SNS COLLEGE OF TECHNOLOGY

(Autonomous)
Coimbatore – 641 035.

SUB CODE & NAME: 19ECT301 &COMMUNICATION NETWORKS

2 MARKS

UNIT 1

1. What are the three criteria necessary for an effective and efficient network?
   The most important criteria are performance, reliability and security.Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w.Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network‟s robustness in a catastrophe. Security issues include protecting data from unauthorized access and viruses.

2. Group the OSI layers by function?
   The seven layers of the OSI model belonging to three subgroups.Physical, data link and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another.Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems.The transport layer ensures end-to-end reliable data transmission.

3. What are header and trailers and how do they get added and removed?
   Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

4. What are the features provided by layering?
   Two nice features:
   • It decomposes the problem of building a network into more manageable components.
   • It provides a more modular design.

5. Why are protocols needed?
   In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

6. What are the two interfaces provided by protocols?
   • Service interface
   • Peer interface
   Service interface- defines the operations that local objects can perform on the protocol.

Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

7. Mention the different physical media?

]• Twisted pair(the wire that your phone connects to)
• Coaxial cable(the wire that your TV connects to)
• Optical fiber(the medium most commonly used for highbandwidth, long-distance links)
• Space(the stuff that radio waves, microwaves and infra red beams propagate through)

8. Define Signals?

Signals are actually electromagnetic waves traveling at the speed of light. The speed of light is, however, medium dependent-electromagnetic waves traveling through copper and fiber do so at about two-thirds the speed of light in vacuum.

9. What is wave's wavelength?

The distance between a pair of adjacent maxima or minima of a wave, typically measured in meters, is called waves wavelength.

10. Define Modulation?

Modulation -varying the frequency, amplitude or phase of the signal to effect the transmission of information. A simple example of modulation is to vary the power (amplitude) of a single wavelength.

11. Explain the two types of duplex?

• Full duplex-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
• Half duplex-it supports data flowing in only one direction at a time.

12. What is spread spectrum and explain the two types of spread spectrum?

Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.
• Frequency Hopping
• Direct sequence

13. Data Communication:

Data can be any text, image, audio, video, and multimedia files. Communication is an act of sending or receiving data. Thus, data communication refers to the exchange of data between two or more networked or connected devices. These devices must be capable of sending and receiving data over a communication medium.

14. Transmission medium & topology

In a network of computers, the transmission media provide the physical path for communication among the nodes and the manner in which the nodes are geometrically interconnected is known as its topology.

15. Protocol Layers and Their Service Models

Layered Architecture. Network designers organize protocols—and the network hardware and software that implement the protocols—in layers.

16. OSI: The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.

17. TCP/IP Model
    TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).

18. Circuit Switching:
    Circuit switching is a type of network configuration in which a physical path is obtained and dedicated to a single connection between two endpoints in the network for the duration of a dedicated connection. Ordinary voice phone service uses circuit switching.

19. Packet Switching:
    Packet switching is the transfer of small pieces of data across various networks. These data chunks or "packets" allow for faster, more efficient data transfer.

20. What is a virtual circuit?
    A logical circuit made between the sending and receiving computers. The connection is made after both computers do handshaking. After the connection, all packets follow the same route and arrive in sequence.

21. What are data grams?
    In datagram approach, each packet is treated independently from all others. Even when one packet represents just a place of a multi packet transmission, thenetwork treats it although it existed alone. Packets in this technology are referred to as datagram.

22. What is meant by switched virtual circuit?
    Switched virtual circuit format is comparable conceptually to dial-up line in circuit switching. In this method, a virtual circuit is created whenever it is needed and exits only for the duration of specific exchange

23. What is meant by Permanent virtual circuit?
    Permanent virtual circuits are comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two uses on a continuous basis. The circuit is dedicated to the specific uses.

24. What are the properties in star topology?
    • Even though a switch has a fixed number of inputs and outputs, which limits the number of hosts that can be connected to a single switch , large networks can be built by interconnecting a number of switches.
    • We can connect switches to each other and to hosts using point-to point links, which typically means that we can build networks of large geographic scope.

25. What is VCI?
    A Virtual Circuit Identifier that uniquely identifies the connection at this switch, and which will be carried inside the header of the packets that belongs to this connection

26. What is multiplexing?
    The job of gathering data chunks at the sources host from different sockets, encapsulating each data chunks with header information to create segments, and passing the segments to the network layer is called multiplexing.

27. What is de-multiplexing?
    The job of delivering the data in a transport layer segment to the correct socket is called demultiplexing.

