(2½ Hours)

[Total Marks: 60]

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labelled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

I	**Choose the correct alternative and rewrite the entire sentence with the correct alternative. (30)**				
1.	_____ is a router that resides within the middle of the network rather than at its periphery.				
	a.	core router	**b.**	aggregation router	
	c.	central router	**d.**	edge router	
2.	The core network, also referred to as a _______.				
	a.	distribution network	**b.**	backbone network	
	c.	access network	**d.**	edge network	
3.	In times of congestion, _________ traffic will continue to supply a high load, and_____ traffic will be crowded off the internet.				
	a.	Elastic, inelastic	**b.**	**Inelastic, elastic**	
	c.	Elastic, real time	**d.**	real time ,elastic	
4.	Which of the following is/are true about SDN Controller?				
	a.	**Manages flow control to the switches/routers 'below' / 'above'**	**b.**	OpenFlow is used to communicate with the networking devices via southbound APIs	
	c.	It is used to collect information about networking devices using SNMP.	**d.**	It is used to collect information about hardware using SNMP.	
5.	What is true for North-bound interface in SDN?				
	a.	North-bound interface communicate traffic with lower plane in SDN.	**b.**	All automation and archestration of system takes place via north-bound inteface	
	c.	Communication between data plane and control plane happens via north-bound interface	**d.**	**The controller controls the packets through north-bound interface**	
6.	The ____plane provides the "intelligence" in designing routes, setting priority and routing policy parameters to meet QoS and QoE requirements and to cope with the shifting traffic patterns.				
	a.	application	**b.**	data	
	c.	control	**d.**	forwarding	

7.	_______ is an open source project dedicated to acceleration the adoption of standardized NFV elements. It will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and to ensure consistency, performance, and interoperability among multiple open source components.				
	a.	Tata Consultancy Services (TCS)	**b.**	**Open Platform for NFV**	
	c.	Alliance for Telecommunications Industry Solutions (ATIS)	**d.**	United Nation Environmental Protection (UNEP)	
8.	__________ is an open source software activity under the auspices of the Linux foundation. Its member companies provide resources to develop an SDN controller for a wide range of applications.				
	a.	Apache Tomcat	**b.**	Microsoft Teams	
	c.	SciPy	**d.**	**OpenDaylight**	
9.	The Open Networking Foundation (ONF) cites four general limitations of traditional network architectures _________________				
	a.	**Static, complex architecture, Inconsistent policies, Inability to scale and Vendor dependence**	**b.**	Adaptability, Automation, Maintainability, Model management, Mobility, Integrated security and On-demand scaling	
	c.	Atomicity, Consistency, Isolated and Durability	**d.**	Need, Requirement gathering, Analysis, design, testing, implementation and maintenance	
10.	To turn the concept of SDN into practical implementation, two requirements must be met:_____________________				
	a.	**• There must be a common logical architecture in all switches, routers, and other network devices to be managed by an SDN controller. • A standard, secure protocol is needed between the SDN controller and the network device.**	**b.**	• There must be a common logical architecture in all Cloud Servers to be managed by an NETWORK controller. • A standard, secure protocol is needed between the SDN controller and the network device.	
	c.	• There must be a common logical architecture in all switches, routers, and other network devices to be managed by an SDN controller. • A standard, secure protocol is needed between the CPU and the DATA LINK device.	**d.**	• There must be a common logical architecture in all APPLICATION LAYER PROGRAMS to be managed by an SDN controller. • A standard, insecure protocol is needed between the SDN controller and the network device.	
11.	The OpenFlow specification defines three types of tables in the logical switch architecture: ______________				
	a.	**flow table, group table and meter table**	**b.**	flow table, up table and down table	

	c.	router table, hub table and switch table	**d.**	data table, meta data table and control table
12.	OFPFF_SEND_FLOW_REM is a _____ in flow table.			
	a.	Memory Location	**b.**	**flag**
	c.	flow label	**d.**	flow status
13.	The NFV framework consists of ____ domains of operation			
	a.	Two	**b.**	**Three**
	c.	Four	**d.**	Five
14.	VNFM performs the following function			
	a.	Inventory of software (for example, hypervisors), computing, storage and network resources dedicated to NFV infrastructure	**b.**	Collection of information for capacity planning, monitoring, and optimization
	c.	Visibility into and management of the NFV infrastructure	**d.**	**Overall coordination and adaptation role for configuration and event reporting between the VIM and the EM.**
15.	_______provides the execution environment of a single VNFC instance.			
	a.	storage resource sharing	**b.**	Network resource sharing
	c.	**Virtual machine management and API**	**d.**	Control and admin agent
16.	______used for requests for VNF lifecycle management and exchange of configuration and state information.			
	a.	Or-Vnfm	**b.**	**Ve-Vnfm**
	c.	Or-Vi	**d.**	Os-Ma
17.	____ domain Provides commercial off-the-shelf (COTS) high-volume servers and storage			
	a.	**Compute**	**b.**	Hypervisor
	c.	Infrastructure network domain	**d.**	Functional
18.	VIM Performs the following			
	a.	**visibility into and management of the NFV infrastructure**	**b.**	instantiation feasibility checking, if required
	c.	instance assisted or automated healing	**d.**	lifecycle management change notification
19.	_________ is computed as a composite function of: the ability of the network to accept additional traffic; the "importance" of each user and the "utility" of his traffic; the data rate of each input transmission medium or the transducer used; and the tolerable delay time for delivery of the traffic.			
	a.	**Precedence**	**b.**	Dependence

	c.	Preference	**d.**	Independence
20.	QoS and QoE enable the network manager to determine whether_______________			
	a.	the netwoks cause delayed in the flow of the packet due to the jitter	**b.**	the networks becomes congested due to the overwhelmed flow of the packets
	c.	the network is behave as per users priority and to send the packet in the different routes of the networks	**d.**	**the network is meeting user needs and to diagnose problem areas that require adjustment to network management and network traffic control.**
21.	__________ classification permits a network operator to strictly limit the effect of LE traffic on best effort/normal or all other network traffic.			
	a.	Packers effort	**b.**	Known effort
	c.	High effort	**d.**	**Lower effort**
22.	In Architectural Framework for QoS Support,_________ refers to the assignment of packets to a traffic class by the ingress router at the ingress edge of the network.			
	a.	Congestion avoidance	**b.**	**Traffic classification**
	c.	Packet marking	**d.**	Traffic shaping
23.	In queue management is ____________, defined in RFC 2309 drops incoming packets probabilistically based on an estimated average queue size.			
	a.	adaptive random early detection	**b.**	weighted random early detection
	c.	**random early detection**	**d.**	Robust random early detection
24.	____________and_________ concerns monitoring the dynamic properties of a traffic stream using performance metrics such as data rate and packet loss rate.			
	a.	Traffic shaping , packaging	**b.**	Traffic marking , encoding
	c.	Traffic policing , decoding	**d.**	**Traffic metering , recording**
25.	A/An _______________ cloud provides service to customers in the form of software, specifically application software running on and accessible in the cloud.			
	a.	**Software as a Service**	**b.**	Platform as a Service
	c.	Infrastructure as a Service	**d.**	Storage as a Service
26.	A cloud consumer may request cloud services from a cloud provider directly or via a cloud ________.			
	a.	provider	**b.**	**broker**
	c.	auditor	**d.**	consumer
27.	___________responsible for connecting functional components in the architecture to create a unified architecture.			
	a.	**Integration**	**b.**	Operational support systems
	c.	Business support systems	**d.**	Development function

28.	CoAP is a specialized ________ transfer protocol for use with constrained nodes and constrained networks in the IoT.				
	a.	file	**b.**	program	
	c.	command	**d.**	**web**	
29.	_________creates groups, finds appropriate member things in the network, manages member presence, and makes group action easy.				
	a.	Protocol Plugin Manager	**b.**	Soft Sensor Manager	
	c.	**Things Manager**	**d.**	Control Manager	
30.	Which is not IoT system pillar of Cisco IoT System?				
	a.	Management and automation	**b.**	Network connectivity	
	c.	Fog computing	**d.**	**Data Manipulating**	

Answer Key :

1.a	**2.b**	**3.b**	**4.a**	**5.d**
6.c	**7.b**	**8.d**	**9.a**	**10.a**
11.a	**12.b**	**13.b**	**14.d**	**15.c**
16.b	**17.a**	**18.a**	**19.a**	**20.d**
21.d	**22.b**	**23.c**	**24.d**	**25.a**
26.b	**27.a**	**28.d**	**29.c**	**30.d**

II	Attempt ***any one*** of the following:		6
	a	Discuss the motivation for the typical network hierarchy of access Networks, distribution networks, and core networks.	

