KARPAGAM ACADEMY OF HIGHER EDUCATION
Coimbatore-641 021
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF CS, CA & IT

SUBJECT NAME: NETWORK ARCHITECTURE AND MANAGEMENT

SUBJECT CODE: 17CSP304 **SEMESTER : III**

CLASS: II- M. Sc (CS)

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

COURSE OBJECTIVE

This course gain an understanding of the concepts and techniques used to model and implement communications between processes residing on independent host computers. The course examines the conceptual framework for specifying a computer network - the network architecture and investigates the set of rules and procedures that mediate the exchange of information between two communicating processes - the network protocols.

COURSE OUTCOME

- Be able to understand and analyze advanced Internet protocols.
- Be able to employ a hierarchy of Java classes to provide a solution to a given set of requirements.
- Can demonstrate an understanding of network architecture both hardware and software.
- Can write software to implement a client-server application using the socket programming API.

UNIT-I
Introduction: Objectives - Component architectures – Reference architecture – Architectural models; Addressing and Routing Architecture: Addressing mechanisms – Routing mechanisms – Addressing strategies – Routing strategies – Architectural considerations; Network Management Architecture: Defining Network Management – Network Management Mechanism - Architectural considerations; Performance Architecture; Developing goals – Performance mechanisms – Architectural considerations

UNIT- II
Security And Private Architecture: Developing a security and privacy plan – Security and privacy Administration & Mechanism - Architectural considerations; Selecting Technologies for the Network Design: Goals – Criteria for Technology Evaluation – Guidelines and constraints on Technology Evaluation – Choices for Network Design;

Interconnecting Technologies Within The Network Design: Shared medium – Switching – Routing – Hybrid mechanism – Applying Interconnection Mechanism to the Design

UNIT- III

Case history of Networking and Management: Challenges of Information Technology Managers – Goals organization and functions – Network and System Management – Network Management System Platform; SNMP Broadband and TMN Management: Network Management Standards & Model – Organization Information and Communication Model – ASN.1 – Encoding structure – Macros – Functional model; Organization and Information Model: Managed Networks – The History of Network Management – Internet Organization and standards – SNMP Model – The Organization and Information Model; Communication and Functional Model: The SNMP Communication Model – Functional Model.

UNIT- IV

SNMPv2 Management: Major changes – System architecture – Structure of Management Information – Management Information Base – SNMPv2 protocol – Compatibility; RMON: Remote monitoring – RMON1 – RMON2 – ATM remote monitoring; Broadband Network Management: ATM Networks - Network and Services – ATM Technology – ATM Network Management; Telecommunication Management Network: Operations systems – Conceptual model – Standards – Architecture – TMN Management service architecture – Integrated view of TMN – Implementation issues.

UNIT- V

Network Management Tools and Systems: Network management tools – Network statistics measurement system – Network Management Systems – System Management; Network Management Applications: Configuration Management - Fault Management - Performance Management – Security Management – Accounting Management – Report Management - Policy Based Management – Service Level Management.

SUGGESTED READINGS

TEXT BOOK

1. James, D. Mc Cabe. (2007) . Network Analysis Architecture and Design (3rd ed.). Morgan Kaufmann Publishers.
2. Mani Subramanian. (2000). Network Management Principles and Practice. New Delhi: Pearson Education Asia Pvt. Ltd.

REFERENCES

1. William Stallings. (1999). SNMP SNMPv2 SNMPv3 and RMON 1 and 2 (3rd ed.). New Delhi: Pearson Education Asia Pvt. Ltd.

WEB SITES

1. http://staff.um.edu.mt/csta1//courses/lectures/csm202/os17.html
2. http://www.inf.uni-konstanz.de/dbis/teaching/ss06/os/ch14-wrongNumber.pdf
3. https://www.cs.columbia.edu/~smb/classes/s06-4118/l26.pdf

Karpagam Academy of Higher Education
Pollachi Main Road, Eacharani Post, Coimbatore-641 021

DEPARTMENT OF CS,CA & IT
LECTURE PLAN

CLASS : II M.Sc CS **SEMESTER : III**

STAFF NAME : Dr. T. Genish

SUBJECT:Network Architecture and Management **SUBCODE:17CSP304**

UNIT I			
S.NO	**Lecture Duration (Hours)**	**Topics To Be Covered**	**Support Materials / Pg.No**
1	1	Introduction to syllabus, Objectives	T1.Pg:211-213
2	1	Component Architectures	T1.Pg:215-228
3	1	Reference Architecture and Architecture Models	T1.Pg:230-238
4	1	Addressing and Routing Architecture: Addressing Mechanisms ,Routing Mechanisms	T1.Pg:257-268
5	1	Addressing Strategies and Routing Strategies,Architectural Considerations	T1.Pg:278-287, 291-292
6	1	Network Management Architecture: Defining Network Management	T1.Pg:300-305
7	1	Network Management Mechanism Architectural Considerations	T1.Pg:306-310 T1.Pg:311-326
8	1	Performance Architecture: Developing Goals	T1.Pg:335-338
9	1	Performance mechanisms,Architectural Considerations	T1.Pg:338-354
10	1	Recapitulation and Discussion of Important Questions	
		Total No of Hours Planned for Unit I	**10**

		UNIT II	
S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
1	1	Security and private Architecture: Developing a security and privacy plan	T1.Pg:361-363
2	1	Security and privacy Administration Security and privacy Mechanism	T1.Pg:364,365 T1.Pg:367-369
3	1	Architectural considerations	T1.Pg:380
4	1	Selecting Technologies for the Network Design: Goals.	W1
5	1	Criteria for Technology Evaluation	W1,W2
6	1	Guidelines and Constraints on Technology Evaluation Choices for Network design	W1,W2
7	1	Interconnecting Technologies within the Network design:Shared Medium	W1
8	1	Switching,Routing and Hybrid Mechanism	
9	1	Applying Interconnection Mechanism to the Design	W1,W2
10	1	**Recapitulation and Discussion of Important Questions**	
		Total No of Hours Planned for Unit II	**10**
		UNIT III	
S.NO	**Lecture Duration (Hours)**	**Topics To Be Covered**	**Support Materials/ Pg.No**
1	1	Case history of Networking and Management: Challenges of Information Technology Managers	T2.Pg:58-61
2	1	Goals, Organization and Functions, Network and System Management , Network Management System Platform	T2.Pg:66-70, T2.Pg:71-74,W1
3	1	SNMP Broadband and TMN Management: Network Management standards Model and Organization Model and Information Model	T2.Pg:129-130 T2.Pg:131-138
4	1	Communication Model,ASN.1 Encoding Structure ,Macros and Function Model	T2.Pg:142-161
5	1	Organization and Information Model: Managed Networks, The History of Network Management, Internet Organization and standards ,SNMP Model	T2.Pg:169-178,W1
6	1	The Organization and Information Model	
7	1	Information Model--Managed Objects, Management Information Base	T2.Pg:178-206
8	1	Communication and Function Model: The SNMP Communication Model	T2.Pg:229-251

9	1	SNMP operations and Functional Model	
10	1	**Recapitulation and Discussion of Important Questions**	
		Total No of Hours Planned for Unit II	**10**
		UNIT IV	
S.NO	**Lecture Duration (Hours)**	**Topics To Be Covered**	**Support Materials/ Pg.No**
1	1	SNMPv2 Management: Major changes, System Architecture, Structure of Management Information	T2.Pg:256-282,W1, R1.pg:331-337
2	1	Management Information Base SNMPv2 Protocol ,Compatibility with SNMPv1	T2.Pg:288-289 T2.Pg:300-304
3	1	RMON: Remote Monitoring,RMON1, RMON2 ATM Remote Monitoring	T2.Pg:347-364 R1.pg:209-225
4	1	Broadband Network Management: ATM Networks, Network and services, ATM Technology	R1.pg:230-241
5	1	ATM Network Management(part1)	T2.Pg:371-387
6	1	ATM Network Management(part2)	T2.Pg:390-409
7	1	Telecommunications Management Network: Conceptual Model, Standards and Architecture	T2.Pg:455-468
8	1	TMN Management Service Architecture, Integrated view of TMN and Implementation issues	T2.Pg:469-472, W1
9	1	**Recapitulation and Discussion of Important Questions**	
		Total No of Hours Planned for Unit IV	**09**
		UNIT V	
S.NO	**Lecture Duration (Hours)**	**Topics To Be Covered**	**Support Materials/ Pg.No**
1	1	Network Management Tools and Systems: Network management tools	T2.Pg:481-498, R1.Pg:1-19
2	1	Network statistics measurement system	T2.Pg:500-503, w2
3	1	Network Management systems System Management	T2.Pg:506-509, T2.Pg:520,21
4	1	Network Management Applications: Configuration Management	T2.Pg:530-533, w3
5	1	Fault Management and Performance Management	T2.Pg:534-539,
6	1	Security Management	T2.Pg:556-574

		Accounting Management and Report Management	T2.Pg:575
7	1	Policy Based Management and Service Level Management	T2.Pg:578
8	1	**Recapitulation and Discussion of Important Questions**	
9	1	**Revision-Previous year ESE question papers**	
		Total No of Hours Planned for Unit V	**09**
		Total No of Hours Allocated	**48**

TEXT BOOK

T2. Mani Subramanian. (2000). Network Management Principles and Practice. New Delhi: Pearson Education Asia Pvt. Ltd.

REFERENCE BOOK

R1: William Stallings. (1999). SNMP SNMPv2 SNMPv3 and RMON 1 and 2 (3rd ed.). New Delhi: Pearson Education Asia Pvt. Ltd.

WEB SITES

W1: http://staff.um.edu.mt/csta1//courses/lectures/csm202/os17.html
W2:http://www.inf.uni-konstanz.de/dbis/teaching/ss06/os/ch14-wrongNumber.pdf
W3: https://www.cs.columbia.edu/~smb/classes/s06-4118/l26.pdf

SYLLABUS

UNIT I

Introduction: Objectives - Component architectures – Reference architecture – Architectural models; Addressing and Routing Architecture: Addressing mechanisms – Routing mechanisms – Addressing strategies – Routing strategies – Architectural considerations; Network Management Architecture: Defining Network Management – Network Management Mechanism - Architectural considerations; Performance Architecture; Developing goals – Performance mechanisms – Architectural considerations

Network Architecture

Component Architectures

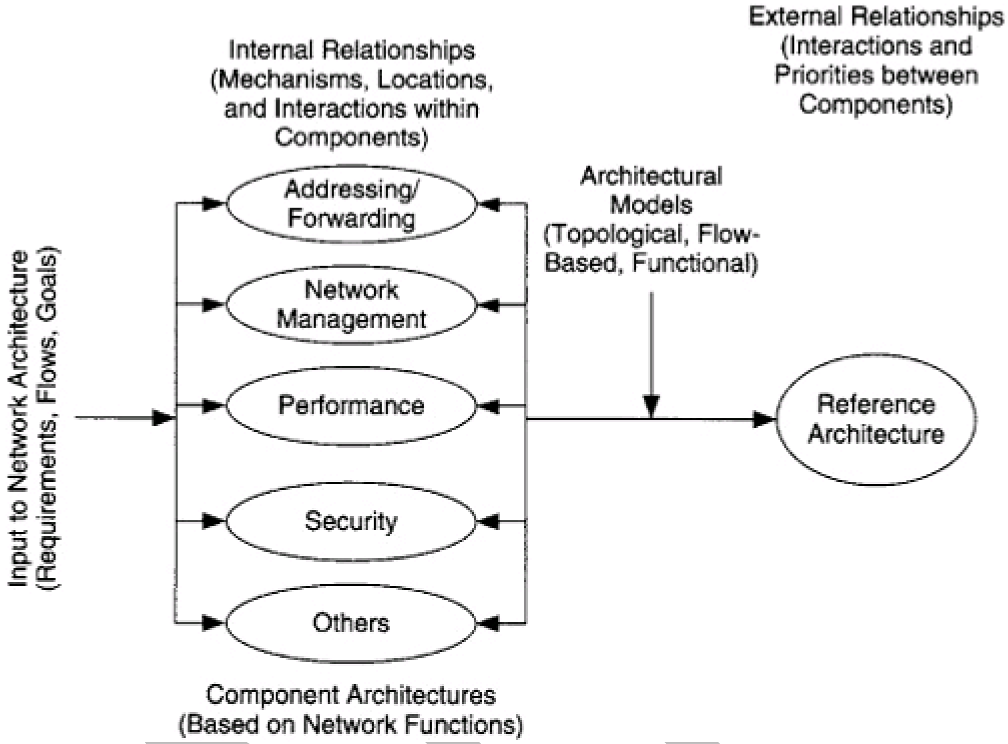
Component architecture is a description of how and where each function of a network is applied within that network. It consists of a set of mechanisms (hardware and software) by which that function is applied to the network, where each mechanism may be applied, and a set of internal relationships between these mechanisms.

Each function of a network represents a major capability of that network. There are four functions that are major capabilities of networks: addressing/routing, network management, performance, and security. Other general functions such as infrastructure and storage could also be developed as component architectures.

Reference Architecture

A reference architecture is a description of the complete network architecture and contains all of the component architectures (i.e., functions) being considered for that network. It is a compilation of the internal and external relationships developed during the network architecture process.

Process Model for Component Architecture Approach



Architectural Models

In developing the architecture for your network there are several architectural models that you can use as a starting point, either as the foundation of your architecture or to build upon what you already have. Three types of architectural models :

1. Topological models: It based on a geographical or topological arrangement and are often used as starting points in the development of the network architecture.
2. Flow-based models: It take particular advantage of traffic flows from the flow specification.
3. Functional models: It focus on one or more functions or features planned for in the network. It is likely that your reference architecture will contain more than one architectural model.

Topological Models

There are two popular topological models:

LAN/MAN/WAN and Access/Distribution/Core models. The LAN/MAN/WAN architectural model is simple and intuitive and is based on the geographical and/or topological separation of networks. Its important feature is that, by concentrating on LAN/MAN/WAN boundaries, it focuses on the features and requirements of those boundaries, and on compartmentalizing functions, service, performance, and features of the network along those boundaries.

Systems and Network Architectures

A systems architecture (also known as an enterprise architecture) is a superset of a network architecture, in that it also describes relationships, but the components are major functions of the system, such as storage, clients/servers, or databases, as well as of the network. In addition, devices and applications may be expanded to include particular functions, such as storage. For example, a systems architecture may include a storage architecture, describing servers, applications, a storage-area network (SAN), and how they interact with other components of the system.

From this perspective, the systems architecture considers the total or comprehensive picture, including the network, servers/clients, storage, servers, applications, and databases. Potentially, each component in the system could have its own architecture. There are likely to be other components, depending on the environment that the network is supporting.

Addressing and Routing Architecture

Addressing Mechanisms

The popular mechanisms for addressing networks: classful addressing, subnetting, variable-length subnetting, supernetting and classless interdomain routing (CIDR), private addressing and network address translation (NAT), and dynamic addressing. Although these mechanisms all basically share the same theme (manipulating address space), we treat them as separate in order to highlight their differences.

