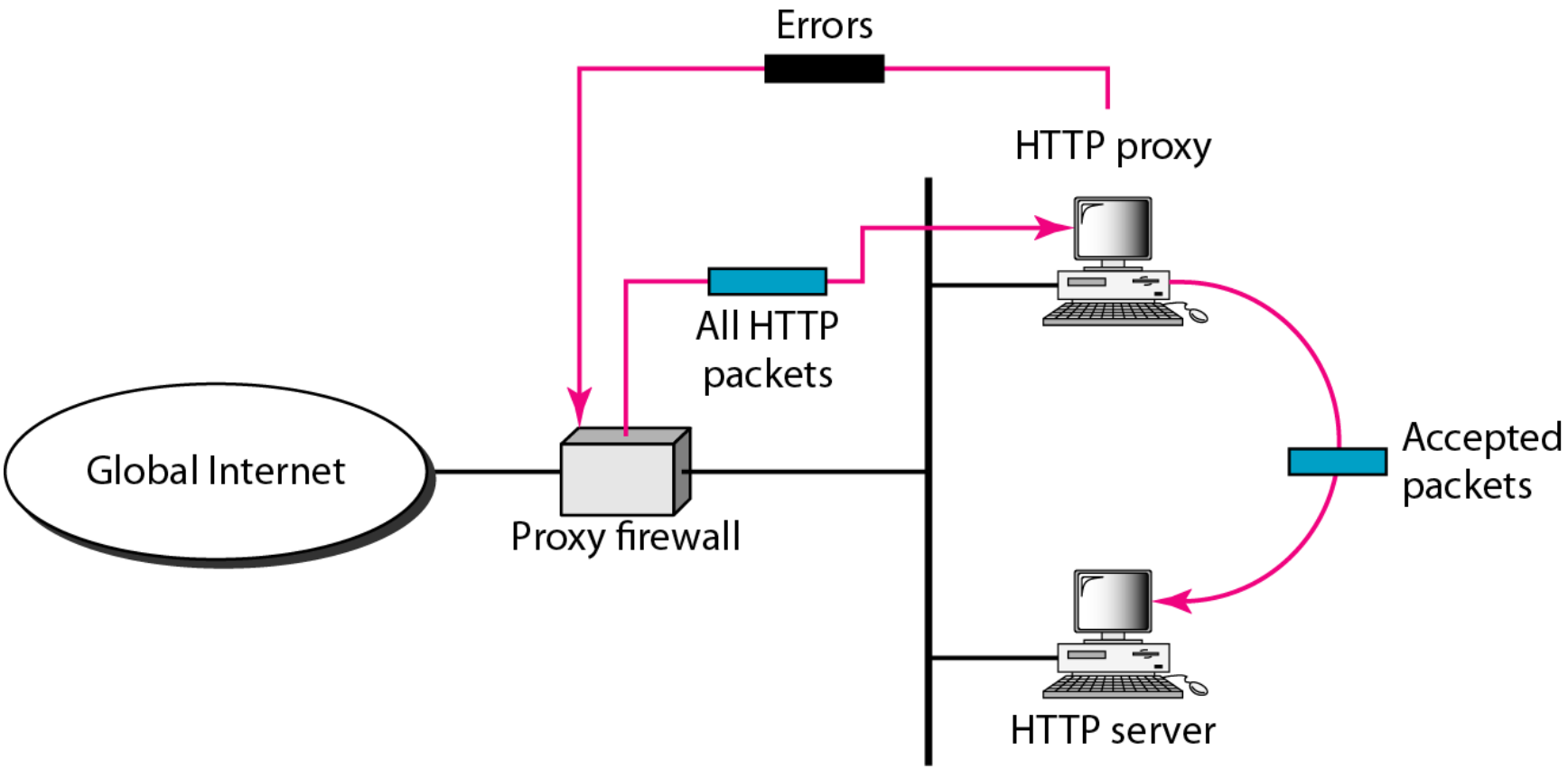
DOWNLOADED FROM KTUASSIST.IN

Proxy Firewall

- The packet filter firewall is based on the information available in the network layer and the transport layer headers.
- However, sometimes we need to filter a message based on the information available in the message itself(at the application layer).
- A proxy firewall does that