Ans : A Typical Network Hierarchy As below figure illustrates, enterprises often design their network facilities in a three-tier hierarchy: access, distribution, and core

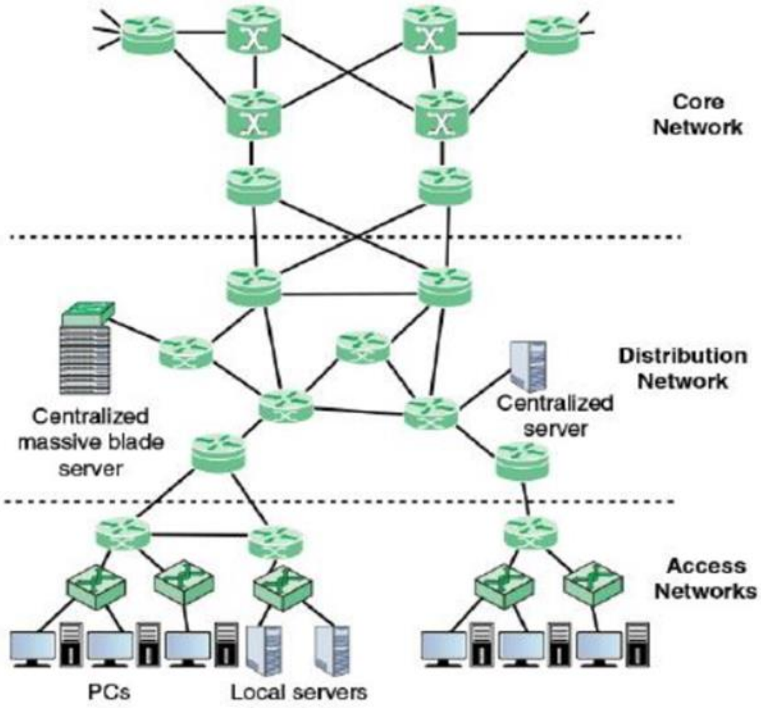


FIGURE 1.3 A Typical Network Hierarchy

Accessnetwork

A network that connects directly to the end user or customer. Closest to the end user is the access network.

Typically, an access network is a local-area network (LAN) or campus-wide network that consisting of LAN switches (typically Ethernet switches) and, in larger LANs, IP routers that provide connectivity among the switches.

Layer 3 switches (not shown) are also commonly used within an LAN. The access network supports end user equipment, such as desktop and laptop computers and mobile devices. A high-performance device for network routing. Layer 3 switches are very similar to routers. The key difference between L3 switches and routers is that a L3 switch replaces some of a router’s software logic with hardware to offer better performance. L3 switches often cost less than traditional routers.

The distribution network connects access networks with each other and with the core network. An edge router in the distribution network connects to an edge router in an access network to provide connectivity. The two routers are configured to recognize each other

		and will generally exchange routing and connectivity information and, typically, some traffic-related information. This cooperation between routers is referred to as peering. The distribution network also serves to aggregate traffic destined for the core router, which protects the core from high-density peering. That is, the use of a distribution network limits the number of routers that establish peer relationships with edge routers in the core, saving memory, processing, and transmission capacity. A distribution network may also directly connect servers that are of use to multiple access networks, such as database servers and network management servers. The core network, also referred to as a backbone network, connects geographically dispersed distribution networks as well as providing access to other networks that are not part of the enterprise network. Typically, the core network will use very high performance routers, high-capacity transmission lines, and multiple interconnected routers for increased redundancy and capacity. The core network may also connect to high-performance, high-capacity servers, such as large database servers and private cloud facilities. Some of the core routers may be purely internal, providing redundancy and additional capacity without serving as edge routers. core/backbone network A central network that provides networking services to attached distribution and access networks. Also referred to as a backbone network. A hierarchical network architecture is an example of a good modular design. With this design, the capacity, features, and functionality of network equipment (routers, switches, and network management servers) can be optimized for their position in the hierarchy and the requirements at a given hierarchical level.	
	b	Explain the concepts of network convergence and unified communications Network convergence refers to the provision of telephone, video and data communication services within a single network. You can think of this convergence in terms of a three-layer model of enterprise communications: Application convergence: These are seen by the end users of a business. Convergence integrates communications applications, such as voice calling (telephone), voice mail, e-mail, and instant messaging, with business applications, such as workgroup collaboration, customer relationship management, and backoffice functions. With convergence, applications provide rich features that incorporate voice, data, and video in a seamless, organized, and value-added manner. One example is multimedia messaging, which enables a user to use a single interface to access messages from a variety of sources (for example, office voice mail, email, SMS text messages, and mobile voice mail). Enterprise services: At this level, the manager deals with the information network in terms of the services that must be available to ensure that users can take full advantage of the applications that they use. For example, network managers need to make sure that appropriate privacy mechanisms and authentication services are in place to support convergence-based applications. They may also be able to track user locations to support remote print services and network storage facilities for mobile workers. Enterprise network management services may also include setting up collaborative environments for various users, groups, and applications and QoS provision. Infrastructure: The network and communications infrastructure consists of the communication links, LANs, WANs, and Internet connections available to the enterprise. Increasingly, enterprise network infrastructure also includes private/public cloud connections to data centers that host high-volume data	

		storage and web services. A key aspect of convergence at this level is the ability to carry voice, image, and video over networks that were originally designed to carry data traffic. Infrastructure convergence has also occurred for networks that were designed for voice traffic. For example, video, image, text, and data are routinely delivered to smartphone users over cell phone networks. UNIFIED COMMUNICATIONS A concept related to network convergence is unified communications (UC). Whereas enterprise network convergence focuses on the consolidation of traditionally distinct voice, video, and data communications networks into a common infrastructure, UC focuses on the integration of real-time communication services to optimize business processes. As with converged enterprise networks, IP is the cornerstone on which UC systems are built. Key elements of UC include the following: 1. UC system's typically provide a unified user interface and consistent user experience across multiple devices and media. 2. UC merges real-time communications services with non-real-time services and business process applications.	
	c	Write a Short Note on i) Quality of Service You can define QoS as the measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a service level agreement (SLA) between a user and a service provider, so as to satisfy specific customer application requirements. Commonly specified properties include the following: Throughput: A minimum or average throughput, in bytes per second or bits per second, for a given logical connection or traffic flow. Delay: The average or maximum delay. Also called latency. Packet jitter: Typically, the maximum allowable jitter. Error rate: Typically maximum error rate, in terms of fraction of bits delivered in error. Packet loss: Fraction of packets lost. Priority: A network may offer a given number of levels of priority. The assigned level for various traffic flows influences the way in which the different flows are handled by the network. Availability: Expressed as a percentage of time available. Security: Different levels or types of security may be defined. QoS mechanisms ensure that business applications continue to receive the necessary performance guarantee even though they no longer run on dedicated hardware, such as when applications are transferred to a cloud. The QoS provided by an infrastructure is partially determined by its overall performance and efficiency. ii) Quality of Experience QOE is a subjective measure of performance as reported by the user. Unlike QOS, which can be precisely measured, QOE relies on human opinion. QOE is important particularly when we deal with multimedia applications and multimedia content delivery. QOS provides measurable, quantitative targets that guide the design	

and operation of a network and enable customer and provider to agree on what quantitative performance the network will deliver for give applications and traffic flows. However, QOS processes by themselves are not sufficient in that they do not take into account the user's perception of network performance and service quality. Although the maximum capacity may be fixed at a certain value by a media transmission system, this does not necessarily fix the quality of the multimedia content at, say, "high." This is because there are numerous ways the multimedia content could have been encoded, giving rise to differing perceived qualities.

There is a wide range of factors and features that can be included in a requirement for QOE, which can, roughly,
be classified into the following categories:

Perceptual: This category encompasses the quality of the sensory aspects of the user experience. For video, examples include sharpness, brightness, contrast, flicker, and distortion. Audio examples include clarity and timbre.

Psychological: This category deals with the user's feeling about the experience. Examples include ease of use, joy of use, usefulness, perceived quality, satisfaction, annoyance, and boredom.

Interactive: This category deals with aspects of an experience related to the interaction between the user and the application or device, such as responsiveness, naturalness of interaction, communication efficiency, and accessibility.

2 Attempt *any one* of the following: **6**

a Why traditional network architecture are inadequate for transmission for carried a data? How this limitation are solved?

Ans : Traditional Network Architectures are Inadequate

Even with the greater capacity of transmission schemes and the greater performance of network devices, traditional network architectures are increasingly inadequate in the face of the growing complexity, variability, and high volume of the imposed load. In addition, as quality of service (QoS) and quality of experience (QoE) requirements imposed on the network are expanded as a result of the variety of applications, the traffic load must
be handled in an increasingly sophisticated and agile fashion.