It should be noted that the concept of classful addressing is a bit outdated. We discuss it here in order to give some background on newer mechanisms and to provide insight into the addressing process.

Categories:

- Classful Addressing
- Subnetting
- Variable-Length Subnetting
- Supernetting
- Private Addressing and NAT

Routing Mechanisms

The routing mechanisms we consider here are establishing routing flows, identifying and classifying routing boundaries, and manipulating routing flows.

Categories:

- Establishing Routing Flows
- Identifying and Classifying Routing Boundaries
- Manipulating Routing Flows

Establishing Routing Flows

In preparing to discuss boundaries and route manipulation, we want to understand how flows will likely be routed through the network. As we see later in this chapter, addressing and routing are both closely coupled to the flow of routing information in the network, and the addressing and routing architecture is based partially on establishing these flows.

Addressing Strategies

During the requirements analysis process, it is important to gather information about device growth expectations, so that you can avoid having to change addressing schemes and reconfigure device addresses during the life cycle of the network.

When applying subnetting, variable-length subnetting, classful addressing, supernetting, private addressing and NAT, and dynamic addressing, we want to make sure that our network addresses and masks will scale to the sizes of the areas they will be assigned to. We also want to establish the degrees of hierarchy in the network.

Routing Strategies

This section introduces and describes popular interior and exterior routing protocols. Now that we have the framework for routing developed and some addressing strategies, let's consider some strategies for applying routing protocols. This section covers the characteristics of some popular routing protocols, criteria for making selections from these protocols, and where to apply and mix these protocols.

Categories:

- Evaluating Routing Protocols
- Choosing and Applying Routing Protocols

Architectural Considerations

In developing our addressing and routing architecture we need to evaluate the sets of internal and external relationships for this component architecture.

Internal Relationships

Depending on the type of network being developed, the set of candidate addressing and forwarding mechanisms for a component architecture can be quite different. For example, a service-provider network may focus on mechanisms such as super-netting, CIDR, multicasts, peering, routing policies, and confederations, whereas the focus of a medium-sized enterprise network would more likely be on private addressing and network address translation, subnetting, VLANs, switching, and the choice and locations of routing protocols.

External Relationships

External relationships are trade-offs, dependencies, and constraints between the addressing/routing architecture and each of the other component architectures (network management, performance, security, and any other component architectures you may develop).

There are common external relationships between addressing/routing and each of the other component architectures, some of which are presented in the following subsections.

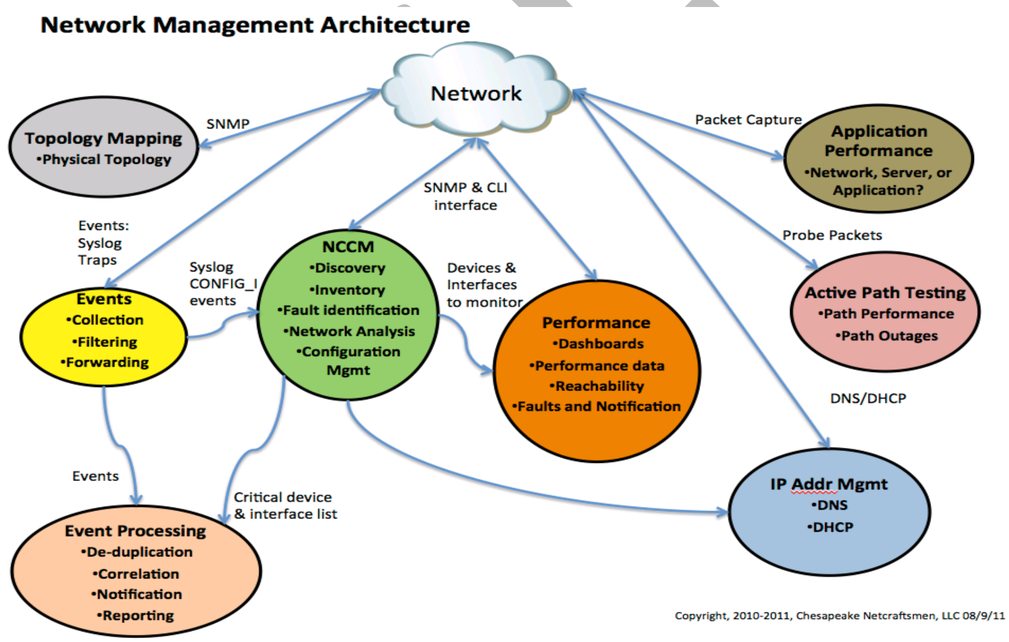
Network Management Architecture

Defining Network Management

Network management can be viewed as a structure consisting of multiple layers:

- Business Management: The management of the business aspects of a network—for example, the management of budgets/resources, planning, and agreements.

- Service Management: The management of delivery of services to users—for example, for service providers this would include the management of access bandwidth, data storage, and application delivery.
- Network Management: The management of all network devices across the entire network.
- Element Management: The management of a collection of similar network devices—for example, access routers or subscriber management systems.
- Network-Element Management: The management of individual network devices—for example, a single router, switch, or hub.



Network Management Mechanisms

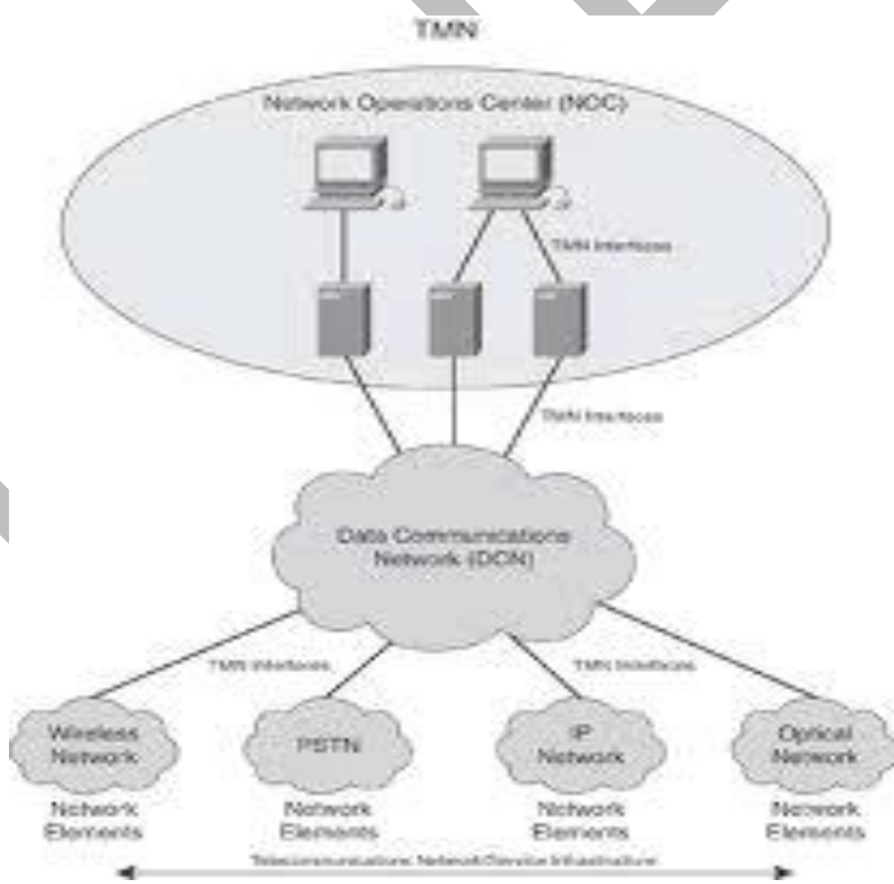
The popular management mechanisms, including network management protocols. There are currently two major network management protocols: the simple network management protocol (SNMP) and the common management information protocol (CMIP). CMIP includes CMIP over TCP/IP (CMOT). These network management protocols provide the mechanism for retrieving, changing, and transport of network management data across the network.

SNMP has seen widespread use and forms the basis for many popular commercial and public network management systems. It provides facilities for collecting and configuring parameters from network devices. These are done through the SNMP commands get (to collect the value of a parameter), get-next (to collect the value of the next parameter in the list), and set (to change the value of a parameter). There are also provisions for the unsolicited notification of events, through the use of traps. A trap is a user-configurable threshold for a parameter. When this threshold is crossed, the values for one or more parameters are sent to a specified location. A benefit of trap generation is that polling for certain parameters can be stopped or the polling interval lengthened, and instead an automatic notice is sent to the management system when an event occurs.

Architectural Considerations

The network management process consists of choosing which characteristics of each type of network device to monitor/manage; instrumenting the network devices (or adding collection devices) to collect all necessary data; processing these data for viewing, storage, and/or reporting; displaying a subset of the results; and storing or archiving some subset of the data.

Network management touches all other aspects of the network. This is captured in the FCAPS model:



Performance Architecture

Developing Goals for Performance

For each component architecture it is important to understand why that function is needed for that particular network. This is especially important for the performance architecture. The process of developing goals for this (or any other) component architecture begins during requirements analysis and is further refined during the architecture process. Therefore, the requirements and flow specifications and maps provide important input to this process.

While performance is always desirable, we need to ensure that the performance mechanisms we incorporate into the architecture are necessary and sufficient to achieve the performance goals for that network.

Performance Mechanisms

As presented in the last chapter, performance mechanisms discussed here are quality of service, resource control (prioritization, traffic management, scheduling, and queuing), service-level agreements, and policies. These mechanisms incorporate the general mechanisms shown in the previous section

Subsets of these mechanisms are usually used together to form a comprehensive approach to providing single-tier and multi-tier performance in a network. These mechanisms provide the means to identify traffic flow types, measure their temporal characteristics, and take various actions to improve performance for individual flows, groups of flows, or for all flows in the network.

Categories:

- Quality of Service
- Prioritization, Traffic Management, Scheduling, and Queuing
- Service-Level Agreements
- Policies

Architectural Considerations

In developing our performance architecture we need to evaluate potential performance mechanisms, determine where they may apply within the network, and examine the sets of internal and external relationships for this component architecture.

Evaluation of Performance Mechanisms

At this point we should have requirements, goals, type of environment, and architectural model(s), and are ready to evaluate potential performance mechanisms. When evaluating performance mechanisms, it is best to start simple (e.g., DiffServ QoS), and work toward more complex solutions only when necessary.

Internal Relationships

Depending on the type of network being developed, the set of candidate addressing and forwarding mechanisms for a component architecture can be quite different.

Two types of interactions are predominant within this component architecture: (1) trade-offs between addressing and forwarding mechanisms and (2) trade-offs within addressing or within forwarding. Addressing and forwarding mechanisms influence the choice of routing protocols and where they are applied. They also form an addressing hierarchy upon which the routing hierarchy is overlaid.

External Relationships

External relationships are trade-offs, dependencies, and constraints between the addressing/routing architecture and each of the other component architectures (network management, performance, security, and any other component architectures you may develop).

There are common external relationships between addressing/routing and each of the other component architectures, some of which are presented in the following subsections.

Categories:

- Interactions between Addressing/Routing and Network Management
- Interactions between Addressing/Routing and Performance
- Interactions between Addressing/Routing and Security

POSSIBLE QUESTIONS

UNIT-I

PART-A **(20 MARKS)**

(Q.NO 1 TO 20 Online Examination)

PART –B **(5*6=30 MARKS)**

1. Explain various component architecture of a network with neat sketches.
2. Discuss in detail about the Performance Mechanisms used in a network.
3. Explain the process of developing Architectural Models for a network system
4. Explain the various architectural considerations for network management process.
5. Explain the Flow based Architectural Model with a neat sketch
6. Discuss about the Network Management Mechanisms in detail.
7. Explain the Addressing and Routing mechanism used in a network.
8. Explain the Reference Architecture with neat sketch.

PART – C

CASE STUDY (COMPULSORY) **(1*10=10 MARKS)**

1. A network's architecture differs from its design in terms of its scope, level of detail, Description and location information. Describe how an architecture and design differ in each characteristic.
2. Discuss A Case Study in Network Architecture Tradeoffs.
3. Write about Teaching Network Architecture through Case Studies

Karpagam Academy of Higher Education
Department of CS, CA & IT
Subject:Network architecture and Management
Subject Code:17CSP304
Class: II-M.Sc(CS) **SEM:III**
Objective type questions
UNIT-I

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	______________ is the process of developing a high level, end to end structure for the network.	Network Architecture	Component Architecture	Reference Architecture	System Architecture	**Network Architecture**
2	______________ is a description of how and whose each function of a network is applied within that network	Network Architecture	Component Architecture	Reference Architecture	System Architecture	**Component Architecture**
3	______________are the hardware and software that help a network Architecture each capability	Functions	Mechanisms	Constraints	Trade-Off	**Mechanisms**
4	______________consists of interaction , protocols and they are used to optimize each function with in the network	Constraints	External Relationships	Internal Relationships	Dependencies	**Internal Relationships**
5	______________ are decision points in the development of each component Architecture	Dependencies	Trade-Off	Route Filtering	Rules	**Trade-Off**
6	______________ occur when one mechanism relies on another mechanism for its operation	Trade-Off	Constraints	Dependencies	Rules	**Dependencies**

7	_______________ are the restrictions that one mechanism places on another	Rules	Rules	Protocols	Constraints	**Constraints**
8	_______________ provides monitoring , configuring & troubleshooting for the network	Network Management	Performance	Route Filtering	security	**Network Management**
9	SLA stands for _______________	Service Level Agreement	Service Level Management	security	Protocols	**Service Level Management**
10	DMZ stands for _______________	Data Media Zone	Decentralized Zone	Delocalized Zone	Demilitarized Zone	**Demilitarized Zone**
11	_______________ is applying identifiers to devices at various protocol layer	Addressing	Protocols	Routing	security	**Addressing**
12	_______________ is subnetting in which multiple subnet masks are used creating subnets of different sizes	Subnet Mask	Supernetting	Variable-Length Subnetting	security	**Variable-Length Subnetting**
13	_______________ is a technique used to inform the network of the default route	Trace Route	Default Route	Route Filtering	Route Shaping	**Default Route**
14	_______________ are packets targeted towards multiple destinations	Unicast	Broadcast	Both A & B	Multicasts	**Multicasts**
15	_______________ is the technique of applying filter to hide networks from the rest of autonomous system	Route Filtering	Peering	Addressing	Route Shaping	**Route Filtering**

16	______________ is processing functions to control plan, allocate deploy and monitor network resources	Component Management	Network Management	Network Architecture	System Management	**Network Management**
17	______________ is setting parameters in a network device for operation and control of that element	Constraints	Parameters	Configuration	Operation	**Configuration**
18	______________ and ______________ management system is in a single hardware platform or distributed across the network	Integration	Centralized And Decentralized Management	Peer to Peer and Client/ Server Management	Filtering	**Centralized And Decentralized Management**
19	______________ data is determining how much network capacity should be reserved for network management	Measuring	Scaling Network	Memory Size	CPU time	**Scaling Network**
20	______________ into OSS refers to how the management system will communicate with higher level OSS.	Measuring	Filtering	Routing	Integration	**Integration**
21	______________ refers to mechanisms that will allocate control and manage network resources for traffic	Program Control	Resource Control	Address Control	Security	**Resource Control**
22	______________ is a requirement to guarantee the confidentiality, integrity and availability of the user	Resource Control	Routing	Component	Security	**Security**