DOWNLOADED FROM KTUASSIST.IN

Proxy Firewall



DOWNLOADED FROM KTUASSIST.IN

Limitations of Firewall

- A firewall does not restrict communication between hosts that are inside the firewall, the adversary who does manage to run code internal to a site can access all local hosts

DOWNLOADED FROM KTUASSIST.IN

Limitations of Firewall

- A firewall does not restrict communication between hosts that are inside the firewall, the adversary who does manage to run code internal to a site can access all local hosts
- How might an adversary get inside the firewall?

DOWNLOADED FROM KTUASSIST.IN

Limitations of Firewall

- A firewall does not restrict communication between hosts that are inside the firewall, the adversary who does manage to run code internal to a site can access all local hosts
- How might an adversary get inside the firewall?
  - He might be a dissatisfied employee with legitimate access
  - Or the adversary's software could be hidden in some software installed from a CD or downloaded from web

DOWNLOADED FROM KTUASSIST.IN

Limitations of Firewall

- Firewall is not fully able to keep malware out of a system
- Malware types: Virus, worms, spyware
- These programs can collect and transmit private information about a computer system

DOWNLOADED FROM KTUASSIST.IN

INTRUSION DETECTION SYSTEMS (IDS)

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

DOWNLOADED FROM KTUASSIST.IN

IDS

- IDS types range in scope from single computers to large networks.
- The most common classifications are Network based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS).
- A system that monitors important operating system files is an example of an HIDS, while a system that analyzes incoming network traffic is an example of an NIDS.

DOWNLOADED FROM KTUASSIST.IN

Intruders

- A significant security problem for networked systems is hostile, unauthorized login or use of a system, by local or remote users; or by software such as a virus, worm, or Trojan horse.
- can identify classes of intruders (hackers or crackers):
  - masquerader
  - misfeasor
  - clandestine user

DOWNLOADED FROM KTUASSIST.IN

Intruders

- Masquerader: An individual who is not authorized to use the computer (outsider)
- Misfeasor: A legitimate user who accesses unauthorized data, programs, or resources (insider)
- Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection (either)

DOWNLOADED FROM KTUASSIST.IN

Intruders

- Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system)

DOWNLOADED FROM KTUASSIST.IN

Intruders

- clearly a growing publicized problem
- may seem benign, but still cost resources
- may use compromised system to launch other attacks
- awareness of intruders has led to the development of CERTs(computer emergency response teams)

DOWNLOADED FROM KTUASSIST.IN

Intrusion Techniques

- aim to gain access and/or increase privileges on a system
- Generally this requires the intruder to acquire information that should have been protected
- In some cases this information is in the form of a user password
- With the knowledge of some other users password, an intruder can log into a system and then exercise access rights of owner

DOWNLOADED FROM KTUASSIST.IN

Intrusion Techniques

- Typically a system must maintain a file that associates a password with each authorized user.
- If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords.
- The password file can be protected in one of two ways:
  - One-way function
  - Access control – access to a password file is limited one or a very few accounts

DOWNLOADED FROM KTUASSIST.IN

Password Learning Techniques

guess attack

1. Try default passwords used with standard accounts shipped with the system
2. Exhaustive try of all short passwords
3. Try words in system's dictionary or list of likely passwords (hacker bulletin boards)
4. Collect information about users (full names, names of spouses and children, pictures and books in their office, related hobbies)
5. Try users' phone numbers, social security numbers, room numbers
6. Try all legitimate license plate numbers
7. Use a trojan horse
8. Tap the line between a remote user and the system

DOWNLOADED FROM KTUASSIST.IN

Intrusion Detection

- Intrusion detection, is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise your system and network resources.

DOWNLOADED FROM KTUASSIST.IN

Intrusion Detection Systems(IDS)

- An intrusion detection system(IDS) is a software that automates the intrusion detection process. It is a system designed to detect unauthorized access to secure systems, ie, hacking.