The traditional internetworking approach is based on the TCP/IP protocol architecture. Three noteworthy characteristics of this approach are as follows:

1. Two-level end system addressing
2. Routing based on destination
3. Distributed, autonomous control

The traditional architecture relies heavily on the network interface identity. At the physical layer of the TCP/IP model, devices attached to networks are identified by hardware-based identifiers, such as Ethernet MAC addresses. At the internetworking level, including both the Internet and private internets, the architecture is a network of networks. Each attached device has a physical layer identifier recognized within its immediate network and a logical network identifier, its IP address, which provides global visibility. The design of TCP/IP uses this addressing scheme to support the networking of autonomous networks, with distributed control. This architecture provides a high level of resilience and scales well in

terms of adding new networks. Using IP and distributed routing protocols, routes can be discovered and used throughout an internet. Using transport-level protocols such as TCP, distributed and decentralized algorithms can be implemented to
respond to congestion. Traditionally, routing was based on each packet's destination address. In this datagram approach, successive
packets between a source and destination may follow different routes through the internet, as routers constantly seek to find the minimum-delay path for each individual packet. More recently, to satisfy QoS requirements, packets are often treated in terms of flows of packets. Packets associated with a given flow have defined QoS characteristics, which affect the routing for the entire flow.
However, this distributed, autonomous approach developed when networks were predominantly static and end systems predominantly of fixed location. Based on these characteristics, the Open Networking Foundation (ONF)
cites four general limitations of traditional network architectures.
i. Static, complex architecture: To respond for demands such as differing levels of QoS, high and fluctuating traffic volumes, and security requirements, networking technology has grown more complex and difficult to manage. This has resulted in a number of independently defined protocols each of which addresses a portion of networking requirements
ii. Inconsistent policies: To implement a network-wide security policy, staff may have to make configuration changes to thousands of devices and mechanisms. In a large network, when a new virtual machine is activated, it can take hours or even days to reconfigure ACLs across the entire
network.
iii. Inability to scale: Demands on networks are growing rapidly, both in volume and variety. Adding more switches and transmission capacity, involving multiple vendor equipment, is difficult because of the complex, static nature of the network.
iv. Vendor dependence: Given the nature of today's traffic demands on networks, enterprises and carriers need to deploy new capabilities and services rapidly in response to changing business needs and user demands. A lack of open interfaces for network functions leaves the enterprises limited by the relatively slow product cycles of vendor equipment.

Requirements

The Open Data Center Alliance (ODCA) provides a useful, concise list of the principal requirements for a modern networking approach, which include the following:
Adaptability: Networks must adjust and respond dynamically, based on application needs, business policy, and network conditions.
Automation: Policy changes must be automatically propagated so that manual work and errors can be reduced.
Maintainability. Introduction of new features and capabilities (software upgrades, patches) must be seamless with minimal disruption of operations.
Model management: Network management software must allow management of the network at a model level, rather than implementing conceptual changes by reconfiguring individual network elements.
Mobility: Control functionality must accommodate mobility, including mobile user devices and virtual servers.
Integrated security: Network applications must integrate seamless security as a core service instead of as an add-on solution.

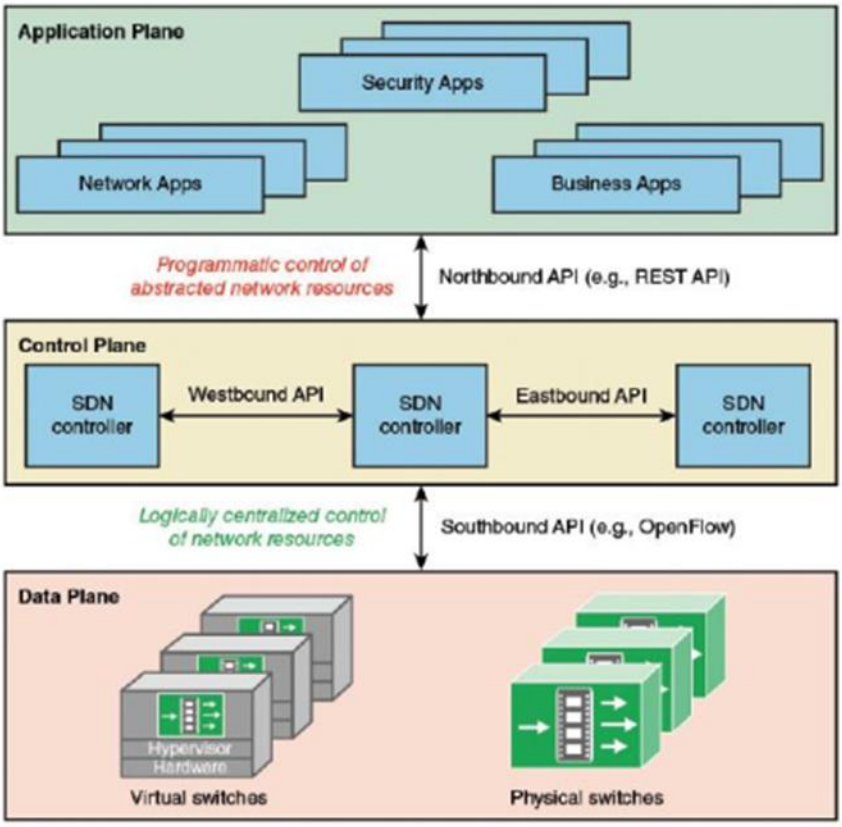
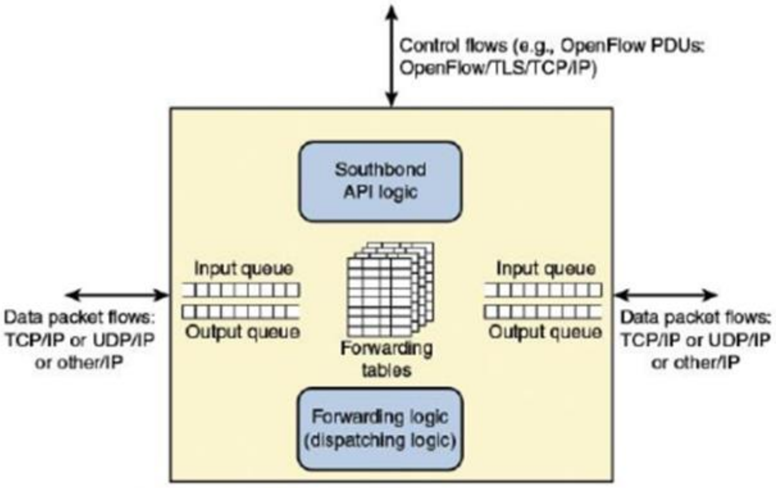
		On-demand scaling: Implementations must have the ability to scale up or scale down the network and its services to support on-demand requests.	
	b	Explain the Software-Defined Architecture. Ans : SDN Architecture An analogy can be drawn between the ways in which computing evolved from closed, vertically integrated, proprietary systems into an open approach to computing and the evolution coming with SDN In the early decades of computing, vendors such as IBM and DEC provided a fully integrated product, with a proprietary processor hardware, unique assembly language, unique operating system (OS), and the bulk if not all of the application software. In this environment, customers, especially large customers, tended to be locked in to one vendor, dependent primarily on the applications offered by that vendor. Migration to another vendor's hardware platform resulted in major upheaval at the application level. The central concept behind SDN is to enable developers and network managers to have the same type of control over network equipment that they have had over x86 servers. The SDN approach splits the switching function between a data plane and a control plane that are on separate devices.The data plane is simply responsible for forwarding packets, whereas the control plane provides the "intelligence" in designing routes, setting priority and routing policy parameters to meet QoS and QoE requirements and to cope with the shifting traffic patterns. Open interfaces are defined so that the switching hardware presents a uniform interface regardless of the details of internal implementation. Similarly, open interfaces are defined to enable networking applications to communicate with the SDN controllers.  *FIGURE 3.3 Software-Defined Architecture*	

		Figure 3.3 showing more detail of the SDN approach. The data plane consists of physical switches and virtual switches. In both cases, the switches are responsible for forwarding packets. The internal implementation of buffers, priority parameters, and other data structures related to forwarding can be vendor dependent. However, each switch must implement a model, or abstraction, of packet forwarding that is uniform and open to the SDN controllers. This model is defined in terms of an open application programming interface (API) between the control plane and the data plane (southbound API).	
	c	What is SDN data plane? Explain the different types of functions performed by the data plane network devices. Ans : SDN DATA PLANE The SDN data plane, referred to as the resource layer in ITU-T Y.3300 and also often referred to as the infrastructure layer, is where network forwarding devices perform the transport and processing of data according to decisions made by the SDN control plane. The important characteristic of the network devices in an SDN network is that these devices perform a simple forwarding function, without embedded software to make autonomous decisions. Data Plane Functions Figure 4.2 illustrates the functions performed by the data plane network devices (also called data plane network elements or switches). The principal functions of the network device are the following:  **FIGURE 4.2** Data Plane Network Device Control support function: Interacts with the SDN control layer to support programmability via resourcecontrol interfaces. The switch communicates with the controller and the controller manages the switch via the OpenFlow switch protocol. Data forwarding function: Accepts incoming data flows from other network devices and end systems and forwards them along the data forwarding paths that have been computed and established according to the rules defined by the SDN applications.	