23	______________ is the protection of devices from physical access , damage and theft	External Security	Security Awareness	Physical Security	Resource Control	**Physical Security**
24	______________ is a security mechanism in which cipher algorithms are applied together	Decryption	Encryption	Filtering	Security Awareness	**Encryption**
25	______________ is the description of complete network architecture and contain all of the component Architecture	Reference Architecture	Network Architecture	Network Management	Performance Architecture	**Reference Architecture**
26	MAN stands for ______________	Man Network	Metropolitan Area Network	Media Access Network	security	**Metropolitan Area Network**
27	______________ are useful managing the development of this architectural model	ICD's	PD's	IANA	NAT	**ICD's**
28	______________ is based on the peer to peer flow model, in which the flow behaviors of the devices and application are fairly consistent throughout the network.	Flow Based Architectural Model	Client/Server Model	Peer To Peer Architectural Model	Centralized Model	**Peer To Peer Architectural Model**

29	________ performance architectural model focus on identifying networks or parts of a network having a single tier of performance , multiple tier of performance	Single - Tier	Service Provider	Multi Tier	Single - Tier Multi Tier Performance	**Single - Tier Multi Tier Performance**
30	________ are the most different to apply to a network because you must where each function will be located	Function Models	Reference Models	Architectural Models	Layered models	**Function Models**
31	A ________ architecture is a super set of a network architecture	Reference	Systems	Components	Security	**Systems**
32	SAN stands for ________	Server Access Network	Small Area Network	Storage Area Network	Storage Access Network	**Storage Area Network**
33	________ are usually assigned using DHCP.	Persistent Address	Transient Address	Private Address	Temporary Address	**Temporary Address**
34	________ address that are assigned for a configuration of time	Temporary	Persistent	Public	Private	**Persistent**
35	Which is the route used when there is no other route for that destination?	Trace Route	Routing	Default Route	security	**Default Route**
36	________ applying predetermined mask length to a addressing to support the range of network sizes	Subnetting	Classless Addressing	Classful Addressing	security	**Classful Addressing**

37	The natural mask for class B address is ______________	255.255.0.0	255.255.255.0	255.0.0.0	255.255.255.255	**255.255.0.0**
38	______________ is aggregating network addresses by changing the address mask	Subnet Mask	Supernetting	Routing	Integration	**Supernetting**
39	______________ maps IP address between public and private space	Routing Boundaries	security	NAT	Functional Area	**NAT**
40	______________Are groups within the system that shares a similar function.	Groups	Workgroup	Devices	Functional Areas	**Functional Areas**
41	______________ are groups of users that have common locations, applications and requirements	Work Groups	Functional Area	Boundaries	Regions	**Work Groups**
42	______________ are physical or logical separations of a network	Routing Boundaries	Physical Boundaries	Physical Interface	security	**Routing Boundaries**
43	______________communicate routing information primarily between AS	BGP	EGPs	IGPs	security	**EGPs**
44	______________ boundaries are found between ASs, between an ASs and an external network	EGP	Soft	Hard	Hybrid	**Hard**
45	______________ are routes that are configured manually, by network personnel or scripts	Dynamic Routes	Safe Routes	Temporary Routes	Static Routes	**Static Routes**

46	A _______________ network is a network with only path into or out of it	Stub	Layers	Routing Boundaries	security	**Stub**
47	_____Management of individual network devices	Service Management	Element Management	Network Element Management	security	**Network Element Management**
48	A _______________ is an individual component of the network that participate at one or more protocol layers	Stub	Layers	Network Devices	DMZ	**Network Devices**
49	______________is the protection of devies from physical acces damage,and theft	security	physical security	application security	n\w security	**physical security**
50	IP sec is a protocol for providing authenticaion and encryption\decryption between devies at the __________ layer	physical	datalink	Network	Transport	**Network**
51	AH stands for	address header	authentication	Access header	Advance Header	**authentication**
52	ESP stands for	encapsulating security payload	Encryption Secured Protocol	Encapsulation Secured Protocol	Encryption Secured Payload	**encapsulating security payload**
53	USM stands for	user security modem	user system model	User Based Security Model	User Security Model	**User Based Security Model**
54	__________message verification ,user identify verification,and data confidentiality	SNMP	USM	DES	MIB	**SNMP**

55	SNMP security also provides for modifying management information base________ views and access modes	SNMP	USM	DES	MIB	**MIB**
56	MIB stands for _______________	Message Information Base	Message Interface Base	Managem ent Information Base	Manageme nt Interface Base	**Management Information Base**
57	NAT stands for _______________	Network Access Translation	Network Address Translation	Network Address Transaction	Network Access Transaction	**Network Address Translation**
58	NAPT stands for _______________	Network Address Port Translation	Network Access Port Translation	Network Address Protocol Translation	n/w access port transaction	**Network Address Port Translation**
59	NAS stands for _______________	Network Address Server	Network Access Server	n/w access service	Network Address Service	**Network Access Server**
60	SMS stands for _______________	Standard Management System	Standard Management System	Subscriber Management System	security Of These	**Subscriber Management System**

SYLLABUS

UNIT II

Security And Private Architecture: Developing a security and privacy plan – Security and privacy Administration & Mechanism - Architectural considerations; Selecting Technologies for the Network Design: Goals – Criteria for Technology Evaluation – Guidelines and constraints on Technology Evaluation – Choices for Network Design; Interconnecting Technologies Within The Network Design: Shared medium – Switching – Routing – Hybrid mechanism – Applying Interconnection Mechanism to the Design

Security and Privacy Architecture

Developing a Security and Privacy Plan

The development of each component architecture is based on our understanding of why that function is needed for that particular network. While one may argue that security is always necessary, we still need to ensure that the security mechanisms we incorporate into the architecture are optimal for achieving the security goals for that network. Therefore, toward developing a security architecture, we should answer the following questions:

1. What are we trying to solve, add, or differentiate by adding security mechanisms to this network?
2. Are security mechanisms sufficient for this network?

The performance architecture, we want to avoid implementing (security) mechanisms just because they are interesting or new. When security mechanisms are indicated, it is best to start simple and work toward a more complex security architecture when warranted. Simplicity may be achieved in the security architecture by implementing security mechanisms only in selected areas of the network (e.g., at the access or distribution [server] networks), or by using only one or a few mechanisms, or by selecting only those mechanisms that are easy to implement, operate, and maintain.

Some common areas that are addressed by the security architecture include:

- Which resources need to be protected
- What problems (threats) are we protecting against
- The likelihood of each problem (threat)

This information becomes part of your security and privacy plan for the network. This plan should be reviewed and updated periodically to reflect the current state of security threats to the network. Some organizations review their security plans yearly, others more frequently, depending on their requirements for security. Note that there may be groups within a network that have different security needs. As a result, the security architecture may have different levels of security.

Security and Privacy Administration

The preparation and ongoing administration of security and privacy in the network are quite important to the overall success of the security architecture. Like the requirements and flows analyses, understanding what your threats are and how you are going to protect against them is an important first step in developing security for your network. In this section we discuss two important components in preparing for security: threat analysis and policies and procedures.

Threat Analysis

A *threat analysis* is a process used to determine which components of the system need to be protected and the types of security risks (threats) they should be protected. This information can be used to determine strategic locations in the network architecture and design where security can reasonably and effectively be implemented.

A threat analysis typically consists of identifying the assets to be protected, as well as identifying and evaluating possible threats. Assets may include, but are not restricted to:

- User hardware (workstations/PCs)
- Servers
- Specialized devices
- Network devices (hubs, switches, routers, OAM&P)
- Software (OS, utilities, client programs)
- Services (applications, IP services)
- Data (local/remote, stored, archived, databases, data in-transit)

And threats may include, but are not restricted to:

- Unauthorized access to data/services/software/hardware
- Unauthorized disclosure of information
- Denial of service
- Theft of data/services/software/hardware
- Corruption of data/services/software/hardware
- Viruses, worms, Trojan horses
- Physical damage

One method to gather data about security and privacy for your environment is to list the threats and assets on a worksheet. This threat analysis worksheet can then be distributed to users, administration, and management, even as part of the requirements analysis process.

Policies and Procedures

There are many trade-offs in security and privacy (as with all other architectural components), and it can be a two-edged sword. Sometimes security is confused with control over users and their actions. This confusion occurs when rules, regulations, and security guardians are placed above the goals and work that the organization is trying to accomplish. The road toward implementing security starts with an awareness and understanding of the possible security weaknesses in the network and then leads to the removal of these weaknesses. Weaknesses can generally be found in the areas of system and application software, the ways that security mechanisms are implemented, and in how users do their work. This last area is where educating users can be most beneficial.

Security policies and procedures are formal statements on rules for system, network, and information access and use, in order to minimize exposure to security threats. They define and document how the system can be used with minimal security risk. Importantly, they can also clarify *to users* what the security threats are, what can be done to reduce such risks, and the consequences of not helping to reduce them. At a high level, security policies and procedures can present an organization's overall security philosophy.

Examples of common high-level security philosophies are to deny specifics and accept everything else, or to accept specifics and deny everything else, as in Figure 9.3. The term *specific* refers to well-defined rules about who, what, and where security is applied. For example, it may be a list of specific routes that can be accepted into this network, or users that are permitted access to certain resources.

Security that denies specifics and accepts all else reflects an open network philosophy, requiring a thorough understanding of potential security threats, as these should be the specifics to be denied. It can be difficult to verify the security implementation for this philosophy, as it is hard to define "all else."

On the other hand, security that accepts specifics and denies all else reflects a closed network philosophy, requiring a thorough understanding of user, application, device, and network requirements, as these will become the specifics to be accepted. It is easier to validate this security implementation, as there is a finite (relatively small) set of "accepted" uses. Of the two philosophies, accept specifics/deny all else is the more common philosophy.

Security and Privacy Mechanisms

There are several security mechanisms available today and many more on the horizon. However, not all mechanisms are appropriate for every environment. Each security mechanism should be evaluated for the network it is being applied to, based on the degree of protection it provides, its impact on users' ability to do work, the amount of expertise required for installation and configuration, the cost of purchasing, implementing, and operating it, and the amounts of administration and maintenance required.

In this section physical security and awareness, protocol and application security, encryption/decryption, network perimeter security, and remote access security.

Physical Security and Awareness

Physical security is the protection of devices from physical access, damage, and theft. Devices are usually network and system hardware, such as network devices (routers, switches, hubs, etc.), servers, and specialized devices, but can also be software CDs, tapes, or peripheral devices. Physical security is the most basic form of security, and the one that is most intuitive to users. Nevertheless, it is often overlooked when developing a security plan. Physical security should be addressed as part of the network architecture even when the campus or building has access restrictions or security guards.

Ways to implement physical security include the following

- Access-controlled rooms (e.g., via card keys) for shared devices (servers) and specialized devices.
- Backup power sources and power conditioning
- Off-site storage and archival
- Alarm systems (e.g., fire and illegal entry alarms)

Physical security also applies to other types of physical threats, such as natural disasters (e.g., fires, earthquakes, and storms). Security from natural disasters includes protection from fire (using alarm systems and fire-abatement equipment), water (with pumping and other water-removal/protection mechanisms), and structural degradation (through having devices in racks attached to floors, walls, etc.). Addressing physical security lays the foundation for your entire network security and privacy plan.

Protocol and Application Security

IPSec is a protocol for providing authentication and encryption/decryption between devices at the network layer. IPSec mechanisms consist of authentication header (AH) and encapsulating security payload (ESP). There are two modes that IPSec operates in: transport and tunneling. In transport mode the IP payload is encrypted using ESP, while the IP header is left. In tunnel mode IPSec can be used to encapsulate packets between two virtual private network (VPN) gateways (IPb and IPc in the figure).

The tunneling process consists of the following:

- IPSec tunnels are created between VPN gateways IPb and IPc in Figure 9.6
- IP packets are encrypted using ESP

Encryption/Decryption

Security mechanisms provide protection against unauthorized access and destruction of resources and information, encryption/decryption protects information from being usable by the attacker.

Encryption/decryption is a security Another example is the secure sockets library (SSL). *Secure sockets library* is a security mechanism that uses RSA-based authentication to recognize a party's digital identity and uses RC4 to encrypt and decrypt the accompanying transaction or communication. SSL has grown to become one of the leading security protocols on the Internet.

One trade-off with encryption/decryption is a reduction in network performance. Depending on the type of encryption/decryption and where it is implemented in the network, network performance (in terms of capacity and delay) can be degraded from 15% to 85% or more. Encryption/decryption usually also requires administration and maintenance, and some encryption/decryption equipment can be expensive. While this mechanism is compatible with other security mechanisms, trade-offs such as these should be considered when evaluating encryption/ decryption.

Network Perimeter Security

For network perimeter security, or protecting the *external interfaces* between your network and external networks, we consider the use of address translation mechanisms and firewalls.

Network address translation, or NAT, is the mapping of IP addresses from one realm to another. Typically this is between public and private IP address space. Private IP address space is the set of IETF-defined private address spaces (RFC 1918):

- Class A 10.x.x.x 10/8 prefix
- Class B 172.16.x.x 172.16/12 prefix
- Class C 192.168.x.x 192.168/16 prefix

NAT is used to create bindings between addresses, such as one-to-one address binding (static NAT); one-to-many address binding (dynamic NAT); and address and port bindings (network address port translation, or NAPT).

While NAT was developed to address the issues of address space exhaustion, it was quickly adopted as a mechanism to enhance security at external interfaces. Routes to private IP address spaces are not propagated within the Internet; therefore, the use of private IP addresses hides the internal addressing structure of a network from the outside. The security architecture should consider a combination of static and dynamic NAT and NAPT, based on the devices that are being protected.

Remote Access Security

Remote access consists of traditional dial-in, point-to-point sessions, and virtual private network connections, as shown in Figure 9.9. Security for remote access includes what is commonly known as AAAA: authentication of users; authorization of resources to authenticated users; accounting of resources and service delivery; and allocation of configuration information (e.g., addresses or default route). AAAA is usually supported by a network device such as a network access server (NAS) or subscriber management system (SMS).

Remote access security is common in service-provider networks (see also the service-provider architectural model), but it is evolving into enterprise networks as enterprises recognize the need to support a remote access model for their networks.

Considerations when providing remote access are as follows (see Figure 9.10):

- Method(s) of AAAA
- Server types and placement (e.g., DMZ)
- Interactions with DNS, address pools, and other services

Architectural Considerations

In developing our security architecture we need to evaluate potential security mechanisms, where they may apply within the network, as well as the sets of internal and external relationships for this component architecture.

Evaluation of Security Mechanisms

At this point we have requirements, goals, type of environment, and architectural model(s) and are ready to evaluate potential security mechanisms. As with each component architecture, when evaluating mechanisms for an architecture, it is best to start simple and work toward more complex solutions only when necessary.