UNIT 2

1. Link layer Addressing
   The link layer addresses are set for network interfaces so that L2 connectivity works correctly in the network stack. Typically, the link layer addresses are 6 bytes long like in Ethernet but for IEEE 802.15. 4 the link layer address length is 8 bytes.

2. Elements of transport protocol
   Layer 3 of the OSI Model: Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network, while maintaining the quality of service requested by the transport layer

3. Transmission Control protocol
   The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets.

4. Application layer protocols
   Application layer protocols define how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer is an abstract layer that handles the sharing protocol of the TCP/IP and OSI model.

5. IPV4
   The IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine. An IPv4 address is typically written in decimal digits, formatted as four 8-bit fields that are separated by periods. Each 8-bit field represents a byte of the IPv4 address.

6. What are the responsibilities of data link layer?
   Specific responsibilities of data link layer include the following. a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

7. What are the ways to address the framing problem?
   - Byte-Oriented Protocols(PPP)
   - Bit-Oriented Protocols(HDLC)
   - Clock-Based Framing(SONET)
8. Distinguish between peer-to-peer relationship and a primary-secondary relationship. peer -to- peer relationship?

All the devices share the link equally.Primary-secondary relationship: One device controls traffic and the others must transmit through it.

9. Define flow control?
   Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment

10. Mention the categories of flow control?
    There are 2 methods have been developed to control flow of data across communication links. a) Stop and wait- send one from at a time. b) Sliding window- send several frames at a time.

11. What is a buffer?
    Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

12. Define Routing?
    It is the process of building up the tables that allow thwe collect output for a packet to be determined.

13. Define ICMP? Internet Control Message Protocol is a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully

14. Write the keys for understanding the distance vector routing?

    The three keys for understanding the algorithm are,
    • Knowledge about the whole networks
    • Routing only to neighbors
    • Information sharing at regular intervals

15. Write the keys for understanding the link state routing?
    The three keys for understanding the algorithm are,
    • Knowledge about the neighborhood.
    • Routing to all neighbors.
    • Information sharing when there is a range.

16. How the packet cost referred in distance vector and link state routing?
    In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

17. Define Reliable flooding?
    It is the process of making sure that all the nodes participating in the routing protocol get a copy of the link state information from all the other nodes.

18. What is meant by congestion?
    Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources.

19. Why the congestion occurs in network?
    Congestion occurs because the switches in a network have a limited buffer size to store arrived packets.

20. What is meant by quality of service?
    The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

21. What are the two categories of QoS attributes?
    The two main categories are,
    • User Oriented
    • Network Oriented

22.List out the user related attributes?
    User related attributes are SCR – Sustainable Cell Rate PCR – Peak Cell Rate MCR-Minimum Cell Rate CVDT – Cell Variation Delay Tolerance.

23.What are the networks related attributes?
    The network related attributes are, Cell loss ratio (CLR) Cell transfer delay (CTD) Cell delay variation (CDV) Cell error ratio (CER).

24. What are the techniques to improve QoS?
    The techniques to improve QoS are
    •Scheduling
    • Traffic shaping
    • Resource reservation
    • Admission control

UNIT 3

1. Define TCP?
   TCP guarantees the reliable, in order delivery of a stream of bytes. It is a fullduplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

2. Define Congestion Control?
   It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

3. What are the functions of transport layer?
   •Breaks messages into packets.
   • Connection control.
   • Addressing.
   • Provide reliability

4. List some ways to deal with congestion
   •packet elimination
   • Flow control

- Buffer allocation
- Choke packets

5. Elements of Transport protocol
   Error Control.
   Flow Control.
   Connection Establishment/Release.
   Multiplexing/De multiplexing.
   Fragmentation and re-assembly.
   Addressing

6. Transmission Control protocol:
   TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

7. Domain Name System(DNS)
   DNS stands for Domain Name System. DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. DNS is required for the functioning of the internet. Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.

8. SNMP
   Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks.

9. WWW
   The World Wide Web—commonly referred to as WWW, W3, or the Web—is a system of interconnected public webpages accessible through the Internet. The Web is not the same as the Internet: the Web is one of many applications built on top of the Internet.

10. HTTP
    Hypertext Transfer Protocol (HTTP) is a method for encoding and transporting information between a client (such as a web browser) and a web server. HTTP is the primary protocol for transmission of information across the Internet.