		These forwarding rules used by the network device are embodied in forwarding tables that indicate for give categories of packets what the next hop in the route should be. In addition to simple forwarding of a packet, the network device can alter the packet header before forwarding, or discard the packet. As shown, arriving packets may be placed in an input queue, awaiting processing by the network device, and forwarded packets are generally placed in an output queue, awaiting transmission. The network device in Figure 4.2 is shown with three I/O ports: one providing control communication with an SDN controller, and two for the input and output of data packets. This is a simple example. The network device may have multiple ports to communicate with multiple SDN controllers, and may have more than two I/O ports for packet flows into and out of the device.	
3	**Attempt <u>*any one*</u> of the following:**		**6**
	a	What is Network functions virtualization (NFV)? Explain the key benefits of NFV. Ans : Network functions virtualization (NFV) is the virtualization of network functions by implementing these functions in software and running them on VMs. NFV decouples network functions, such as Network Address Translation (NAT), firewalling, intrusion detection, Domain Name Service (DNS), and caching, from proprietary hardware appliances so that they can run in software on VMs. NFV builds on standard VM technologies, extending their use into the networking domain. • Network function devices: Such as switches, routers, network access points, customer premises equipment (CPE), and deep packet inspectors • Network-related compute devices: Such as firewalls, intrusion detection systems, and network management systems. • Network-attached storage: File and database servers attached to the network. In traditional networks, all devices are deployed on proprietary/closed platforms. All network elements are enclosed boxes, and hardware cannot be shared. Each device requires additional hardware for increased capacity, but this hardware is idle when the system is running below capacity. With NFV, however, network elements are independent applications that are flexibly deployed on a unified platform comprising standard servers, storage devices, and switches. In this way, software and hardware are decoupled, and capacity for each application is increased or decreased by adding or reducing virtual resources NFV Benefits The following are the most important potential benefits: • Reduced CapEx, by using commodity servers and switches, consolidating equipment, exploiting economies of scale, and supporting pay-as-you grow models to eliminate wasteful overprovisioning. • Reduced OpEx, in terms of power consumption and space usage, by using commodity servers and switches, consolidating equipment, and exploiting economies of scale, and reduced network management and control expenses. Reduced CapeX and OpEx are perhaps the main drivers for NFV. • The ability to innovate and roll out services quickly, reducing the time to deploy new networking services to support changing business requirements, seize new market opportunities, and improve return on investment of new services. Also lowers the risks	

associated with rolling out new services, allowing providers to easily trial and evolve services to determine what best meets the needs of customers.

- Ease of interoperability because of standardized and open interfaces.
- Use of a single platform for different applications, users and tenants. This allows network operators to share resources across services and across different customer bases.
- Provided agility and flexibility, by quickly scaling up or down services to address changing demands.
- Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required.
- A wide variety of ecosystems and encourages openness. It opens the virtual appliance market to pure software entrants, small players and academia, encouraging more innovation to bring new services and new revenue streams quickly at much lower risk.

b Explain the elements of the NFV infrastructure and their interrelationships.

Ans: Figure 7.8 shows a more detailed look at the ISG NFV reference architectural framework. You can view this architecture as consisting of four major blocks.

• NFV infrastructure (NFVI): Comprises the hardware and software resources that create the environment in which VNFs are deployed. NFVI virtualizes physical computing, storage, and networking and places them into resource pools

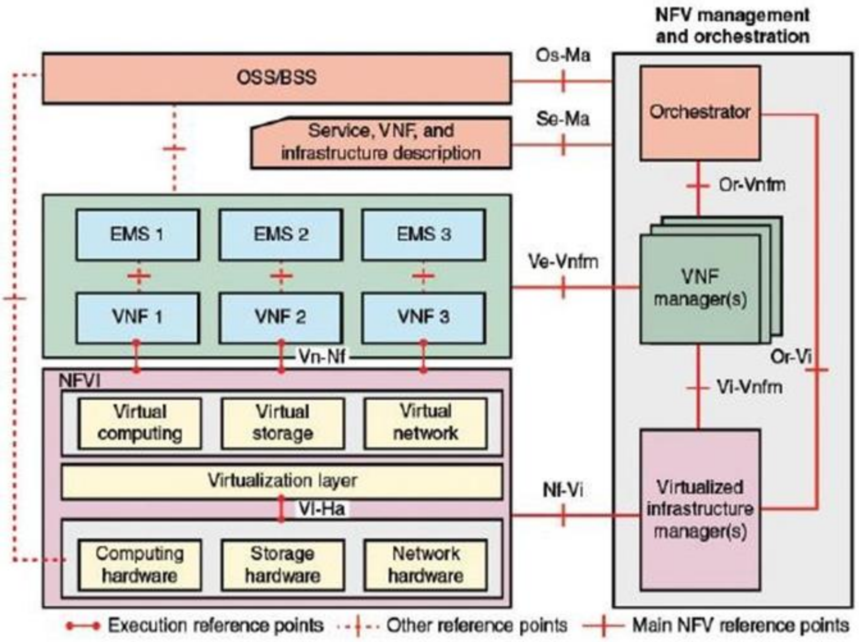


FIGURE 7.8 NFV Reference Architectural Framework

• VNF/EMS: The collection of VNFs implemented in software to run on virtual computing, storage, and networking resources, together with a collection of element management systems (EMS) that manage the VNFs.

• NFV management and orchestration (NFV-MANO): Framework for the management and orchestration of all resources in the NFV environment. This includes computing, networking, storage, and VM resources.

•OSS/BSS: Operational and business support systems implemented by the VNF service provider.
It is also useful to view the architecture as consisting of three layers. The NFVI together with the virtualized infrastructure manager provide and manage the virtual resource environment and its underlying physical resources. The VNF layer provides the software implementation of network functions, together with element management systems and one or more VNF managers. Finally, there is a management, orchestration, and control layer consisting of OSS/BSS and the
NFV orchestrator.

NFV Management and Orchestration
The NFV management and orchestration facility includes the following functional blocks:
•NFV orchestrator: Responsible for installing and configuring new network services (NS) and virtual network function (VNF) packages, NS lifecycle management, global resource management, and validation and authorization of NFVI resource requests.
•VNF manager: Oversees lifecycle management of VNF instances.
•Virtualized infrastructure manager: Controls and manages the interaction of a VNF with computing, storage, and network resources under its authority, in addition to their virtualization

Reference Points
The main reference points include the following considerations:
•Vi-Ha: Marks interfaces to the physical hardware. A well-defined interface specification will facilitate for operators sharing physical resources for different purposes, reassigning resources for different purposes, evolving software and hardware independently, and obtaining software and hardware component from different vendors.
•Vn-Nf: These interfaces are APIs used by VNFs to execute on the virtual infrastructure. Application developers, whether migrating existing network functions or developing new VNFs, require a consistent interface the provides functionality and the ability to specify performance, reliability, and scalability requirements.
•Nf-Vi: Marks interfaces between the NFVI and the virtualized infrastructure manager (VIM). This interface can facilitate specification of the capabilities that the NFVI provides for the VIM. The VIM must be able to manage all the NFVI virtual resources, including allocation, monitoring of system utilization, and fault management.
•Or-Vnfm: This reference point is used for sending configuration information to the VNF manager and collecting state information of the VNFs necessary for network service lifecycle management.
•Vi-Vnfm: Used for resource allocation requests by the VNF manager and the exchange of resource configuration and state information.
•Or-Vi: Used for resource allocation requests by the NFV orchestrator and the exchange of resource configuration and state information.
•Os-Ma: Used for interaction between the orchestrator and the OSS/BSS systems.
•Ve-Vnfm: Used for requests for VNF lifecycle management and exchange of configuration and state information.
•Se-Ma: Interface between the orchestrator and a data set that provides information regarding the VNF deployment template, VNF forwarding graph, service-related information, and NFV infrastructure information models.

	c	Write a short note on virtual local-area network (VLAN). Ans: Ans: a virtual local-area network (VLAN) is a logical subgroup within a LAN that is created by software rather than by physically moving and separating devices. It combines user stations and network devices into a single broadcast domain regardless of the physical LAN segment they are attached to and allows traffic to flow more efficiently within populations of mutual interest. The VLAN logic is implemented in LAN switches and functions at the MAC layer. Because the objective is to isolate traffic within the VLAN, a router is required to link from one VLAN to another. Routers can be implemented as separate devices, so that traffic from one VLAN to another is directed to a router, or the router logic can be implemented as part of the LAN switch, as shown in Figure 9.3. VLANs enable any organization to be physically dispersed throughout the company while maintaining its group identity. For example, accounting personnel can be located on the shop floor, in the research and development center, in the cash disbursement office, and in the corporate offices, while all members reside on the same virtual network, sharing traffic only with each other. Figure 9.3 shows five defined VLANs. A transmission from workstation X to server Z is within the same VLAN, so it is efficiently switched at the MAC level. A broadcast MAC frame from X is transmitted to all devices in all portions of the same VLAN. But a transmission from X to printer Y goes from one VLAN to another. Accordingly, router logic at the IP level is required to move the IP packet from X to Y. Figure 9.3 shows that logic integrated into the switch, so that the switch determines whether the incoming MAC frame is destined for another device on the same VLAN. If not, the switch routes the enclosed IP packet at the IP level.	