- Evaluation of Security Mechanisms
- Internal Relationships
- External Relationships

Selecting technologies for the network design:

Physical network design involves the selection of LAN and WAN technologies for campus and enterprise network designs. During this phase of the top-down network design process, choices are made regarding cabling, physical and data link layer protocols, and internetworking devices (such as switches, routers, and wireless access points). A logical design, "Logical Network Design," covered, forms the foundation for a physical design. In addition, business goals, technical requirements, network traffic characteristics, and traffic flows "Identifying Your Customer's Needs and Goals," influence a physical design.

A network designer has many options for LAN and WAN implementations. No single technology or device is the right answer for all circumstances. The goal of "Physical Network Design," is to give you information about the scalability, performance, affordability, and manageability characteristics of typical options, to help you make the right selections for your particular customer.

Common design goals includes optimizing the following

- Network deployment and operations costs, includes the cost for circuits and servies.
- Security, including maximizing security across the network, mapping security to a particular groups requirement or providing multiple security models within the network.
- One or more performance characteristics.
- Ease of use and manageability of the network
- Supportability of the network.

Criteria for technology evaluation

Areas that could be include:-
Time and costs
Functional qualities
Aesthetic and visual appeal
Materials, constructing,assembly quality requirements
Safety
Environmental considerations
Ergonomics
Care and handling.

Guidelines and Constraints on Technology Evaluations

Guideline 1: If predictable and/or guaranteed requirements are listed in the flow specification (service plan), then either the technology or a combination of technology and supporting protocols or mechanisms must support these requirements. This guideline restricts the selection of candidate technologies to those that can support predictable and/or guaranteed requirements.

There are a couple of reasons to distinguish between services types. First, by separating those flows that have strict RMA, capacity, and/or delay requirements, we are taking the first steps toward offering multiple, various services to users, applications, and devices. As mechanisms for offering services evolve , becoming better understood and widely available, we will be prepared to take advantage of these services in the network design.

Second, flows that require predictable services need to be handled differently by the network. Given the nature of predictable requirements in flows, they are not as tolerant as best-effort flows to variances in network performance. Thus, we need to ensure that predictable flows receive more predictable performance from the network. This is the basis for our selection of candidate technologies for predictable flows.

For flows that have predictable requirements, we want to choose candidate technologies that can support these requirements. Predictable service is a bounded service, so we want technologies that can provide mechanisms that bound or control performance. Mechanisms to consider come from the performance architecture, for example:

- Quality-of-service levels in ATM
- Committed information rate levels in frame relay
- Differentiated service or integrated service levels in IP
- Nonstandard or proprietary methods

Such options provide more predictability than traditional best-effort services and can play a part in offering guaranteed services. Support for guaranteed service is much more stringent than that for predictable services and includes feedback to ensure that the services are being delivered or to provide accountability when service is not being delivered. To offer a guaranteed service, a candidate technology must be capable of:

- Determining the state of network resources and available levels of performance for the end-to-end path of the traffic flow.
- Allocating and controlling network resources along the end-to-end path of the traffic flow.
- Providing mechanisms to arbitrate and prioritize who gets or keeps service when it is contended for.

Guideline 2: When best-effort, predictable, and/or guaranteed capacities are listed in the flow specification, the selection of technology may also be based on capacity planning for each flow. Capacity planning uses the combined capacities from the flow specification to select candidate technologies, comparing the scalability of each technology to capacity and growth expectations for the network.

When comparing capacity estimates from the flow specification to capacities expected from candidate technologies, we want to determine a capacity boundary that will indicate that a technology's capacity is insufficient for a flow. In capacity planning, we want to design toward that capacity boundary and make sure that the technology has capacity to spare. If the flow contains only best-effort capacities, then a guideline is for the combined (summary) capacity of that flow to be approximately 60% of the capacity boundary for that flow. If the flow contains predictable capacities, then the guideline is for the predictable capacity of that flow to be approximately 80%, or the combined best-effort capacity to be 60%, of the capacity boundary of the flow, whichever is greater.

These guidelines are based on experience and should be used as a first attempt to evaluate technologies based on capacity. As you use them, you should be able to modify them to better approximate your network design. For example, if you can estimate the degree of burstiness in the data flow from an application, you can use it to modify the boundary capacity. Some bursty networks are designed to the boundary capacity divided by burstiness. Thus, if the burstiness (peak data rate/average data rate) of a predictable application is 5, then the design is based on 80% 5, or 16% of the boundary capacity. Doing this enables the network to accommodate a much higher capacity during times of burstiness from applications. To be able to use these guidelines, you need to know the characteristics of each flow in the flow specification.

Interconnecting Technologies Within the Network Design

The design process by connecting these technologies together within the network design. Methods to connect technologies (interconnection strategies), in conjunction with the technology choices made in the previous chapter, provide detail to the design in preparation for planning and installation.

Shared medium

In telecommunication, a **shared medium** is a medium or channel of information transfer that serves more than one user at the same time. Most channels only function correctly when one user is transmitting, so a channel access method is always in effect.

In circuit switching, each user typically gets a fixed share of the channel capacity. A multiplexing scheme divides up the capacity of the medium. Common multiplexing schemes include time-division multiplexing and frequency-division multiplexing. Channel access methods for circuit switching include time division multiple access, frequency-division multiple access, etc.

In packet switching, the sharing is more dynamic — each user takes up little or none of the capacity when idle, and can utilize the entire capacity if transmitting while all other users are idle. Channel access methods for packet switching include carrier sense multiple access, token passing, etc.

Switching

Switch is an electrical component that can break an electrical circuit, interrupting the current or diverting it from one conductor to another.[1][2]

The most familiar form of switch is a manually operated electromechanical device with one or more sets of electrical contacts, which are connected to external circuits. Each set of contacts can be in one of two states: either "closed" meaning the contacts are touching and electricity can flow between them, or "open", meaning the contacts are separated and the switch is nonconducting. The mechanism actuating the transition between these two states (open or closed) can be either a "*toggle*" (flip switch for continuous "on" or "off") or "*momentary*" (push-for "on" or push-for "off") type.

A switch may be directly manipulated by a human as a control signal to a system, such as a computer keyboard button, or to control power flow in a circuit, such as a light switch. Automatically operated switches can be used to control the motions of machines, for example, to indicate that a garage door has reached its full open position or that a machine tool is in a position to accept another workpiece. Switches may be operated by process variables such as pressure, temperature, flow, current, voltage, and force, acting as sensors in a process and used to automatically control a system.

Routing

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes, typically hardware devices called routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time, but multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Because structured addresses allow a single routing table entry to represent the route to a group of devices, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging) in large networks, and has become the dominant form of addressing on the Internet, though bridging is still widely used within localized environments.

Applying Interconnection Mechanisms to the Design

Interconnections are important from at least two perspectives: They are used to change the degree of concentration of networks or flows at the interconnection (hierarchy), as well as the number of alternate paths provided by the interconnection mechanisms (redundancy).

Hierarchy

Throughout the first part of this book, we looked for locations where information comes together in the network, whether it is applications, users, flows, or broadcast domains, and we examined where boundaries between areas occur. Such locations point to a consolidation of information, which leads to the formation of hierarchies in the network. Hierarchies play an important role in interconnection mechanisms, for as they indicate consolidation points in the network, they are likely to show where multiple technologies interconnect.

Redundancy

Redundancy, or the number of alternate paths in the network, is an important part of providing reliability in the network. Another commonly used term associated with redundancy is *path diversity*. Looking at the number of alternate paths is a fairly simple view of redundancy and is not end-to-end. To evaluate end-to-end redundancy, we must consider all components in the end-to-end path, which is often a complex task. A simple view of redundancy is often sufficient in determining criteria for interconnection.

During the requirements and flow analyses, we discussed and listed service metrics for reliability, but until this section, we have not been able to do much in the network design to support it. Where mission-critical applications and predictable/ guaranteed reliability occurs in flows, redundancy is likely to be required. There are two components of redundancy to consider: the number of paths at convergence points and the degree of redundancy provided by alternate paths. In providing alternate paths in the network, there will be locations where these paths converge. It is at these convergence points where redundancy effects the interconnection mechanism.

Low-Redundancy Path

In a low-redundancy path, the alternate path may not be immediately available when the primary path is disabled. There may be some configuration, possibly even human intervention, required to make the alternate path operational. This means that there will be a significant delay, on the order of minutes, while the alternate path is brought up. Furthermore, the performance characteristics of this alternate path may be significantly less than those of the primary path.

Low-redundancy paths are often known as *cold spares* . This is the same situation as when a failed component requires replacement from on-site spares before service can be restored.

Hybrid Mechanism

NHRP

The NHRP is one method to take advantage of a shorter, faster data-link layer path in NBMA networks. For example, if we have multiple IP subnetworks using the same NBMA infrastructure, instead of using the standard IP path from source to destination, NHRP can be used to provide a shorter path directly through the NBMA network

NBMA is one method for diverging from the standard IP routing model to optimize paths in the network. A strong case for the success of a method such as NHRP is the open nature of the ongoing work on NHRP by the Internet Engineering Task Force, along with its acceptance as part of the MPOA mechanism.

MPOA

MPOA applies NHRP to LANE to integrate LANE and multiprotocol environments and to allow optimized switching paths across networks or subnetworks. MPOA is an attempt to build scalability into ATM systems, through integrating switching and routing functions into a small number of NHRP/MPOA/LANE-capable routers and reducing the routing functions in the large number of edge devices.

MPOA builds on LANE to reduce some of the trade-offs discussed earlier with LANE. First, by integrating LANE with NHRP, paths between networks or subnetworks can be optimized over the ATM infrastructure. We now also have an integrated mechanism for accessing other network-layer protocols. The complexity trade-off with LANE is still there, however, and is increased with the integration of NHRP with MPOA. There are numerous control, configuration, and information flows in an MPOA environment, between MPOA clients (MPCs), MPOA servers (MPSs), and LECSs. In each of these devices reside network-layer routing/forwarding engines, MPOA client-server functions, LANE client functions, and possibly NHRP server functions.

It should be noted that, until link-layer and network-layer functions are truly integrated, perhaps through a common distributed forwarding table (combining what we think of today as switching and routing tables), where and how information flows are configured, established, and maintained by the network will be quite confusing. MPOA may be an answer toward this integration, as well as PNNI or NHRP.

POSSIBLE QUESTIONS

UNIT-II

PART-A **(20 MARKS)**

(Q.NO 1 TO 20 Online Examination)

PART –B **(5*6=30 MARKS)**

1. Explain about Developing a security and privacy plan.
2. Discuss in detail about the Criteria for Technology Evaluation.
3. What are the choices for Network Design.
4. Describe Shared medium.
5. Explain about Hybrid mechanism.
6. How to apply Interconnection Mechanism to the Design.

PART – C

CASE STUDY (COMPULSORY) **(1*10=10 MARKS)**

1. Discuss about various constraints for technology evaluation.
2. Give a brief notes on Switching.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Subject:Network architecture and Management
Subject Code:17CSP304
Class: II-M.Sc(CS) SEM:III
Objective type questions
UNIT-II

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	A____ analysis is a process used to determine which components of the system need to be protected.	security	servers	threat	network	**threat**
2	ACL stands for	Access control list	Access computer log	Access config list	ALU control list	**Access control list**
3	____protection is used to protect the devices from physical access,damage and theft.	servers	logical	physical	security	**physical**
4	ESP stands for	Encapsulating security payload	Encryption security protocol	Encryption server payload	Encapsulating server protocol	**Encapsulating security payload**
5	Ipsec tunnels are created between ___gateways.	ESP	AH	VPN	ACL	**VPN**
6	In transport mode the IP payload is encrypted using _____	AH	VPN	ESP	MAC	**ESP**
7	_______is a common method for building an isolated network across a internet.	Transport	Tunneling	SNMp	MAC	**Tunneling**
8	DES stands for	Data Encryption Standard	Data Enlarge stage	Data eliminate stage	digest encryption stage	**Data Encryption Standard**

9	____access consists of traditional dial-in,point-to-point sessions,and VPN connections	Local	Remote	physical	logical	**Remote**
10	________ medium is used in network design	local	shared	physical	remote	**shared**
11	plain text to cipher text is called_________	Decryptio n	Encryptio n	Remote	Logical	**Encryptio n**
12	ciphertext to plaintext is called______	Logical	Decryptio n	Encryptio n	Remote	**Decryptio n**
13	_______is a mechanism in network devices to explicitly deny packets at strategic points within the netwok.	Route filtering	Switch filtering	Packet filtering	Remote filtering	**Packet filtering**
14	Network _____describe the physical aspects of your network design.	plan	map	blueprints	location	**blueprints**
15	Which diagram shows the connectivity and relationships among network devices.	Map	Remote	physical	logical	**logical**
16	which plan is similar to a network diagram or blueprint but focuses on a specific function.	Performa nce	Routing	Compone nt	Architectu re	**Compone nt**
17	The _____is the ultimate product of the analysis,architecture and design processes.	Logical design	Physical design	Network design	Packet filtering	**Network design**
18	MPLS stands for _____	Multi-protocol label switching	Multi-physical label switching	Multi-protect label switch	Multi-protocol logical switching	**Multi-protocol label switching**

19	_____is the ability to refuse access to network resources.	Classification	VPN	Traffic	Admission Control	**Admission Control**
20	Which protocol is used to send a destination network unknown message back to originating hosts?	TCP	ARP	ICMP	SNMP	**ICMP**
21	A____is a networking device that forwards data packets between computer networks.	Switches	HUB	Router	VPN	**Router**
22	A____ is a network security system designed to prevent unauthorized access from a private network.	Switches	HUB	Router	Firewall	**Firewall**
23	A____is a device that connects devices together on a computer network	Switch	HUB	Router	Firewall	**Switch**
24	A_____bridge is networking that connects multiple network segments.	Switch	Bridge	Router	Firewall	**Bridge**
25	____are commonly used to connect segments of a LAN.	Switch	Hub	Bridge	Routers	**Hub**
26	____contains multiple ports.	Switch	Routers	Bridge	Hub	**Hub**
27	A___ network is a LAN in which all nodes are directly connected to a common central computer.	Hub	Star	Ring	Switch	**Star**

28	A____network is a network topology in which each node connects to exactly two other nodes forming a single continious pathway for signals through each node.	Hub	Star	Ring	Switch	**Ring**
29	Bus topology also called as _____topology.	Switch	Line	Ring	Star	**Line**
30	A topology in which nodes are directly connected to a common linear half-duplex link called a ________	Switch	Hub	Bus	Ring	**Bus**
31	A_____gateway is a network point that acts as an entrance to another network.	Hub	Bus	Gateway	Router	**Gateway**
32	A___mesh topology in which each node relays data for the network.	Hub	Mesh	Router	Hub	**Mesh**
33	The topology with highest reliability is ___ topology	LAN	WAN	MESH	HUB	**MESH**
34	____is a standard used to define a method of exchanging data over a computer network.	ICMP	ARP	Protocol	SNMP	**Protocol**