- Intrusion Prevention System(IPS) is a software with all the properties of IDS, with the additional feature that it stops the intrusions

DOWNLOADED FROM KTUASSIST.IN

False Positives and Negatives

- The IDS adopts statistical methods to understand the threats to the system
- Therefore IDS cannot provide complete and accurate detection
- The false alarms are defined as follows
  - False Positive: when the IDS incorrectly identifies a harmless activity as malicious, a false positive is said to have occurred
  - False Negative: when the IDS fails to identify a malicious activity, a false negative is said to have occurred

DOWNLOADED FROM KTUASSIST.IN

Intrusion Detection Techniques

- The following approaches are used to detect intrusion
  - Statistical Anomaly Detection
  - Rule Based Detection

DOWNLOADED FROM KTUASSIST.IN

Intrusion Detection Techniques

- Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

- Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Then statistical tests are applied to observed behavior to determine whether that behavior is not legitimate user behavior
- It falls into two categories:
  - Threshold detection
  - Profile based

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection

- Threshold detection: defines thresholds for the frequency of occurrence of various events(independent of user)
  - Counting the number of occurrences of a specific event type over an interval of time.
  - If the count surpasses threshold, then intrusion is assumed

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection

- Threshold detection: examples –
  - The number of failed attempts to login to the system
  - The amount of CPU utilized by a program
  - The number of files accessed by a given user over a certain period of time

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection

- Threshold detection
- Profile based: it focuses on characterizing the past behavior of individual users or related group of users and then detecting significant deviations
  - The foundation for profile based approach is an analysis of Audit records

DOWNLOADED FROM KTUASSIST.IN

Audit Records

- fundamental tool for intrusion detection
- Some record of ongoing activity by users must be maintained as input to an intrusion detection system
- native audit records
  - part of all common multi-user O/S
  - already present for use
  - may not have information wanted in desired or convenient form
- detection-specific audit records
  - created specifically to collect wanted information
  - at cost of additional overhead on system

DOWNLOADED FROM KTUASSIST.IN

Audit Records

- Consider the command

  copy game.exe to <library>game.exe

  issued by smith to copy an executable file game from the current directory to the <library> directory.

- The following audit records may be generated:

Subject	Action	Object	Exception condition	Resource Usage	Timestamp
Smith	Execute	copy.exe	0	CPU=3	11058721680
Smith	Read	<smith>game.exe	0	CPU=2	11058721679
Smith	Execute	<library>game.exe	Write-viol	CPU=3	11058721680

- In this case, the copy is aborted because smith does not have write permission to <Library>

DOWNLOADED FROM KTUASSIST.IN

Audit Records

- Each audit record contains the following fields:
  - Subject: initiator of action
  - Action: example read, execute, I/O operation etc
  - Object: Receptors of action. Examples include files, messages, records, printers etc.
  - Exception-condition: denotes which exception condition is raised on return
  - Resource usage: ex: processor time, I /O units used etc.
  - Time-stamp: unique time and date stamp identifying when the action took place

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection – Profile based

- An analysis of audit records over a period of time can be used to determine the activity profile of the average user.
- Current audit records are the input used to detect intrusion.
- The designer must decide on a number of quantitative measures or metrics that can be used to measure user behavior
- Examples of metrics that are useful for profile based intrusion detection are the following:
  - Counter, gauge, interval timer, resource utilization etc.

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection – Profile based

- Examples of parameters or metrics that are useful for profile-based intrusion detection are the following :
  - Counter: times of logins, number of times a command executed during a single user session, number of password failures, etc.
  - Gauge: the number of logical connections assigned to a user application, the number of outgoing messages queued for a user process, etc.
  - Interval timer: the length of time between successive logins to an account, etc.
  - Resource utilization: number of pages printed during a user session, total time consumed by a program execution, etc.

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection – Profile based

- Counter
  - A nonnegative integer that may incremented but not decremented
  - Examples include the number of logins by a single user during an hour, the number of password failures during a minute, the number of times a given command is executed etc.