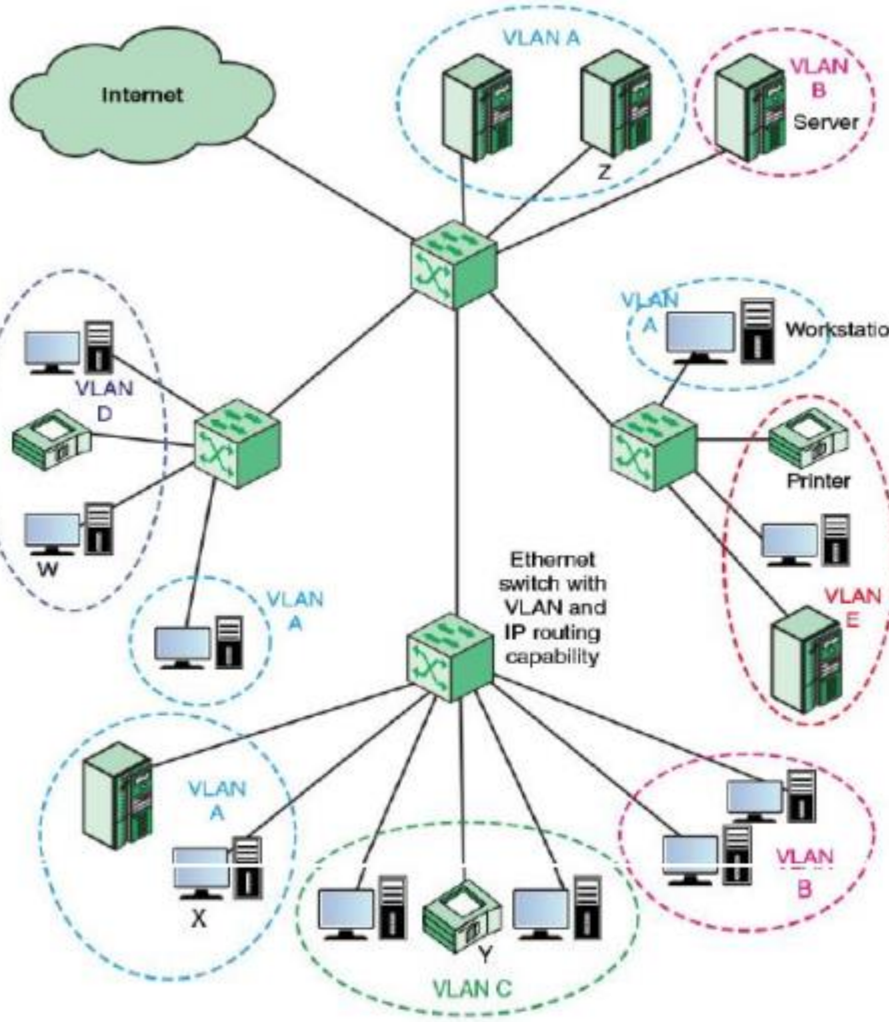


FIGURE 9.3 A VLAN Configuration

A VLAN is a broadcast domain consisting of a group of end stations, perhaps on multiple physical LAN segments, that are not constrained by their physical location and can communicate as if they were on a common LAN. A number of different approaches have been used for defining membership, including the following:

•Membership by port group: Each switch in the LAN configuration contains two types of ports: a trunk port, which connects two switches; and an end port, which connects the switch to an end system. A VLAN can be defined by assigning each end port to a specific VLAN. This approach has the advantage that it is relatively easy to configure. The principle disadvantage is that the network manager must reconfigure VLAN membership when an end system moves from one port to another.

•Membership by MAC address: Because MAC layer addresses are hardwired into the workstation's network interface card (NIC), VLANs based on MAC addresses enable network managers to move a workstation to a different physical location on the network and have that workstation automatically retain its VLAN membership. The main problem with this method is that VLAN membership must be assigned initially. In networks with thousands of users, this is no easy task. Also, in environments where notebook PCs are used, the MAC address is associated with the docking station and not with the notebook

PC. Consequently, when a notebook PC is moved to a different docking station, its VLAN membership must be reconfigured.

•Membership based on protocol information: VLAN membership can be assigned based on IP address, transport protocol information, or even higher-layer protocol information. This is a quite flexible approach, but it does require switches to examine portions of the MAC frame above the MAC layer, which may have a performance impact.

4 Attempt *<u>any one</u>* of the following: 6

a Explain the concept of differentiated services.

Ans: The differentiated services (DiffServ) architecture is designed to provide a simple, easy-to- implement, low- overhead tool to support a range of network services that are differentiated on the basis of performance. Several key characteristics of DiffServ contribute to its efficiency and ease of deployment:

•IP packets are labeled for differing QoS treatment using the existing IPv4 or IPv6 DSField. Thus, no change is required to IP.

•A service level specification (SLS) is established between the service provider (Internet domain) and the customer prior to the use of DiffServ. This avoids the need to incorporate DiffServ mechanisms in applications. Therefore, existing applications need not be modified to use DiffServ. The SLS is a set of parameters and their values that together define the service offered to a traffic stream by a DiffServ domain.

•A traffic conditioning specification (TCS) is a part of the SLS that specifies traffic classifier rules and any corresponding traffic profiles and metering, marking, discarding/shaping rules which are to apply to the traffic stream.

•DiffServ provides a built-in aggregation mechanism. All traffic with the same DiffServ octet is treated the same by the network service. For example, multiple voice connections are not handled individually but in the aggregate. This provides for good scaling to larger networks and traffic loads.

•DiffServ is implemented in individual routers by queuing and forwarding packets based on the DiffServ octet. Routers deal with each packet individually and do not have to save state information on packet flows.

Services

The DiffServ type of service is provided within a DiffServ domain, which is defined as a contiguous portion of the Internet over which a consistent set of DiffServ policies are administered. Typically, a DiffServ domain would be under the control of one administrative entity. The services provided across a DiffServ domain are defined in an SLA, which is a service contract between a customer and the service provider that specifies the forwarding service that the customer should receive for variousExplain the concept of differentiated services.

Ans: The differentiated services (DiffServ) architecture is designed to provide a simple, easy-to- implement, low- overhead tool to support a range of network services that are differentiated on the basis of performance. Several key characteristics of DiffServ contribute to its efficiency and ease of deployment:

•IP packets are labeled for differing QoS treatment using the existing IPv4 or IPv6 DSField. Thus, no change is required to IP.

•A service level specification (SLS) is established between the service provider (Internet domain) and the customer prior to the use of DiffServ. This avoids the need to incorporate

		DiffServ mechanisms in applications. Therefore, existing applications need not be modified to use DiffServ. The SLS is a set of parameters and their values that together define the service offered to a traffic stream by a DiffServ domain. •A traffic conditioning specification (TCS) is a part of the SLS that specifies traffic classifier rules and any corresponding traffic profiles and metering, marking, discarding/shaping rules which are to apply to the traffic stream. •DiffServ provides a built-in aggregation mechanism. All traffic with the same DiffServ octet is treated the same by the network service. For example, multiple voice connections are not handled individually but in the aggregate. This provides for good scaling to larger networks and traffic loads. •DiffServ is implemented in individual routers by queuing and forwarding packets based on the DiffServ octet. Routers deal with each packet individually and do not have to save state information on packet flows. Services The DiffServ type of service is provided within a DiffServ domain, which is defined as a contiguous portion of the Internet over which a consistent set of DiffServ policies are administered. Typically, a DiffServ domain would be under the control of one administrative entity. The services provided across a DiffServ domain are defined in an SLA, which is a service contract between a customer and the service provider that specifies the forwarding service that the customer should receive for various classes of packets. A customer may be a user organization or another DiffServ domain. Once the SLA is established, the customer submits packets with the DiffServ octet marked to indicate the packet class. The service provider must ensure that the customer gets at least the agreed QoS for each packet class. To provide that QoS, the service provider must configure the appropriate forwarding policies at each router and must measure the performance being provided for each class on an ongoing basis. A DiffServ framework document lists the following detailed performance parameters that might be included in an SLA: •Detailed service performance parameters such as expected throughput, drop probability, and latency. •Constraints on the ingress and egress points at which the service is provided, indicating the scope of the service. •Traffic profiles that must be adhered to for the requested service to be provided, such as token bucket parameters. •Disposition of traffic submitted in excess of the specified profile. •The framework document also gives some examples of services that might be provided: •Traffic offered at service level A will be delivered with low latency. •Traffic offered at service level B will be delivered with low loss. •90 percent of in-profile traffic delivered at service level C will experience no more than 50 ms latency. •95 percent of in-profile traffic delivered at service level D will be delivered. •Traffic offered at service level E will be allotted twice the bandwidth of traffic delivered at service level F. Traffic with drop precedence X has a higher probability of delivery than traffic with drop precedence Y.	
	b	With the help of diagram, Explain the QoE/QoS Layered Model. Ans: The QoE/QoS Layered Model	

The QoE/QoS layered approach does not ignore the QoS aspect of the network, but instead, user and service level perspectives are complementary, as shown in Figure 11.4.