35	__determininh and persistently maintaining connection information along the path of a connection between source and destination.	Soft state	Hard state	IGP	Protocol	**Hard state**
36	__routing protocols that communicate routing information primarily within an AS	Soft state	Hard state	IGPs	Protocol	**IGPs**
37	RIP and RIPV2 IGPs are based on______algorithm	stack	queue	distance-vector routing	SNMP	**distance-vector routing**
38	____is used to determine and maintain the connection establishment for a short period of time.	Soft state	Hard state	IGPs	Protocol	**Soft state**
39	_____is used to optimize the availabe capacity of the network and its cost.	service planning	capacity planning	state planning	planning	**capacity planning**
40	_______is used to maximize the performance ,security and adaptability to users and management	service planning	capacity planning	state planning	planning	**service planning**
41	____ is used to describe a connectionless technology	stateful	state	hard state	stateless	**stateless**
42	A ___is a group of network addressable devices that can be reached by a single network address.	Domain	Broadcast domain	hard state	stateless	**Broadcast domain**

43	____method is used to isolate each area of the network.	isolate()	Black-box	White-box	Grey-box	**Black-box**
44	____ is a connection oriented technology.	stateful	state	hard state	stateless	**stateful**
45	segment the design into workable parts are called as _______	domains	region	areas	path	**areas**
46	NHRP stands for	Next-host Resolution Protocol	Next-hope Resolution Protocol	Next-high Resolution Protocol	Next-Hop Resolution Protocol	**Next-Hop Resolution Protocol**
47	when all devices on the network share the same physical medium is called as a ______	structure	domain	areas	shared medium	**shared medium**
48	____ provide support for end -to -end services	ATM	cell	shared medium	SNMP	**ATM**
49	Interconnection mechanisms that combine characteristics of switching and routing are termed as ________	Linear Mechanism	Non-linear Mechanism	Hybrid Mechanism	shared medium	**Hybrid Mechanism**
50	_____switching is based on flow information,dependent on the type of service required.	packet	service	areas	segment	**service**
51	____switching is used to describe mechanisms for optimizing paths in a hybrid environment.	packet	service	areas	segment	**service**

52	_____is also called as a path diversity.	Relay	Redundancy	switching	service	**Redundancy**
53	_____is forwarding information between segments of a network.	Relay	Redundancy	switching	service	**switching**
54	OSI stands for ________	open source interconnect	open service integertaed	open systems Interconnect	open source integerated	**open systems Interconnect**
55	LANE stands for______	LAN Emulation	LAN Ethernet	LAN Evolution	LAN End	**LAN Emulation**
56	State informations are kept in ____memory	Main	secondary	cache	ROM	**cache**
57	____ used in backbone networks in WAN	ATM	cell	shared medium	SNMP	**ATM**
58	Data communication system within a building or campus is _______	WAN	MAN	LAN	Router	**LAN**
59	OSPF Is an____	EGP	IGP	SNMP	ATM	**IGP**
60	____is a routing protocol	OSPF	ARP	MIME	IP	**OSPF**

SYLLABUS

UNIT III

Case history of Networking and Management: Challenges of Information Technology Managers – Goals organization and functions – Network and System Management – Network Management System Platform; SNMP Broadband and TMN Management: Network Management Standards & Model – Organization Information and Communication Model – ASN.1 – Encoding structure – Macros – Functional model; Organization and Information Model: Managed Networks – The History of Network Management – Internet Organization and standards – SNMP Model – The Organization and Information Model; Communication and Functional Model: The SNMP Communication Model – Functional Model.

Challenges of IT Managers

Managing a corporate network is becoming harder as it becomes larger and more complex. When we talk about network management, it includes not only components that transport information in the network, but also systems that generate traffic in the network.

The systems could be hosts, database servers, file servers, or mail servers. In the client–server environment, network control is no longer centralized, but distributed.

Computer and telecommunication networks are merging fast into converged network with common modes and media of transportation and distribution. As in the case of broadband networks, the IT manager needs to maintain both types of networks. Thus, the data communications manager functions and telecommunication manager functions have been merged to that of the IT manager.

With the explosion of information storage and transfer in the modern information era, management of information is also the responsibility of the IT manager, with the title of CIO, Chief Information Officer. For example, the IT manager needs to worry in detail about who can access the information and what information they can access, i.e., authentication and authorization issues of security management. The corporate network needs to be secured for privacy and content, using firewalls and encryption. Technology is moving so fast and corporate growth is so enormous, that a CIO has to keep up with new technologies and the responsibility for financial investment that the corporation commits to.

A good example of indeterminacy in the fast-moving technology industry was competition between the two technologies of Ethernet and ATM to desktop. ATM was predicted to be the way to go a few years ago. However, this has not been the case because of the development of enhanced capability and speed of Ethernet. Another current example related to this is the decision that one has to make in the adoption and deployment of WAN—whether it should be IP, ATM, or MPLS.

DAY 26

Network Management: Goals, Organization, and Functions

Network Management can be defined as Operations, Administration, Maintenance, and Provisioning (OAMP) of network and services. The Operations group is concerned with daily operations in providing network services. The network Administration is concerned with establishing and administering overall goals, policies, and procedures of network management. The Installation and Maintenance (I&M) group handles functions that include both installation and repairs of facilities and equipment. Provisioning involves network planning and circuit provisioning, traditionally handled by the Engineering or Provisioning department. We will describe each of these functions in this section. Although we continue to use the terminology of network management, in the modern enterprise environment this addresses all of IT and IT services.

Goal of Network Management

The goal of network management is to ensure that the users of network are provided IT services with a quality of service that they expect. Toward meeting this goal, the management should establish a policy to either formally or informally contract an SLA with users.

From a business administration point of view, network management involves strategic and tactical planning of engineering, operations, and maintenance of network and network services for current and future needs at minimum overall cost. There needs to be a well-established interaction between the various groups performing these functions. presents a top-down view of network management functions.

It comprises three major groups: (i) network and service provisioning, (ii) network and service operations, and (iii) network I&M. It is worth considering the different functions as belonging to specific administrative groups, although there are other ways of assigning responsibilities based on local organizational structure. Network provisioning is the primary responsibility of the Engineering group. The Customer Relations group deals with clients and subscribers in providing services planned and designed by the Engineering group. Network I&M is the primary responsibility of the Plant Facilities group..

Figure 1.22. Network Management Functional Groupings

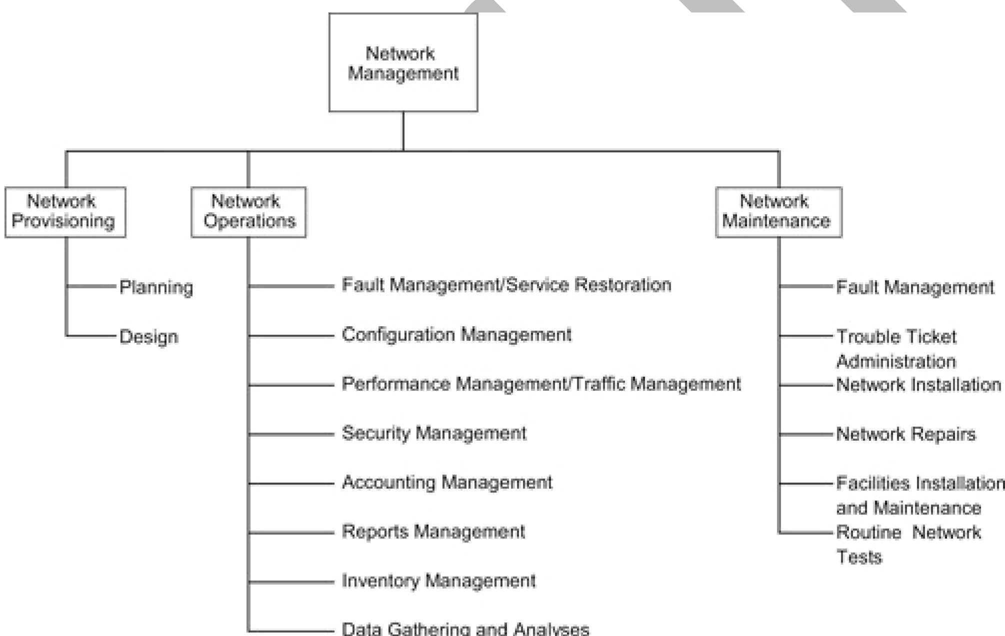
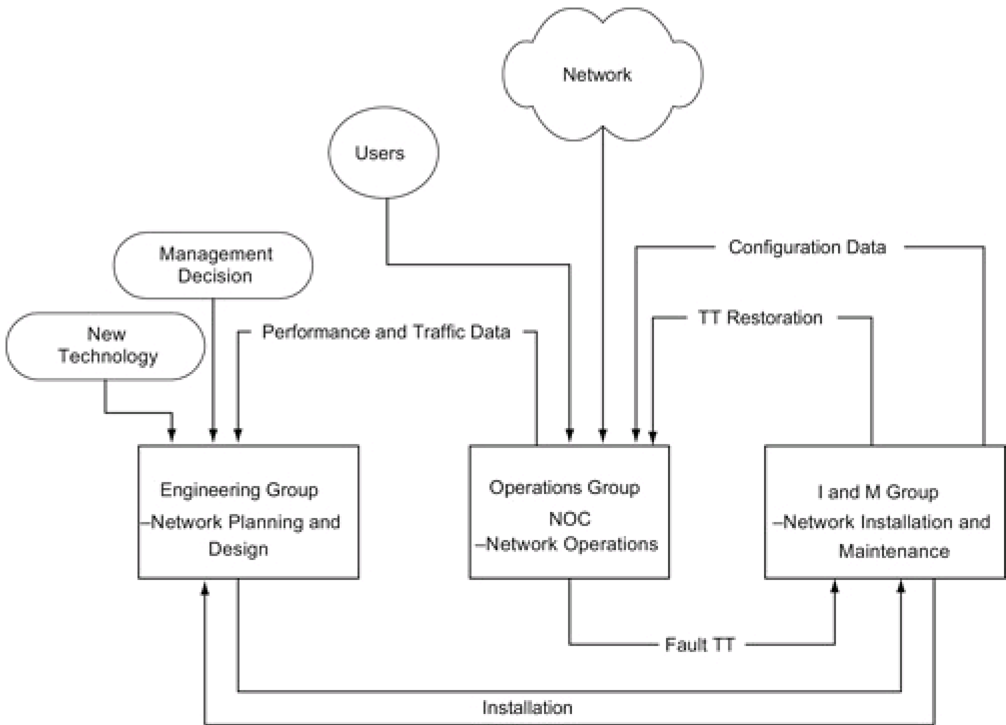


Figure 1.23. Network Management Functional Flow Chart



DAY 27

Network management system

A **network management system (NMS)** is a combination of hardware and software used to monitor and administer a computer network or networks.

Individual network elements (NEs) in a network are managed by an element management system.

Tasks and operational details

An NMS manages the network elements, also called managed devices. Device management includes faults, configuration, accounting, performance, and security (FCAPS) management. Management tasks include discovering network inventory, monitoring device health and status, providing alerts to conditions that impact system performance, and identification of problems, their source(s) and possible solutions.

Protocols

An NMS employs various protocols to accomplish these tasks. For example, SNMP protocol can be used to gather the information from devices in the network hierarchy.

Network statistics

The NMS collects device statistics and may maintain an archive of previous network statistics including problems and solutions that were successful in the past. If faults recur, the NMS can search the archive for the possible solutions.

Network management Platform

Configuration Management: There are three sets of configuration of the network. One is the static configuration and is the permanent configuration of the network. However, it is likely that the current running configuration, which is the second, could be different from that of the permanent configuration. Static configuration is one that the network would bring up if it is started from an idle status. The third configuration is the planned configuration of the future when the configuration data will change as the network is changed. This information is useful for planning and inventory management. The configuration data are automatically gathered as much as possible and are stored by NMSs. NOC has a display that reflects the dynamic configuration of the network and its status.

Performance Management: Data need to be gathered by NOC and kept updated in a timely fashion in order to perform some of the above functions, as well as tune the network for optimum performance. This is part of performance management. Network statistics include data on traffic, network availability, and network delay. Traffic data can be captured based on volume of traffic in various segments of the network. They can also be obtained based on different applications such as Web traffic, email, and network news, or based on transport protocols at various layers such as TCP, UDP, IP, IPX, Ethernet, TR, FDDI, etc.

Security Management can cover a very broad range of security. It involves physically securing the network, as well as access to the network by users. Access privilege to application software is not the responsibility of NOC unless the application is either owned or maintained by NOC. A security database is established and maintained by NOC for access to the network and network information.

Accounting Management administers cost allocation of the usage of network. Metrics are established to measure the usage of resources and services provided. The SNMP is the most popular protocol to acquire data automatically using protocol- and performance-analyzing tools.

DAY 28

Network Management Standards

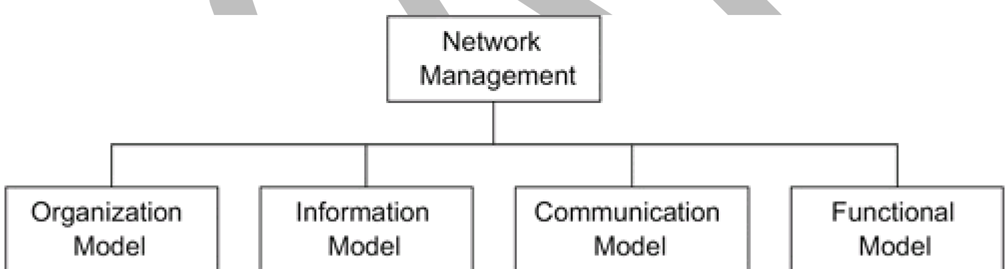
There are several network management standards that are in use today.

Table 3.1 lists four standards, along with a fifth class based on emerging technologies, and their salient points. The first four are the OSI model, the Internet model, TMN, and IEEE LAN/MAN. A detailed treatment of the various standards can be found in [Black, 1995]. The first category in Table 3.1, Open System Interconnection (OSI) management standard, is the standard adopted by the International Standards Organization (ISO). The OSI management protocol standard is Common Management Information Protocol (CMIP). The OSI management protocol has built-in services, Common Management Information Service (CMIS), which specify the basic services needed to perform the various functions. It is the most comprehensive set of specifications and addresses all seven layers. OSI specifications are structured and deal with all seven layers of the OSI Reference Model. The specifications are object oriented and hence managed objects are based on object classes and inheritance rules. Besides specifying the management protocols, CMIP/CMIS also address network management applications. Some of the major drawbacks of the OSI management standard were that it was complex and that the CMIP stack was large. Although these are no longer impediments to the implementation of the CMIP/CMIS network management, SNMP is the protocol that is extensively deployed.

Network Management Models

The OSI network model is an ISO standard and is most complete of all the models. It is structured and it addresses all aspects of management. Figure 3.1 shows an OSI network management architectural model that comprises four models. They are the organization model, the information model, the communication model, and the functional model. Although, the above classification is based on the OSI architectural model, and only parts of it are applicable to other models, it helps us understand the holistic picture of different aspects of network management.