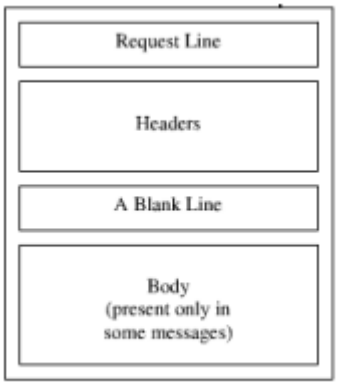
11. What is meant by segment?
    At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

12. What is meant by segmentation?
    When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

13. What is meant by Concatenation?
    The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

14. What are the three events involved in the connection?
    For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:
    • Connection establishment
    • Data transfer
    • Connection release

15. Give the format of HTTP request message?



16. Discuss the three main division of the domain name space.
    Domain name space is divided into three different sections: generic domains, country domains & inverse domain. Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes. Country domain: Uses two characters to identify a country as the last suffix. Inverse domain: Finds the domain name given the IP address.

17. What are the requests messages support SNMP and explain it?
    • GET
    • SET
    The former is used to retrieve a piece of state from some node and the latter is used to store a new piece of state in some node.

18. What are the types of DNS Message
    Two types of messages
    Query: header and question records
    Response: Header, question records, answer records, authoritative records, and additional records.

19. What are the four main properties of HTTP?
    •Global Uniform Resource Identifier
    • Request response exchange.
    • Statelessness.
    • Resource meta data

20. What is URL?
    URL is a string identifier that identifies a page on the World Wide Web.

21. What are the responsibilities of Application Layer?
    The Application Layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as e-mail, shared database management and other types of distributed information services
    - Network virtual Terminal,
    - File transfer, access and Management (FTAM),
    - Mail services,
    - Directory Services

22. Write down the three types of WWW documents.
    The documents in the WWW can be grouped into three broad categories: static, dynamic and active.
    A) Static: Fixed-content documents that are created and stored in a server.
    B) Dynamic: Created by web server whenever a browser requests the document.
    C) Active: A program to be run at the client side.

23. What is fully Qualified Domain Name?
    If a label is terminated by a null string is called a Fully Qualified Domain Name.

24. What is Generic Domains?
    Generic domain defines registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database. Eg.
    com – Commercial organizations,
    edu - Educational institutions,
    gov – Government Institutions.

25. What are the types of messages in HTTP transaction?
    The types of messages in HTTP transaction are
    - Request messages
    - Response messages

UNIT 4

1. Name four factors needed for a secure network?
   Privacy: The sender and the receiver expect confidentiality.
   Authentication: The receiver is sure of the sender‟s identity and that an imposter has not sent the message.
   Integrity: The data must arrive at the receiver exactly as it was sent.
   Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

2. How is a secret key different from public key?
   In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In public key, there are two

keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

3. Define Cryptography
    - Cryptography refers to the science and art of transforming messages to makeν them secure and immune to attacks.
    - Original message before being transformed is called plaintext.
    - After the message is transformed, is called ciphertext.
    - An encryption algorithm transforms the plaintext to ciphertext; a decryption algorithm transforms the ciphertext back to plaintext.
    - The term cipher is used to refer to encryption and decryption algorithms.

4. What are the advantages & disadvantages of public key encryption?
   Advantages:
   a) Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
   b) The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.
   Disadvantage:
   If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

5. Threats in network
   Active Network Threats: Activities such as Denial of Service (DoS) attacks and SQL injection attacks where the attacker is attempting to execute commands to disrupt the network's normal operation.

6. Cryptographic Techniques
   Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary. Based on the security needs and the threats involved, various cryptographic methods such as symmetric key cryptography or public key cryptography can be used during transportation and storage of the data.

7. Firewalls
   A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

8. Email Security
   Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise. Organizations can enhance their email security posture by establishing policies and using tools to protect against malicious threats such as malware, spam, and phishing attacks.

9. What are the advantages & disadvantages of secret key encryption?
   Advantage:
   Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages:

a) Each pair of users must have a secret key. If N people in world want to use this method, there needs to be N (N-1)/2 secret keys. For one million people to communicate, a half-billion secret keys are needed.

b) The distribution of the keys between two parties can be difficult.

10. Define substitution & transposition encryption?

Substitution: A character level encryption in which each character is replaced by another character in the set.

Transposition: A Character level encryption in which the characters retain their plaintext but the position of the character changes.

11. Differentiate conventional (symmetric) from public key (asymmetric) encryption.

Conventional Encryption	**Public-Key Encryption**
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	Needed to work: 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not of the same one).
Needed for Security: 1. The key must be kept secret. 2. It must be impossible or atleast impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of cipher text must be insufficient to determine the key.	Needed for security: 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of the cipher text must be insufficient to determine the other key.