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection – Profile based

- Gauge
  - A nonnegative integer that may be incremented or decremented
  - Examples include the number of logical connections assigned to a user application and the number of outgoing messages queued for a user process.

DOWNLOADED FROM KTUASSIST.IN

Statistical Anomaly Detection – Profile based

- Interval timer
  - The length of time between two related events
  - An example is the length of time between successive logins to an account
- Resource utilization
  - Quantity of resources consumed during a specified period
  - Examples include the number of pages printed during a user session and total time consumed by a program execution

DOWNLOADED FROM KTUASSIST.IN

Audit Record Analysis

- Using the metrics, various tests can be performed to determine whether current activities fit within acceptable limits.
  - mean & standard deviation
  - Multivariate model – is based on correlations between two or more variables
  - time series
  - operational

DOWNLOADED FROM KTUASSIST.IN

Advantage of Statistical Analysis

- The main advantage is that a prior knowledge of security flaws is not required.
- The detector program learns what is “normal” behavior and then looks for deviations
- The approach is not based on system dependent characteristics and vulnerabilities

DOWNLOADED FROM KTUASSIST.IN

Rule-Based Intrusion Detection

- Rule-based techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is suspicious.

DOWNLOADED FROM KTUASSIST.IN

Rule-based Penetration Identification

- It uses rules for identifying known penetrations or penetrations that would exploit known weaknesses, or identify suspicious behavior.

DOWNLOADED FROM KTUASSIST.IN

Rule-based Penetration Identification

- Examples of rules are
  - Users should not read files in other users personal directories
  - Users must not write other users files
  - Users should not make copies of system programs
  - Users who log in after hours often access the same files they used earlier.

DOWNLOADED FROM KTUASSIST.IN

Rule-based Penetration Identification

- The rules used are specific to machine and operating system.
- The rules are generated by “experts”, from interviews of system administrators and security analysts.
- Thus the strength of the approach depends on the skill of those involved in setting up the rules.

DOWNLOADED FROM KTUASSIST.IN

Comparison with firewalls

- Although they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening.
- Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network.
- An IDS describes a suspected intrusion once it has taken place and signals an alarm.
- An IDS also watches for attacks that originate from within a system.

DOWNLOADED FROM KTUASSIST.IN

What is an Intrusion Detection System?

- Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
- An IDS detects activity in traffic that may or may not be an intrusion.
- IDSs can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.

DOWNLOADED FROM KTUASSIST.IN

Host Based Intrusion Detection Systems

- Host intrusion detection systems (HIDS) run on individual hosts or devices on the network.
- A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.
- It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

DOWNLOADED FROM KTUASSIST.IN

Network Based Intrusion Detection

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
- Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
- Most Network-based IDS log their activities and report or alarm on questionable events.

DOWNLOADED FROM KTUASSIST.IN

Comparison

Host Based

- Narrow in scope (watches only **specific** host activities)
- More complex setup
- Better for detecting attacks from the **inside**
- **More expensive** to implement
- Detection is based on what any **single host** can record
- Does not see packet headers
- Usually only responds **after** a suspicious log entry has been made
- OS-specific
- Detects local attacks before they hit the network
- Verifies success or failure of attacks

Network Based

- Broad in scope (watches **all** network activities)
- Easier setup
- Better for detecting attacks from the **outside**
- **Less expensive** to implement
- Detection is based on what can be recorded on the **entire network**
- Examines packet headers
- Near **real-time** response
- OS-independent
- Detects network attacks as payload is analyzed
- Detects unsuccessful attack attempts

DOWNLOADED FROM KTUASSIST.IN

Hybrid Intrusion Detection

- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
- A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
- A Hybrid IDS is often deployed on an organization's most critical servers.

DOWNLOADED FROM KTUASSIST.IN

Honeypots

- Are decoy servers or systems setup to gather information regarding an attacker of intruder into networks or systems.
- Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.
- Provide you early warning about new attacks and exploitation trends which allow administrators to successfully configure a behavioral based profile and provide correct tuning of network sensors.
- Can capture all keystrokes and any files that might have been used in the intrusion attempt.

DOWNLOADED FROM KTUASSIST.IN