Figure 3.1. OSl Network Management Model

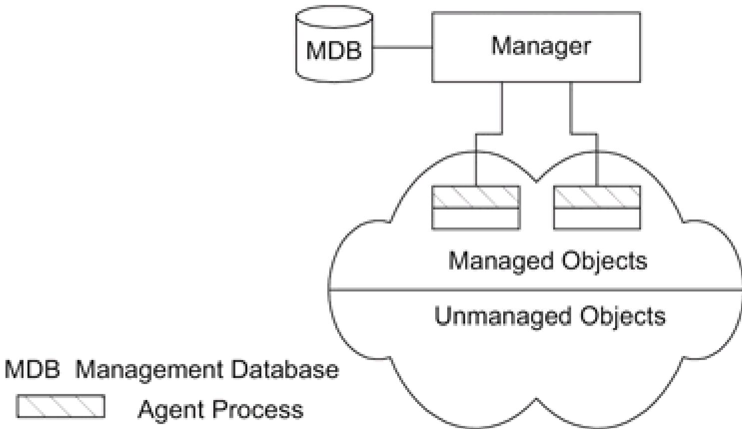


DAY 29

Organization Model

The organization model describes the components of network management and their relationships. Figure 3.2 shows a representation of a two-tier model. Network objects consist of network elements such as hosts, hubs, bridges, routers, etc. They can be classified into managed and unmanaged objects or elements. The managed elements have a management process running in them called an agent. The unmanaged elements do not have a management process running in them. For example, one can buy a managed or unmanaged hub. Obviously the managed hub has management capability built into it and hence is more expensive than the unmanaged hub, which does not have an agent running in it. The manager communicates with the agent in the managed element.

Figure 3.2. Two-Tier Network Management Organization Model



DAY 30

Information Model

An information model is concerned with the structure and storage of information. Let us consider, for example, how information is structured and stored in a library and is accessed by all. A book is uniquely identified by an International Standard Book Number (ISBN). It is a ten-digit number identification that refers to a specific edition of a specific book. For example, ISBN

0-13-437708-7 refers to the book "Understanding SNMP MIBs" by David Perkins and Evan McGinnis. We can refer to a specific figure in the book by identifying a chapter number and a figure number; e.g., Fig. 3.1 refers to Figure 1 in Chapter 3. Thus, a hierarchy of designation {ISBN, Chapter, Figure} uniquely identifies the object, which is a figure in the book. "ISBN," "Chapter," and "Figure" define the syntax of the three pieces of information associated with the figure; and the definition of their meaning in a dictionary would be the semantics associated with them.

The representation of objects and information that are relevant to their management forms the management information model. As discussed in Section 3.3, information on network components is passed between the agent and management processes. The information model specifies the information base to describe managed objects and the relationship between managed objects. The structure defining the syntax and semantics of management information is specified by Structure of Management Information (SMI). The information base is called the Management Information Base (MIB). The MIB is used by both agent and management processes to store and exchange management information.

The MIB associated with an agent is called an agent MIB and the MIB associated with a manager is designated as the manager MIB. The manager MIB consists of information on all the network components that it manages; whereas the MIB associated with an agent process needs to know only its local information, its MIB view. For example, a county may have many libraries. Each library has an index of all the books in that location—its MIB view. However, the central index at the county's main library, which manages all other libraries, has the index of all books in all the county's libraries—global manager MIB view.

DAY 31

Communication Model

Address the model associated with how the information is exchanged between systems. Management data are communicated between agent and manager processes, as well as between manager processes. Three aspects need to be addressed in the communication of information between two entities: transport medium of message exchange (transport protocol), message format of communication (application protocol), and the actual message (commands and responses).

In the former, visual and audio media are the transport mechanisms, and electronic exchange is used in the latter. The communication at the application level could be exchanged in English, Spanish, or any other mutually understandable language between the two. This would be the application-level protocol that is decided between Azita and Roberto. Finally, there are messages exchanged between Azita and Roberto. For example, Azita could request what cars are available and Roberto would respond with the cars that are in stock. Azita could then set a price range and Roberto responds with cars that match the price range. These exchanged messages are the commands/requests/operations and responses/notifications. They can be considered services requested by Azita and provided by Roberto.

Abstract Syntax Notation One: ASN.1

In both the information model and the communication model, discussed in the previous sections, we have addressed functions. In these models, SMI needs to be specified syntactically and semantically, which will be the content of this section.

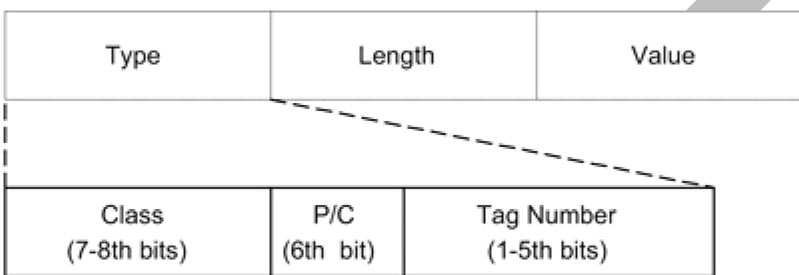
It is important for communication among systems that a formalized set of rules is agreed upon on the structure and meaning of the language of communication, namely syntax and semantics of the language. There are numerous sets of application and transport protocols. Thus, it is beneficial to choose a syntactical format for the language that specifies the management protocol in the application layer, which is transparent to the rest of the protocol layers. One such format is an old and well-proven format, Abstract Syntax Notation One, ASN.1. We will introduce ASN.1 here to the extent needed to understand its use in network management.

DAY 32

Encoding Structure

The ASN.1 syntax containing the management information is encoded using the BER defined for the transfer syntax. The ASCII text data are converted to bit-oriented data. We will describe one specific encoding structure, called TLV, denoting Type, Length, and Value components of the structure. This is shown in Figure 3.18. The full record consists of type, length, and value.

Figure 3.18. TLV Encoding Structure



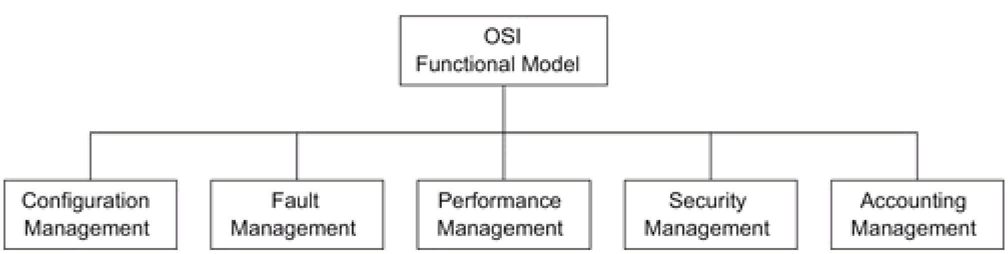
Macros

The data types and values that we have so far discussed use ASN.1 notation of syntax directly and explicitly. ASN.1 language permits extension of this capability to define new data types and values by defining ASN.1 macros. The ASN.1 macros also facilitate grouping of instances of an object or concisely defining various characteristics associated with an object.

Functional Model

The functional model component of an OSI model addresses user-oriented applications. They are formally specified in the OSI model and are shown in Figure 3.22. The model consists of five models: configuration management, fault management, performance management, security management, and accounting management. Part III of the book is devoted to the application aspects of network management.

Figure 3.22. Network Management Functional Model



DAY 33

Managed Network: Case Histories and Examples

The real-world experiences that, demonstrate the power of network management before learning how it is accomplished. As with any good technology, the power of technology could result in both positive and negative results. Atomic energy is a great resource, but an atomic bomb is not! An NMS is a powerful tool, but it could also bring your network down, when not "managed" properly.

As part of my experience in establishing a network operations center, as well as in teaching a network management course, One of the visits was to an AT&T Network Control Center, which monitored the network status of their network in the entire eastern half of the United States. We could see the network of nodes and links on a very large screen, mostly in green indicating that the network was functioning well.

Monitoring was done by the NMSs and operations support systems without any human intervention. Even the healing of the network after a failure was accomplished automatically—self-healing network as it is called. Any persistent alarm was pursued by the control center, which tested the network remotely using management tools to isolate and localize the trouble. It was an impressive display of network management capability.

History of SNMP Management

SNMP management began in the 1970s. Internet Control Message Protocol (ICMP) was developed to manage Advanced Research Project Agency NETwork (ARPANET). It is a mechanism to transfer control messages between nodes. A popular example of this is Packet Internet Groper (PING), which is part of the TCP/IP suite now. PING is a very simple tool that is used to investigate the health of a node and the robustness of communication with it from the source node. It started as an early form of network-monitoring tool.

ARPANET, which started in 1969, developed into the Internet in the 1980s with the advent of UNIX and the popularization of client–server architecture. Data were transmitted in packet form using routers and gateways. TCP/IP-based networks grew rapidly, mostly in defense and academic communities and in small entrepreneurial companies taking advantage of the electronic medium for information exchange. National Science Foundation officially dropped the name ARPANET in 1984 and adopted the name Internet.

DAY 34

Internet Organizations and Standards

Organizations

We mentioned in the previous section that the IAB recommended the development of SNMP. The IAB was founded in 1983 informally by researchers working on TCP/IP networks. Its name was formally changed from the Internet Advisory Board to the Internet Architecture Board in 1989 and was designated with the responsibility to manage two task forces—the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).

The IRTF is tasked to consider long-term research problems in the Internet. It creates focused, long-term, and small research groups working on topics related to Internet protocols, applications, architecture, and technology.

SNMP Model

We described an example of a managed network in Section 4.1. We saw that numerous management functions were accomplished in that example. We will now address how this is done in SNMP management. An NMS acquires a new network element through a management agent or monitors the ones it has acquired. There is a relationship between manager and agent. Since one manager is responsible for managing the designated functions of many agents, it is hierarchical in structure. The infrastructure of the manager–agent and the SNMP architecture that it is based on form the organization model.

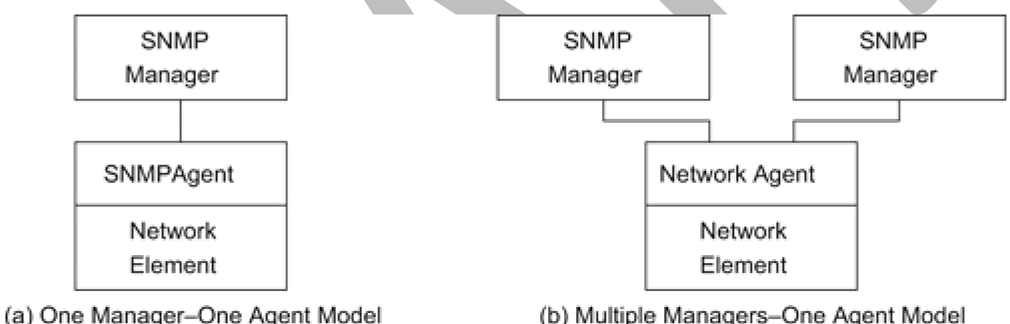
Information is transmitted and is received by both the manager and the agent. For example, when a new network element with a built-in management agent is added to the network, the discovery process in the network manager broadcasts queries and receives positive response from the added element. The information must be interpreted both semantically and syntactically by the agent and the manager. We covered the syntax, ASN.1, in Section 3.7. Definition of semantics and syntax form the basis of the information model. We present a detailed definition of a managed object, rules for the SMI, and a virtual information database, MIB, which groups managed objects and provides a relational framework.

DAY 35

Organization Model

The initial organization model of SNMP management is a simple two-tier model. It consists of a network agent process, which resides in the managed object, and a network manager process, which resides in the NMS and manages the managed object. This is shown in Figure 4.5(a). Both the manager and the agent are software modules. The agent responds to any management system that communicates with it using SNMP. Thus, multiple managers can interact with one agent as shown in Figure 4.5(b)

Figure 4.5. Two-Tier Organization Model



SNMP Communication Model

The SNMPv1 communication model defines specifications of four aspects of SNMP communication: architecture, administrative model that defines data access policy, SNMP protocol, and SNMP MIB. Security in SNMP is managed by defining community, and only members belonging to the same community can communicate with each other. A manager can belong to multiple communities and can thus manage multiple domains. SNMP protocol specifications and messages are presented. SNMP entities are grouped into an SNMP MIB module.

SNMP Architecture

The SNMP architectural model consists of a collection of network management stations and network elements or objects. Network elements have management agents built in them, if they are managed elements. The SNMP communications protocol is used to communicate information between network management stations and management agents in the elements.

Functional Model

There are no formal specifications of functions in SNMPv1 management. Application functions are limited, in general, to network management in SNMP and not to the services provided by the network.

There are five areas of functions (configuration, fault, performance, security, and accounting) addressed by the OSI mode. Some configuration functions, as well as security and privacy-related issues, were addressed as part of the SNMP protocol entity specifications in the previous section. For example, the override function of traps is one of the objects in the SNMP group, which has the access privilege of read and write and hence can be set remotely. Security functions are built in as part of the implementation of the protocol entity. Community specifications and authentication scheme partially address these requirements.

POSSIBLE QUESTIONS

UNIT-III

PART-A **(20 MARKS)**

(Q.NO 1 TO 20 Online Examination)

PART –B **(5*6=30 MARKS)**

1. Discuss about Challenges of Information Technology Managers.
2. Explain in detail about goals organization and functions.
3. Describe about SNMP Broadband and TMN Management.
4. Discuss the concept of Macros.
5. What is Functional model?
6. Explain about Internet Organization and standards.
7. Explain about SNMP Model.