12. Define – Key and Plaintext

In cryptography, a key is defined as a piece of information that determines the functional output of a cryptographic algorithm or cipher. In encryption, a key specifies the particular transformation of plaintext into cipher text or vice versa during decryption. Plaintext is ordinary readable text before being encrypted into cipher text or after being decrypted.

13. What is encipherment?

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

14. What is a passive attack?

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

15. What is the difference between a mono-alphabet cipher and a polyalphabetic cipher?
    Mono-alphabetic cipher is a mono-alphabetic cipher is a substitution cipher in which the cipher alphabet is fixed through the encryption process. All of the substitution ciphers we have seen prior to this handout are mono-alphabetic; these ciphers are highly susceptible to frequency analysis. Polyalphabetic Cipher is a polyalphabetic cipher is a substitution cipher in which the cipher alphabet changes during the encryption process.

16. Compare the symmetric and asymmetric key cryptography.
    Symmetric Encryption uses a single secret key that needs to be shared among the people who needs to receive the message while Asymmetric encryption uses a pair of public key, and a private key to encrypt and decrypt messages when communicating.
    1. Symmetric Encryption is an age old technique while asymmetric Encryption is relatively new.
    2. Asymmetric Encryption was introduced to complement the inherent problem of the need to share the key in symmetric encryption model eliminating the need to share the key by using a pair of public-private keys.

17. What is meant by replay attack?
    A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

18. Define – Virus
    Computer Viruses is defined as the malicious software programs that damage computer program entering into the computer without the permission of the users, and also run against the wishes of the users. They are replicated by themselves. Viruses are so dangerous and malicious that they can be automatically copied and pasted from memory to memory over and over.
    Types of virus: Boot sector Virus, Macro virus, Multipartite Virus, Stealth virus

19. List out the design goals of firewalls.
    1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
    2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
    3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system.

20. What is a Firewall?
    A Firewall is a security system to protect an internal network from unauthorized servers and networks based on predefined rules. It acts as a barrier and only allows the secured network to send or receive data.

21. How does a Firewall work?
    A Firewall analyses the network traffic and filters it so that the unsecured and suspicious networks cannot attack the system. The point where information is exchanged with an external network is called a port.

22. What is application level gateway?
    An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

UNIT 5

1. Multimedia Applications:
   A multimedia application is interactive software that combines several types of media at once to convey information to an audience. Different types of media that can be used include: text. images (photographs, illustrations) audio (music, sounds)

2. Cloud Computation
   Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

3. Next Generation Internet Architecture
   Next Generation Network (NGN) refers to a packet-based network and it can be used for both telecommunication services as well as data and it supports mobility.

4. Green Communication Networks
   Green Communications and Networking introduces novel solutions that can bring about significant reductions in energy consumption in the information and communication technology (ICT) industry—as well as other industries, including electric power.

5. Data Center Networking
   Data center networking is the integration of a constellation of networking resources — switching, routing, load balancing, analytics, etc. — to facilitate the storage and processing of applications and data.

6. Give the applications of Multimedia?
   Document Imaging
   Image Processing and Image Recognition
   Full Motion Digital Video Applications
   Electronic messaging
   Entertainment
   Corporate Communications

7. Define Cloud Computing
   The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

8. What is the difference between parallel and distributed computing?

S.No.	Parallel Computing	Distributed Computing
1.	Many operations are performed simultaneously	System components are located at different locations
2.	Single computer is required	Uses multiple computers
3.	Multiple processors perform multiple operations	Multiple computers perform multiple operations
4.	It may have shared or distributed memory	It has only distributed memory

9. List any four Cloud Service Providers (CSP)
   - Amazon Web Services (AWS)
   - Microsoft Azure.
   - Google Cloud.
   - Salesforce

10. List the three types of service models available in cloud
    - Infrastructure-as-a-service (IaaS)
    - Platform-as-a-service (PaaS)
    - Software-as-a-service (SaaS)

11. Define Virtualization

    Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers). Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware.

12. List the four types of virtualization in cloud
    - Network virtualization
    - Storage virtualization
    - Desktop virtualization
    - Application virtualization

13. Define Internet Cloud

    An Internet cloud is envisioned as a public cluster of servers provisioned on demand to perform collective web services or distributed applications using data-center resources.

    ❖ Cloud Platform Design Goals

    ❖ Enabling Technologies for Clouds

    ❖ A Generic Cloud Architecture