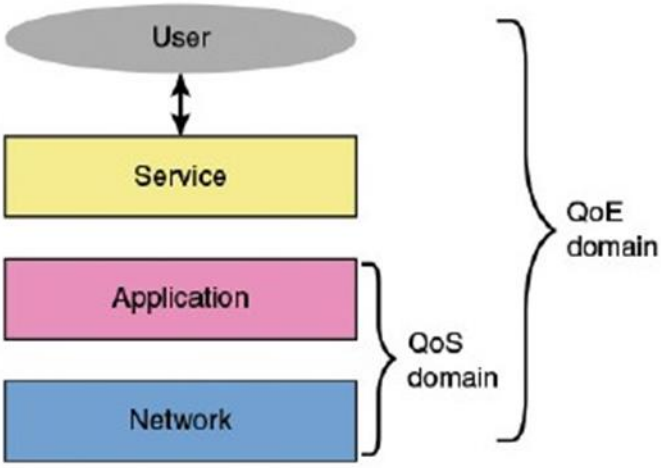


FIGURE 11.4 QoE/QoS Layered Model with the Domains of Interest for the Frameworks

The levels in the layered approach are as follows:

•User: The user interacts with the service. It is their degree of delight or annoyance from using the service that is to be measured. Being linked to human perception, QoE is hard to describe in a quantitative way, and it varies from person to person. The complexities of QoE at the user level stem from the differences between individual user characteristics, of which some might be time-varying, whereas others are of a relatively stable nature. The current practice in any QoE measurement is to identify and control for the relatively stable characteristics of a user in a way that is satisfactory to at least a large proportion of the potential user group.

•Service: The service level provides a virtual level where the user's experience of the overall performance of the service can be measured. It is the interface where the user interacts with the service (for example, the visual display to the user). It is also where tolerance thresholds are measured. As an illustration, the QoE measures from the user perspective for streaming applications could be startup time, audio/visual quality, channel change delay, and buffering interruptions.

•Application-level QoS (AQoS): AQoS deals with the control of application-specific parameters such as content resolution, bit rate, frame rate, color depth, codec type, layering strategy, and sampling rate. The network capacity often dictates the bandwidth that will be allocated to a service for transmission. Because of this fixed underlying resource, some parameters at the application level are usually adjusted and controlled to achieve a desired quality level.

•Network-level QoS (NQoS): This level is concerned with the low-level network parameters such as service coverage, bandwidth, delay, throughput, and packet loss. There are a number of ways in which network-level QoS parameters impact QoE. One such way is via network delay, which impacts QoE especially for interactive services. For instance, the interactive nature of web browsing that requires multiple retrieval events within a certain window of time might be affected by delay variations of the network. Voice over IP (VoIP) services might have stringent response-time demands, whereas e-mail services might tolerate much longer delays.

Although the trade-offs between quality and network capacity may begin with application-level QoS because of network capacity considerations, an understanding of the user requirements at the service level (that is, in terms QoE measures) would enable a better choice of application-level QoS parameters to be mapped onto the network- level QoS parameters.

c Explain the Black-Box Media-Based QoS/QoE Mapping Models.

Ans : Black-box media-based quality models rely on the analysis of media gathered at system entrance and exit. Hence, they account implicitly for the characteristics of examined media processing system. They are classified into two categories:

a.Double-sided or full-reference quality models: They use as inputs the clean stimulus and the corresponding degraded stimulus. They compare the clean and degraded stimulus in a perceptual domain that accounts for psychophysics capability of human sensory system. The perceptual domain is a transformation of traditional physical temporal and frequency domains performed according to characteristics of users perceptions. Basically, the larger the perceptual distance, the greater the degradation level. This model needs to align clean and degraded stimulus because the comparison is made on per-block basis. The stimulus alignment should be realized autonomously, that is, without adding extra control information describing stimulus structure.

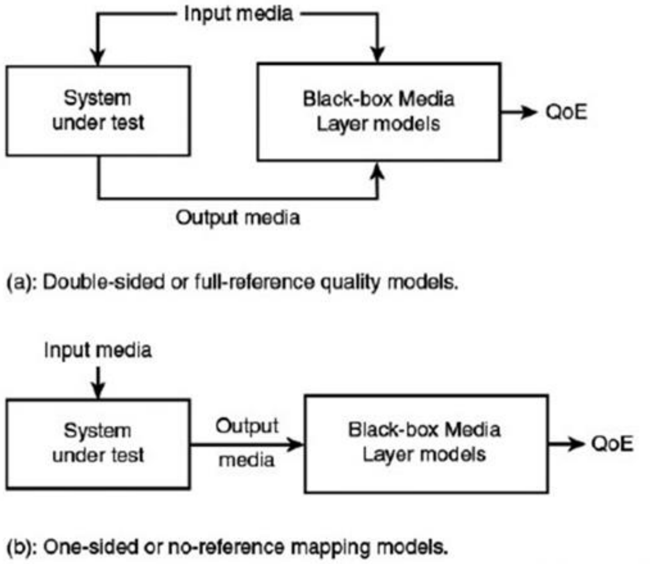


FIGURE 12.1 Black-Box Media-Based QoS/QoE Mapping Models

b. One-sided or no-reference quality models: They rely solely on the degraded stimulus to estimate the final QoE values. They parse the degraded stimulus to extract the observed distortions, which are dependent on the media type, for example, audio, image and video. As an example, artifacts extracted from audio stimulus include whistle, circuit noises, echoes, level saturation, clapping, interruptions, and pauses. The gathered distortions are adequately combined and transformed to compute the QoE values.

The main advantage of black-box quality models resides in their ability to measure QoE values using information gathered at the periphery of a given media processing system. Hence, they may be used in a generic fashion over different infrastructures and technologies. Moreover, it enables enhancing unconditionally quality models, that is,

		independently of technical and ethical constraint related to the measurement processes. Furthermore, black- box quality models may easily operate on either per-user or per-content basis. The main shortcoming of black-box quality models resides in the requirements to access the final representation of stimulus, which is often inaccessible in practice for privacy reasons. Moreover, full-reference quality models use clean stimulus as inputs that is often unavailable or hardly accessible at the system output. The full-reference black-box quality models are widely used for onsite benchmarking, diagnosis, and tuning of network equipments, where clean stimulus is available. The black-box quality models are used offline for the evaluation of application-layer components, such as codec, packet loss concealment (PLC), and buffering schemes.	
5	**Attempt *any one* of the following:**		**6**
	a	Write a short note on the NIST Cloud Computing Reference Architecture Ans: The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. Cloud Computing Actors The reference architecture depicted in Figure 13.4 defines five major actors in terms of the roles and responsibilities, as defined in the list that follows. •Cloud consumer: A person or organization that maintains a business relationship with and uses services from cloud providers. •Cloud provider (CP): A person, organization, or entity responsible for making a service available to interested parties. •Cloud auditor: A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation. •Cloud broker: An entity that manages the use, performance and delivery of cloud services and negotiates relationships between CPs and cloud consumers. •Cloud carrier: An intermediary that provides connectivity and transport of cloud services from CPs to cloud consumers. To summarize, a cloud provider can provide one or more of the cloud services to meet IT and business requirements of cloud consumers. For each of the three service models (SaaS, PaaS, IaaS), the CP provides the storage and processing facilities needed to support that service model, together with a cloud interface for cloud service consumers. The cloud carrier is a networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs. Typically, a CP will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and CPs.	