PART – C

CASE STUDY (COMPULSORY) **(1*10=10 MARKS)**

1. Discuss about the current SNMP scenario.
2. Explain in detail about Network Management System Platform.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Subject:Network architecture and Management
Subject Code:17CSP304
Class: II-M.Sc(CS) SEM:III
Objective type questions
UNIT-III

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	Network management can be defined as ___________	OMA&P	OAM&P	SNMP	ARP	**OAM&P**
2	NMS stands for_________	Network Management system	Network Manager system	Network Management server	Network Management service	**Network Management system**
3	OSI classified the network management functions into ______ types.	3	6	5	10	**5**
4	NOC stands for______	Network Operation Center	New Operation Center	Network Opcode Center	Network Operation Computer	**Network Operation Center**
5	____provisioning consists of network planning and design .	Architecture	Performance	Network	Security	**Network**
6	The network which recover itself from failure is called_____	Self-handling	Fault handling	Self-healing	self-service	**Self-healing**

7	____is used to identify and track the fault in the network.	NOC	Trouble Ticket	Service restoratio n	Security	**Trouble Ticket**
8	How many types of configurations are there In configuration Management ?	5	4	3	6	**3**
9	The ___configuration is one that would come up if the network is started from idle status.	dynamic	static	planned	configure d	**static**
10	_____Management can cover a very broad range of security which includes physically securing the network.	static	security	privacy	fault	**security**
11	____is involved in all the mechanism of the network management.	static	LOC	NOC	fault	**NOC**
12	MIB stands for_____	Manage ment Informati on Base	Middle Idle Block	Manage ment Introduct ionBase	Middle Informati on Block	**Managem ent Informati on Base**
13	____is called as a network element.	Routers	Fault handling	security	NOC	**Routers**
14	The managed elements have a management process running in them it is called as an_______	Manager	Router	Agent	NONE	**Agent**

15	Network objects consist of _____ such as hosts,hubs,bridges and routers.	Network register	Network Manager	Network Elements	Network Domain	**Network elements**
16	OSI specifications are object-oriented and hence a managed object belongs to an ________	status	access	Object class	Object	**Object class**
17	The ____of an object defines the external perspective of the object.	class	operations	attribute	Object	**attribute**
18	_____is used to model the object.	class	operations	attribute	Syntax	**Syntax**
19	____ exhibited by its response to an operation.	class	Behaviour	attribute	Syntax	**Behaviour**
20	The applications in the manager module initiate _____ to the agent in the internet model.	Response	Request	Both A and B	NONE	**Request**
21	CMIS stands for____	Common Management Information Protocol	Common Maintain Information Protocol	Common Mask Information Protocol	Correct Management Information Protocol	**Common Management Information Protocol**
22	The OSI Model uses ____ along with common management informative services.	SNMP	ICMP	CMIP	ARP	**CMIP**

23	___ and___ specify the management communication protocol for OSI and internet management.	ARP & DES	AES &DES	CMIP & SNMP	ICMP	**CMIP & SNMP**
24	_____ represents the set of rules for communicating information between system.	Syntax	Abstract Syntax	Transfer Syntax	Semantic	**Transfer Syntax**
25	____ is set of rules used to specify data types and structure for storage of information.	Syntax	Abstract Syntax	Transfer Syntax	Semantic	**Abstract Syntax**
26	_____ is a type derived from another type that is given a new tag id	Tag	Tagged type	UnTagged type	NULL	**Tagged type**
27	BER stands for	Basic encoding rules	Basic email rules	Basic encompose rules	Block encoding rules	**Basic encoding rules**
28	The syntax that contains the management information is encoded using the ____ for transfer	BER	ASCII	ACL	NONE	
29	The configuration data is gathered automatically and stored by ___ at the NOC.	BER	ASCII	ACL	NMS	**NMS**

30	______management addresses the setting and changing of configuration of network and their components.	Fault	Performa nce	Configur ation	Security	**Configura tion**
31	_____ managent is used to set up the Parameters for the network.	Fault	Performa nce	Configur ation	Security	**Configura tion**
32	_____ management involves detection and isolation of the problem causing the failure in the network.	Fault	Performa nce	Configur ation	Security	**Fault**
33	_______management is concerned with the performance and behaviour of the network.	Fault	Performa nce	Configur ation	Security	**Performa nce**
34	______management deals with access control and physical security.	Fault	Performa nce	Configur ation	Security	**Security**
35	____ management deals with cost and administration of the network.	Accounti ng	Performa nce	Configur ation	Security	**Accountin g**
36	Tags in the ______ are specified to Application.	Universa l class	Applicati on class	none	both a and b	**Applicatio n class**

37	_______class ia similar to the gloabal variable in a software program.	Universal class	Application class	none	both a and b	**Universal class**
38	Recovery from failure is called as _______	Response	Request	Restoration	both a and b	**Restoration**
39	Most common and serious problems of networks are __________	Assigning duplicate IP address	interface problem	traffic overload	connectivity failures	**connectivity failures**
40	The operation group is concerned with _____________	daily operations are providing N/W services	establishing & administrating goals,policies,&procedure of N/W management	functions including both installation & repairs	planning & provisiioning of circuits	**daily operations are providing N/W services**
41	Administration is concerned with ______________	daily operations are providing N/W services	establishing & administrating goals,policies,&procedure of N/W management	functions including both installation & repairs	planning & provisiioning of circuits	**establishing & administrating goals,policies,&procedure of N/W management**

42	Installation & maintanence group handles__________	daily operations are providing N/W services	establishing & administrating goals,policies,&procedure of N/W management	functions including both installation & repairs	planning & provisiioning of circuits	**functions including both installation & repairs**
43	Provisioning involves _______________	daily operations are providing N/W services	establishing & administrating goals,policies,&procedure of N/W management	functions including both installation & repairs	planning & provisiioning of circuits	**planning & provisiioning of circuits**
44	Goal of N/W management is __________	network prvisioning	network operations	to ensure that the users of a N/W aservice IT services with expected qos	network installation & service	**to ensure that the users of a N/W aservice IT services with expected qos**
45	N/W management function comprises of __________	network prvisioning	network operations	network installation &maintanence	all the three	**all the three**
46	I&M stands for __________	installation & maintanence	Installation and monitoring	installation & maintanence	security	**installation & maintanence**

47	The ______message is generated by agent process	get next	trap	get response	get request	**get response**
48	The message generated is called_________	event	trap	set request	get request	**event**
49	A ________is unsolicited message generated by an agent process without a message	trap	event	get response	get request	**trap**
50	______deal with structure management information and management information basic	the information model	the organisation model	the SNMP model	SMTP	**the information model**
51	SMI defence by_______________	frfc1213	rfc1253	rfc1155	rfc2012	**rfc1155**
52	MIBS speecified by_____________	Rfc1155	rfc1253	Rfc1213	rfc2012	**Rfc1213**
53	The_______defencing the name is mnemonic and is all in lowercase letters	descriptor	object identifier	octet string	component object	**descriptor**
54	__________are atomic	primitive types	define types	constructed types	component object	**primitive types**
55	The_______data type is used to specify other binary as textual information that is 8 bit long	octet string	integer	null	component object	**octet string**

56	__________is an application wide datatype and is a non negative integer	counter	gauge	time tick	component object	**counter**
57	_________used to define an information module	module identity	object type	notification type	component object	**module identity**
58	The_____are designed to help function of new data type is sm1v2	texual convention	object definitions	module definition	component object	**texual convention**
59	The ________ macro define a group of related object is MIB module	object group	notificatio group	module compliance	component object	**object group**
60	________is application wide data type that supports the capability to pass arbitary ASN! Syntax	timestick	OF	object	opaque	**opaque**

SYLLABUS

UNIT IV

SNMPv2 Management: Major changes – System architecture – Structure of Management Information – Management Information Base – SNMPv2 protocol – Compatibility; RMON: Remote monitoring – RMON1 – RMON2 – ATM remote monitoring; Broadband Network Management: ATM Networks - Network and Services – ATM Technology – ATM Network Management; Telecommunication Management Network: Operations systems – Conceptual model – Standards – Architecture – TMN Management service architecture – Integrated view of TMN – Implementation issues.

Major Changes in SNMPv2

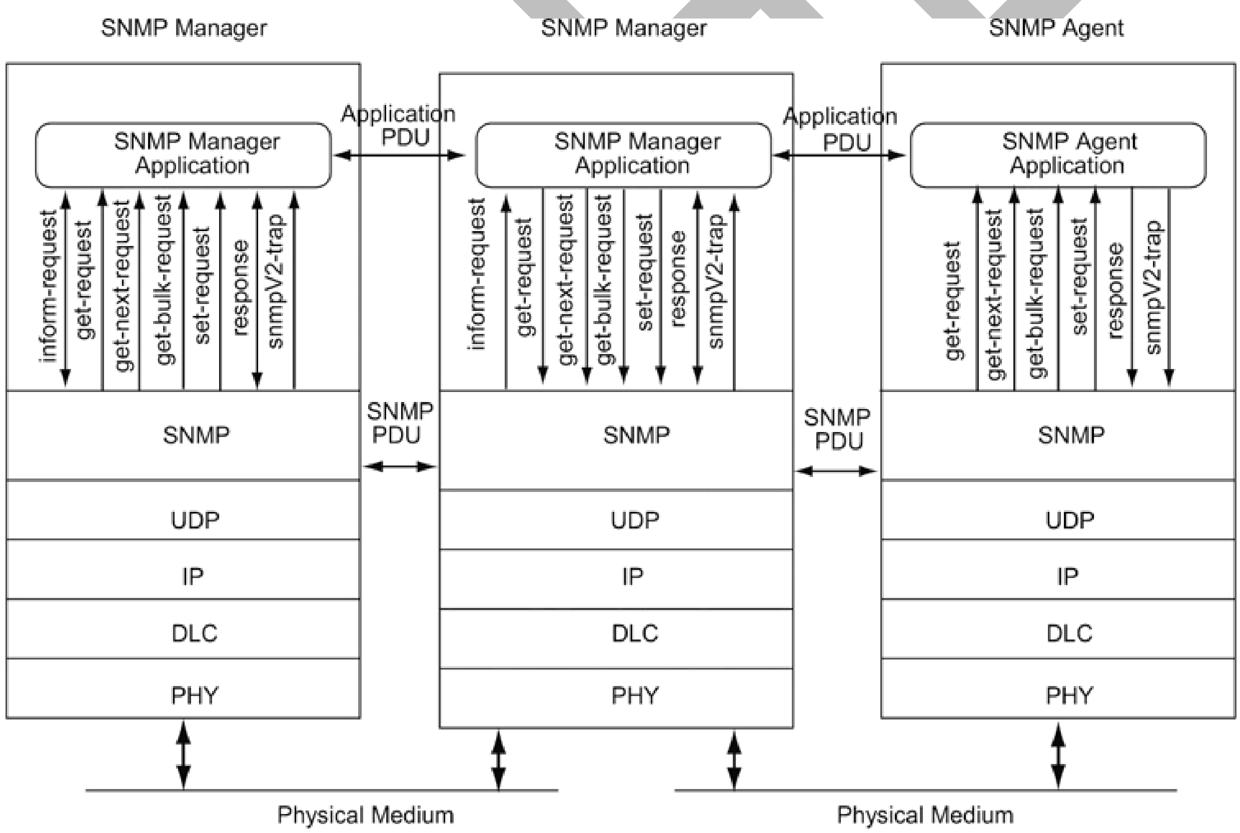
Several significant changes were introduced in SNMPv2. One of the most significant changes was to improve the security function that SNMPv1 lacked. Unfortunately, after significant effort, due to lack of consensus, this was dropped from the final specifications, and SNMPv2 was released with the rest of the changes. The security function continued to be implemented on an administrative framework based on the community name and the same administrative framework as in SNMPv1 was adopted for SNMPv2. SNMPv2 Working Group has presented a summary of the community-based Administrative Framework for the SNMPv2 framework, and referred to it as SNMPv2C in RFC 1901. RFC 1902 through RFC 1907 present the details on the framework. There are significant differences between the two versions of SNMP, and unfortunately version 2 is not backward compatible with version 1. RFC 1908 presents implementation schemes for the coexistence of the two versions.

The basic components of network management in SNMPv2 are the same as version 1. They are the agent and the manager, both performing the same functions. The manager-to-manager communication, Thus, the organizational model in version 2 remains essentially the same. In spite of the lack of security enhancements, major improvements to the architecture have been made in SNMPv2. We will list some of the highlights that would motivate the reader's interest in SNMPv2.

SNMPv2 System Architecture

SNMPv2 system architecture looks essentially the same as that of version 1. However, there are two significant enhancements in SNMPv2 architecture, which are shown in Figure 6.2. First, there are seven messages instead of five. second, two manager applications can communicate with each other at the peer level. Another message, report message, is missing from Figure 6.2. This is because even though it has been defined as a message, SNMPv2 Working Group did not specify its details. It is left for the implementers to generate the specifications. It is not currently being used and is hence omitted from the figure.

Figure SNMPv2 Network Management Architecture



SNMPv2 Structure of Management Information

There are several changes to SMI in version 2, as well as enhancements to SMIv2 over that of SMIv1. As stated earlier, SMIv2 [RFC 1902] is divided into three parts: module definitions, object definitions, and notification definitions.

We introduced the concept of a module in, which is a group of assignments that are related to each other. Module definitions describe the semantics of an information module and are formally defined by an ASN.1 macro, MODULE-IDENTITY.

SNMv2 Management Information Base

Two new MIB modules, security and SNMPv2, have been added to the Internet MIB. The SNMPv2 module has three submodules: snmpDomains, snmpProxys, and snmpModules. snmpDomains extends the SNMP standards to send management messages over transmission protocols other than UDP, which is the predominant and preferred way of transportation [RFC 1906]. Since UDP is the preferred protocol, systems that use another protocol need a proxy service to map on to UDP. Not much work has been done on snmpProxys, as of now.

There are changes made to the core MIB-II defined in SNMPv1. An overview of the changes to the Internet MIB and their relationship. The system module and the snmp module under mib-2 have significant changes as defined in RFC 1907. A new module snmpMIB has been defined, which is {snmpModules 1}. There are two modules under snmpMIB: snmpMIBObjects and snmpMIBConformance.

SNMPv2 Protocol

SNMPv2 protocol operations are based on a community administrative model, which is the same as in SNMPv1. This was discussed in Section 5.2.2. We presented SNMPv2 protocol operations from a system architecture view. In this section we will discuss details of PDU data structures and protocol operations.

Data Structure of SNMPv2 PDUs

The PDU data structure in SNMPv2 has been standardized to a common format for all messages. This improves the efficiency and performance of message exchange between systems. The significant improvement is bringing the trap data structure in the same format as the rest.

The generic PDU message structure of SNMPv1. The PDU type is indicated by an INTEGER. The error-status and error-index fields are either set to zero or ignored in the get-request, get-next-request, and set messages. The error-status is set to zero in the get-response message if there is no error; otherwise the type of error is indicated. The PDU and error-status The error-index is set to zero if there is no error. If there is an error, it identifies the first variable binding in the variable-binding list that caused the error message. The first variable binding in a request's variable-binding list is index one, the second is index two, etc.

Compatibility with SNMPv1

An SNMP proxy server, in general, converts a set of non-SNMP entities into a set of SNMP-defined MIB entities. Unfortunately, SNMPv2 MIB is not backward compatible with SNMPv1 and hence requires conversion of messages. SNMPv2 IETF Working Group has proposed two schemes for migration from SNMPv1 to SNMPv2: bilingual manager and SNMP proxy server.

Bilingual Manager

One of the migration paths to transition to SNMPv2 from version 1 is to implement both SNMPv1 and SNMPv2 interpreter modules in the manager with a database that has profiles of the agents' version. The interpreter modules do all the conversions of MIB variables and SNMP protocol operations in both directions. The bilingual manager does the common functions needed for a management system. The SNMP PDU contains the version number field to identify the version.

SNMP Management: RMON

The success of SNMP management resulted in the prevalence of managed network components in the computer network. SNMPv1 set the foundation for monitoring a network remotely from a centralized network operations center (NOC) and performing fault and configuration management. However, the extent to which network performance could be managed was limited. The characterization of the performance of a computer network is statistical in nature. This led to the logical step of measuring the statistics of important parameters in the network from the NOC and the development of remote monitoring (RMON) specifications.

What is Remote Monitoring?