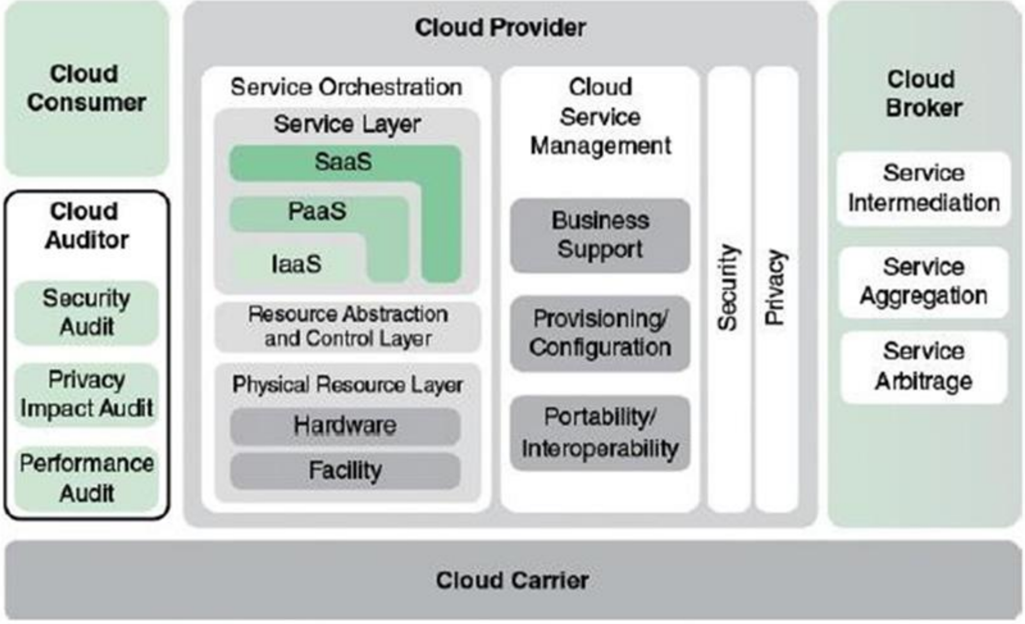


FIGURE 13.4 NIST Cloud Computing Reference Architecture

A cloud broker is useful when cloud services are too complex for a cloud consumer to easily manage. Three areas of support can be offered by a cloud broker.
A cloud auditor can evaluate the services provided by a CP in terms of security controls, privacy impact, performance, and so on. The auditor is an independent entity that can assure that the CP conforms to a set of standards.
Figure 13.5 illustrates the interactions between the actors. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information. This figure shows that cloud networking issues in fact involve three separate types of networks.

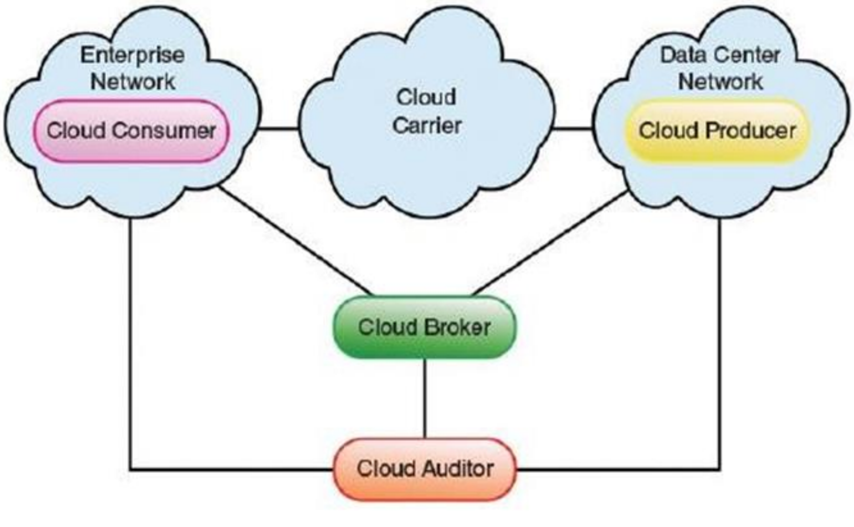


FIGURE 13.5 Interactions Between Actors in Cloud Computing

b Write a short note on:

Sensors

A sensor measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal. In both cases, the sensor output is typically input to a microcontroller or other management element.

The left side of Figure 14.2, shows the interface between a sensor and the controller for that sensor. A sensor may take the initiative in sending sensor data to the controller, either periodically or when a defined threshold is crossed; this is the active mode. Alternatively, or in addition, the sensor may operate in the passive mode, providing data when requested by the controller.

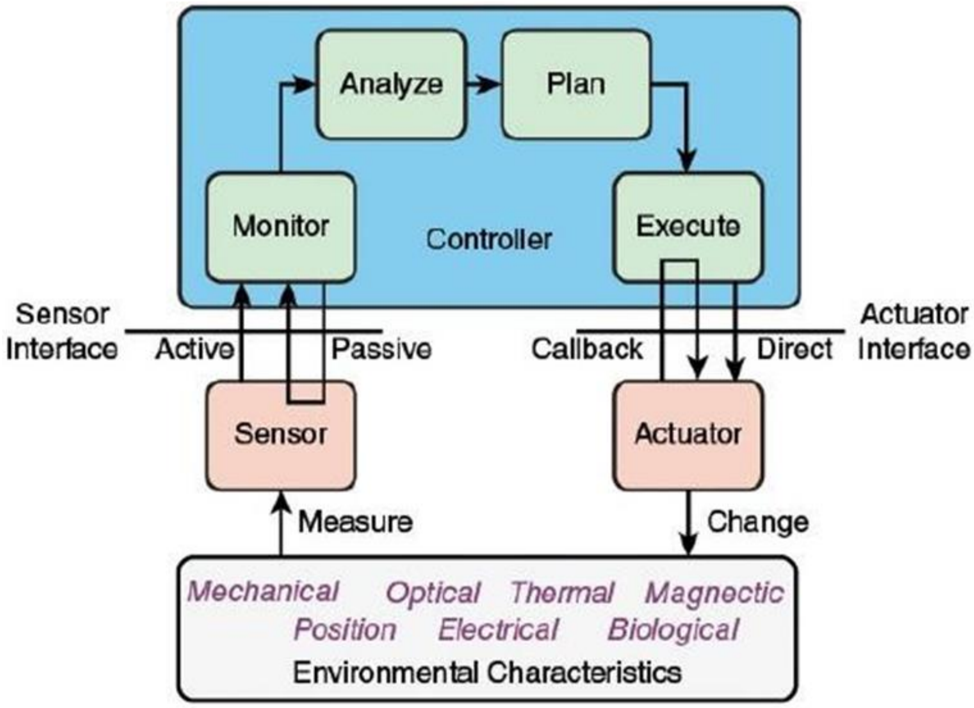


FIGURE 14.2 Interfaces for Sensors and Actuators

Types of Sensors

The variety of sensors used in IoT deployments is huge. Sensors may be extremely tiny, using nanotechnology, or quite substantial, such as a surveillance camera. Sensors may be deployed individually or in very small numbers on the one hand, or in large numbers on the other. Various types of sensors are.

Category	What It Does	Device Examples
Position measuring devices	Designed to detect and respond to changes in angular position or in linear position of the device	Potentiometer, linear position sensor, hall effect position sensor, magnetoresistive angular, encoders (quadrature, incremental rotary, absolute rotary, optical)
Proximity, motion sensors	Designed to detect and respond to movement outside of the component but within the range of the sensor	Ultrasonic proximity, optical reflective, optical slotted, PIR (passive infrared), inductive proximity, capacitive proximity, reed switch, tactile switch
Inertial devices	Designed to detect and respond to changes in the physical movement of the sensor	Accelerometer, potentiometer, inclinometer, gyroscope, vibration sensor/switch, tilt sensor, Piezo shock sensor, LVDT/RVDT
Pressure/force	Designed to detect a force being exerted against it	IC barometer, strain gauge, pressure potentiometer, LVDT, silicon transducer, Piezoresistive sensor, capacitive transducer
Optical devices	Designed to detect the presence of light or a change in the amount of light on the sensor	LDR, photodiodes, phototransistors, photo interrupters, reflective sensors, IrDA transceiver, solar cells, LTV (light voltage) sensors
Image, camera devices	Designed to detect and change a viewable image into a digital signal	CMOS image sensor
Magnetic devices	Designed to detect and respond to the presence of a magnetic field	Hall effect sensor, magnetic switch, linear compass IC, Reed sensor
Media devices	Designed to detect and respond to the presence or the amount of a physical substance on the sensor	Gas, smoke, humidity, moisture, dust, float level, fluid flow
Current and voltage devices	Designed to detect and respond to changes in the flow of electricity in a wire or circuit	Hall effect current sensor, DC current sensor, AC current sensor, voltage transducer
Temperature	Designed to detect the amount of heat using different techniques and in different mediums	Thermistor NTC, thermistor PTC, resistance temp detectors (RTD)s, thermocouple, thermopile, digital IC, analog IC, infrared thermometer/pyrometer
Specialized	Designed to provide detection, measurement, or response in specialized situations, which also may include multiple functions	Audio Microphone, Geiger-Müller tube, chemical

TABLE 14.2 Types of Sensors

RFID

Radio-frequency identification (RFID) technology, which uses radio waves to identify items, is increasingly becoming an enabling technology for IoT. The main elements of an RFID system are tags and readers. RFID tags are small programmable devices used for object, animal and human tracking. They come in a variety of shapes, sizes, functionalities, and costs. RFID readers acquire and sometimes rewrite information stored on RFID tags that come within operating range (a few inches up to several feet).

Applications

The range of applications of RFID is wide and ever expanding. Four major categories of application are tracking and identification, payment and stored-value systems, access control, and anticounterfeiting.

The most widespread use of RFID is for tracking and identification. Another key area is payment and stored value systems.

Here is a partial list of applications in these four areas:

Tracking and identification:

- Large assets, for example, railway cars and shipping containers
- Livestock with rugged tags
- Pets with implanted tags
- Supply-chain management with EPC
- Inventory control with EPC
- Retail checkout with EPC
- Recycling and waste disposal
- Patient monitoring
- Tagging children at school Drivers' licenses and passports Payment and stored-value systems:
- Electronic toll systems
- Contact-less credit cards (for example, American Express Blue card)
- Stored-valued systems (for example, ExxonMobil Speedpass)
- Subway and bus passes
- Casino tokens and concert tickets Access control:
- Building access with proximity cards
- Ski lift passes
- Concert tickets
- Automobile ignition systems

Anticounterfeiting:

- Casino tokens (for example, Wynn Casino Las Vegas)
- High-denomination currency notes
- Luxury goods (for example, Prada)
- Prescription drugs

Tags

Figure 14.8 shows the key elements of an RFID system. Primary wireless communication is between a tag and a reader. The reader retrieves identification information and, depending on the application, other information about the tagged item. The reader then communicates this to a computer system which includes an RFID- related database and RFID-related applications.

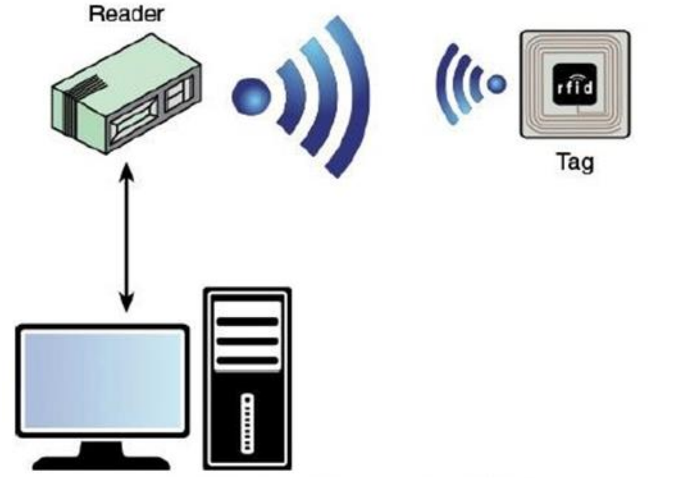


FIGURE 14.8 Elements of an RFID System

Figure 14.9 shows the two key components of a tag. The antenna is a metallic path in the tag whose layout depends on the size and shape of the tag and the operating frequency. Attached to the antenna is a simple microchip with very limited processing and nonvolatile storage

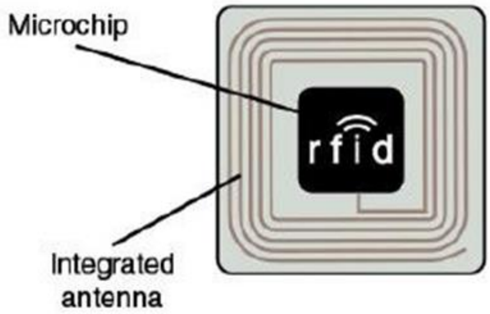


FIGURE 14.9 RFID Tag

Readers

RFID readers communicate with tags through an RF channel. There is a wide variety of different readers in terms of functionality and basic operating style. In general, there are three categories of readers:

- Fixed: Fixed readers create portals for automated reading of tags as they pass by. Common applications are to read tags as the associated items enter a room, pass through warehouse dock doors, or travel on a conveyor line.
- Mobile: Mobile readers are hand-held devices with an RFID antenna and reader and some computing capability. They are made for manually reading tags on the move.
- Desktop: This type of reader is typically attached to a PC or point-of-sale terminal and provides easy input.

Operating Frequency

True physical tag maximum read distance is determined by the individual RFID reader and antenna power, the chip used in the RFID tag, the material and thickness of material the tag is coated or covered with, the type of antenna the tag uses, the material the tag is attached to, and so on. The frequency range used by tag and reader is a limiting factor on read range.

c Write a short note on:

i) IoTivity

IoTivity is an open source software initiative. Their objective is to provide a standard and open source implementation so devices and services will be able to work together regardless of who makes them.

Two organizations are playing a key role in the IoTivity project

- Open Interconnect Consortium (OIC)
- Linux Foundation.

The project is sponsored by the OIC. OIC is an industry consortium whose purpose is to promote an open source implementation to improve interoperability between the billions of devices making up the IoT. To this end, OIC is working on developing standards and an overall framework that will establish a single solution covering interoperability across multiple vertical markets and use cases.

The IoTivity Project is hosted by the Linux Foundation, the nonprofit consortium dedicated to fostering the growth of Linux and collaborative development. As a Linux Foundation project, IoTivity is overseen by an independent steering group that will work with the OIC. Developers who want to get involved with the project can access RESTful-based application programming interfaces (APIs) and submit code for peer review through the project's server. It will be made available across the project's server. It will be made available across a range of programming languages, operating systems, and hardware platforms

ii) ioBridge

IoBridge provides software, firmware, and web services designed to make it simple and cost-effective to Internet- enable devices and products for manufacturers, professionals and casual users. By providing all the components necessary to web-enable things, ioBridge's customers avoid the complexity and cost associated with piecing together solutions from multiple vendors. The ioBridge offering is essentially a turnkey solution for a broad range of IoT users.

ioBridge Platform

IoBridge provides a complete end-to-end platform that is secure, private, and scalable for everything from do- it- yourself (DIY) home projects to commercial products and professional applications. ioBridge is both a hardware and cloud services provider.

Figure 15.15 illustrates some of the major features of ioBridge's technology. The tight integration between the embedded devices and the cloud services enable many of the features shown in the diagram that are not possible with traditional web server technology.

The major offerings on the device side are firmware, Iota modules, and gateways. Firmware is added where possible to devices to add the functionality to communicate with ioBridge services. Iotas are tiny embedded firmware or hardware modules with either Ethernet or Wi-Fi network connectivity. Gateways are small devices that can act as protocol converters and bridges between IoT devices and ioBridge services

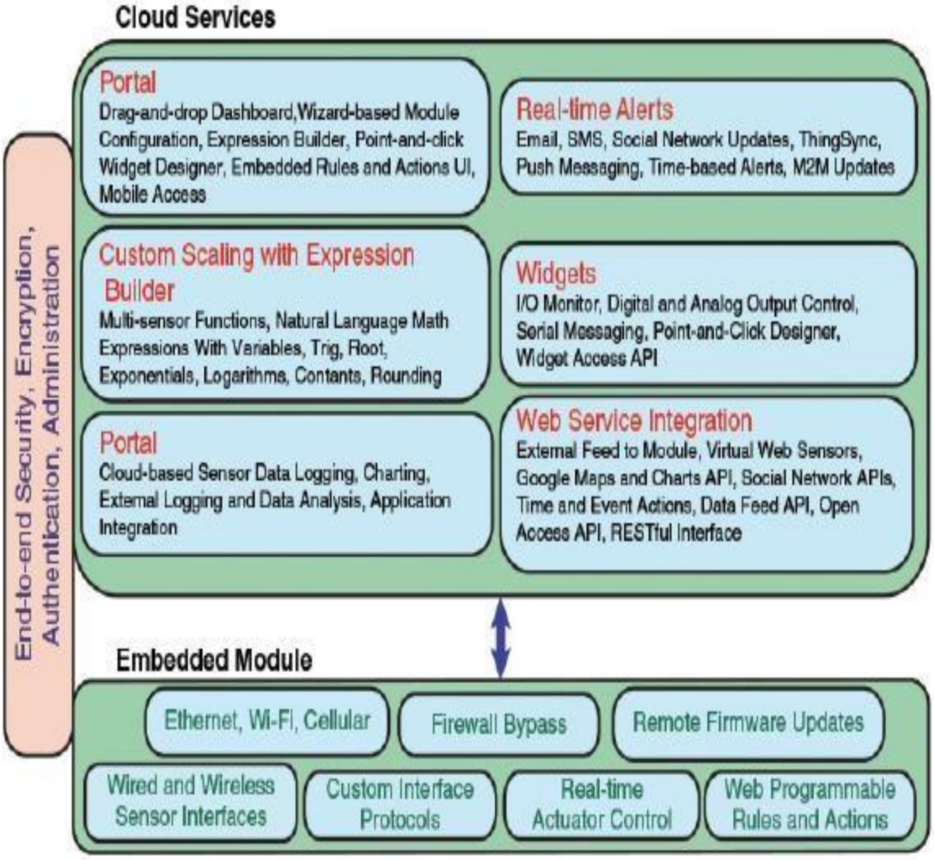


FIGURE 15.15 The ioBridge Internet of Things Platform