We saw examples of SNMP messages going across the network between a manager and an agent. It is a passive operation and does nothing to the packets, which continue to proceed to their destinations. This is called monitoring or probing the network and the device that does the function is called the network monitor or the probe. Let us distinguish between the two components of a probe: (1) physical object that is connected to the transmission medium and (2) processor, which analyzes the data. If both are at the same place geographically, it is a local probe, which is how sniffers used to function.

The monitored information gathered and analyzed locally can be transmitted to a remote network management station. In such a case, remotely monitoring the network using a probe is referred to as remote network monitoring or RMON. fiber-distributed data interface (FDDI) backbone network with a local Ethernet LAN. There are two remote LANs, one a token-ring LAN and another, an FDDI LAN, connected to the backbone network. The network management system (NMS) is on the local Ethernet LAN. There is either an Ethernet probe or an RMON on the Ethernet LAN monitoring the local LAN. The FDDI backbone is monitored by an FDDI probe via the bridge and Ethernet LAN. A token-ring probe monitors the token-ring LAN. It communicates with the NMS via routers and the wide area network (WAN). The remote FDDI is monitored by the built-in probe on the router. The FDDI probe communicates with the NMS via the WAN. All four probes that monitor the four LANs and communicate with the NMS are RMON devices.

RMON1

RMON1 is covered by RFC 1757 for Ethernet LAN and RFC 1513. There are two data types introduced as textual conventions, and ten MIB groups (rmon 1 to rmon 10.

RMON1 Textual Conventions

Two new data types that are defined in RMON1 textual conventions are OwnerString and EntryStatus. Both these data types are extremely useful in the operation of RMON devices. RMON devices are used by management systems to measure and produce statistics on network elements. We will soon see that this involves setting up tables that control parameters to be monitored. Typically, there is more than one management system in the network, which could have permission to create, use, and delete control parameters in a table. Or, a human network manager in charge of network operations does such functions. For this purpose, the owner identification is made part of the control table defined by the OwnerString data type. The EntryStatus is used to resolve conflicts between management systems in manipulating control tables.

RMON2

RMON1 dealt primarily with data associated with the OSI data link layer. The success and popularity of RMON1 led to the development of RMON2. RMON2 [RFC 2021] extends the monitoring capability to the upper layers, from the network layer to the application layer. The term application level is used in the SNMP RMON concept to describe a class of protocols, and not strictly the OSI layer 7 protocol. The error statistics in any layer include all errors below the layer, down to the network layer. For example, the network layer errors do not include data link layer errors, but the transport layer errors include the network layer errors.

Several of the groups and functions in RMON2 at higher layers are similar to that of the data link layer in RMON1. We will discuss the groups and their similarity here.

ATM Remote Monitoring

Rmon advantages for gathering statistics on Ethernet and token-ring LANs. RMON1 dealt with the data link layer and RMON2 with higher-level layers. IETF RMON MIBs have been extended to perform traffic monitoring and analysis for ATM networks (RMON MIB framework for the extensions, as portrayed by the ATM Forum. Switch extensions for RMON and ATM RMON define RMON objects at the “base” layer, which is the ATM sublayer level. ATM protocol IDs for RMON2 define additional objects needed at the higher-level layers [RFC 2074].

Broadband Network and Services

As new technologies emerge, service providers offer new services to commercial and residential communities using those technologies. In turn, offering of new services by service providers is propelling information technology to new heights. This is especially true in broadband technology. Let us first define what broadband network and services are, which we briefly introduced in Section 2.7.

The broadband network and the narrowband Integrated Services Digital Network (ISDN) are multimedia networks that provide integrated analog and digital services over the same network. Narrowband ISDN is low-bandwidth network that can carry two 56 kilobaud rate channels. The broadband network can transport very high data rate signals. The narrowband ISDN is also known as Basic ISDN.

ATM Technology

The ATM has helped bring about the merger of computer and telecommunication networks. There are five important concepts comprising ATM technology [Keshav, 1997]. They are (1) virtual path–virtual circuit (VP–VC), (2) fixed packet size or cells, (3) small packet size, (4) statistical multiplexing, and (5) integrated services. The implementation of these concepts in a network that is made up of ATM switches achieves high-speed network that can transport all three services (voice, video, and data). The desired quality of service is provided to individual streams (unlike the current Internet) at the same time. The network is also easily scaleable. The ATM Forum, an organization that specifies standards for ATM implementation, has also provided a framework for network management.

ATM Network Management

Broadband network management consists of managing the WAN using ATM technology, as well as access networks from the central office to the home. We will discuss the former in this section. We will discuss access technology management in the next chapter.

WAN facilities are provided by public service providers, who perform the following management functions: operation, administration, maintenance, and provisioning (OAMP).

Typically, a large enterprise or corporation services its private network. However, they too use the public service providers' facilities to transport information over a long distance. This is referred to as public network. ATM networks are classified as private and public networks. The standards for the management of each and the interactions between them have been addressed by the ATM Forum, which is an international organization accelerating cooperation on ATM technology. The user interface to the private network is the private user-network interface (UNI), and the interface to the public network is the Public UNI.

Telecommunications Management Network

Why TMN?

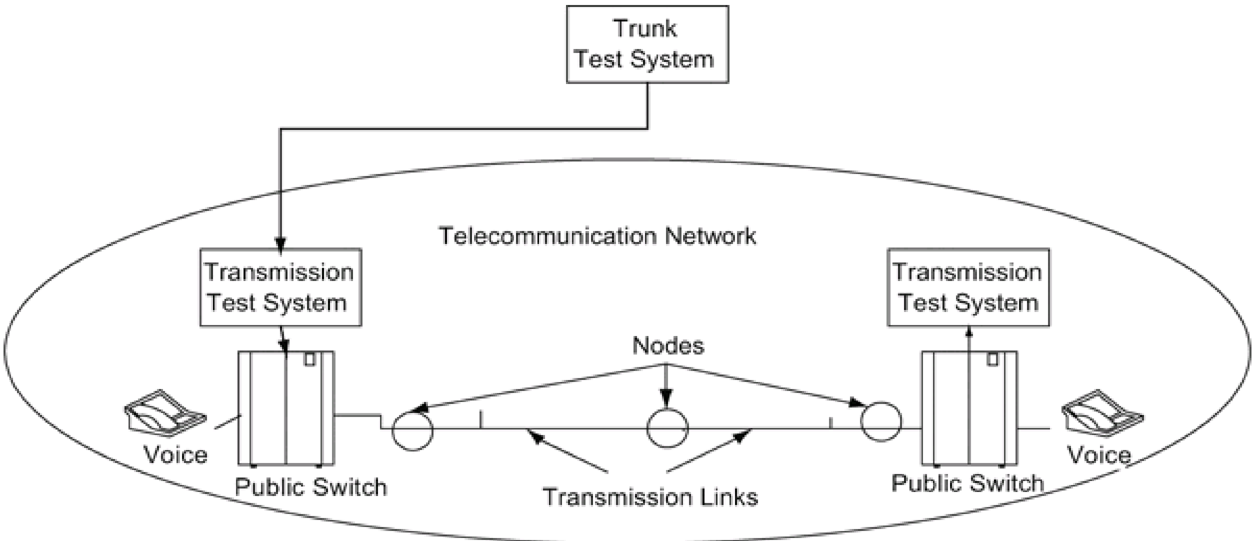
With the proliferation of SNMP management that has left OSI network management by the wayside, we can ask the question why we are spending time on discussing TMN. Historically, TMN was born out of necessity to extend the private and proprietary, but well-developed network management systems, and make them interoperable. In those days, the large telecommunication organizations referred to the systems that maintained the network and network elements as operations systems. ITU-T formed a working group in 1988 to develop a framework for TMN. ISO was also working on standardizing network management with OSI management framework using CMIP. With globalization and deregulation of the telecommunications industry, the urgency for interoperability of network management systems was strongly felt. With the slow progress of these standards bodies, industry-sponsored groups such as the Network Management Forum started developing standards in parallel to speed up the process.

Unfortunately, the standards and frameworks developed were so complex and expensive to implement using the then-present technology, TMN and OSI network management never got off the ground. However, TMN is the only framework that addressed not only management of network elements, but also the management of network, service, and business. These later issues are so critical in today's business environment with numerous network and service providers (they are not the same as they used to be). Customer service, quality, and cost of business form a three-legged stool [Adams and Willetts, 1996]. You knock out one leg and the stool falls down. TMN framework not only addresses the management of quality of network and network elements, but also service management and business management.

Operations Systems

TMN is built using the building blocks of the operations support system. The use of the terminology, operations support system, in the telephone industry was changed to operations system, as it is also used to control the network and network elements. For example, user configurable parameters in the ATM network can be controlled by users via the M3 interface. The operations system (let us not confuse operations system with operating system) does not directly play a role in the information transfer, but helps in the OAMP of network and information systems. Two examples of operations systems that are used in the operation of telephone network and services: trunk test system and traffic measurement system. The terminology of OSS is back in common use again. We will use both terms in this chapter.

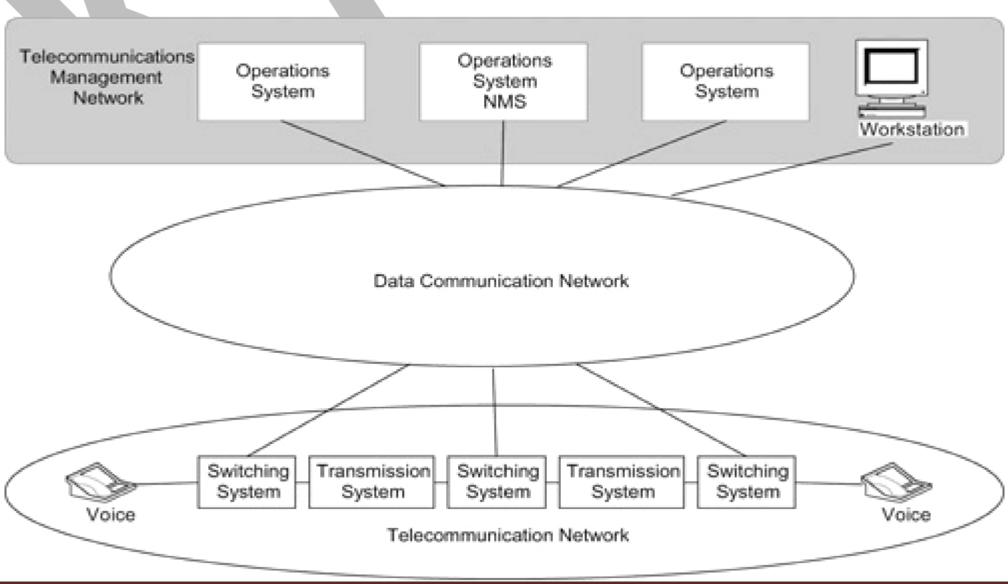
Figure. Operations Support System for Network Transmission



TMN Conceptual Model

From a TMN point of view, the network management system is treated as an operations support system. It manages the data communication and telecommunication network.

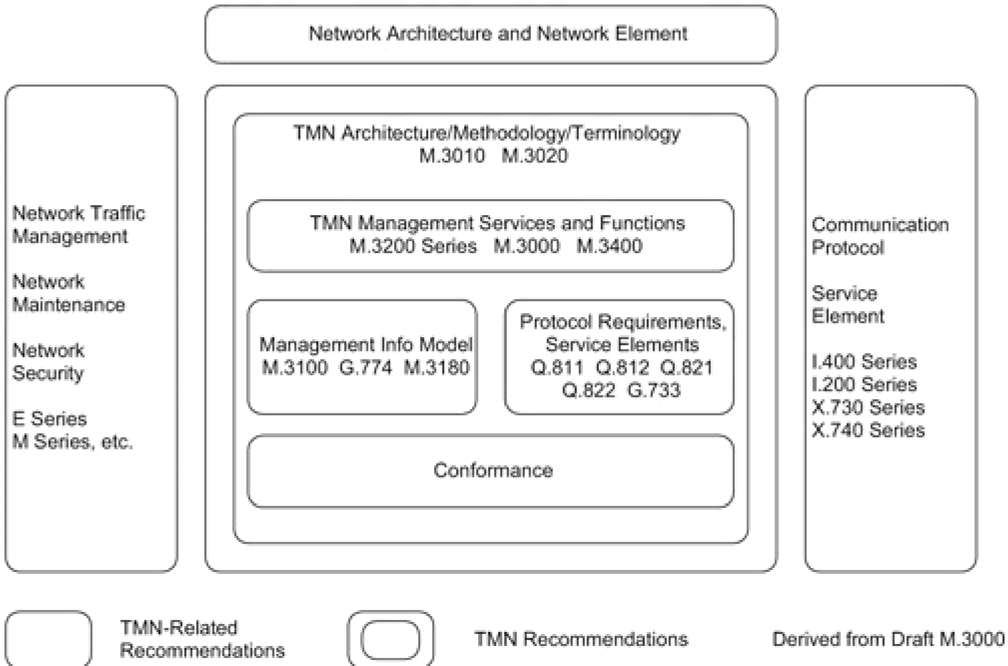
Figure TMN Relationship to Data and Telecommunication Networks



TMN Standards

ITU-T is the standards body that has developed TMN standards. It is based on the OSI framework. Its scope has been expanded M.3000 document presents a tutorial of TMN. The other documents in the M series address TMN architecture, methodology, and terminology. The Q series addresses the Q interface, such as Q3 and G.733, the protocol profile for the Q interface.

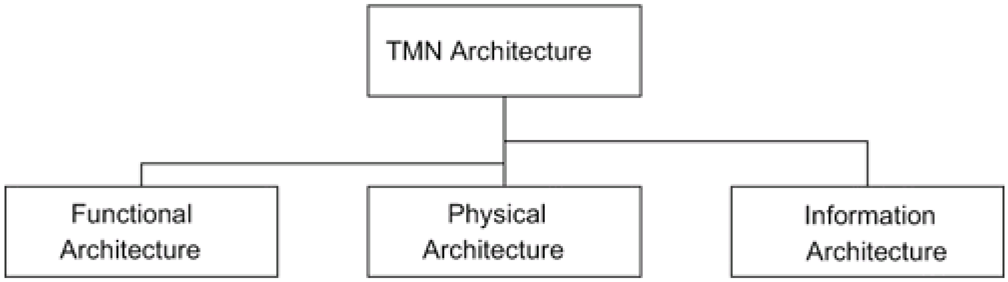
Figure TMN Recommendations and Scope



TMN Architecture

TMN architecture is defined in M.3010 describing the principles for a TMN. There are three architectural perspectives: functional, physical, and information. The functional architecture identifies functional modules or blocks in the TMN environment, including the reference point between them. The requirements for interface are specified. The physical architecture defines the physical blocks and interfaces between them. Information architecture deals with the information exchange between managed objects and management systems, using a distributed object-oriented approach. We will look at each of these three perspectives in the next three subsections. You may also obtain more details from the references [Cohen, 1994; M.3010; NMF; Raman, 1999; Sidor, 1998].

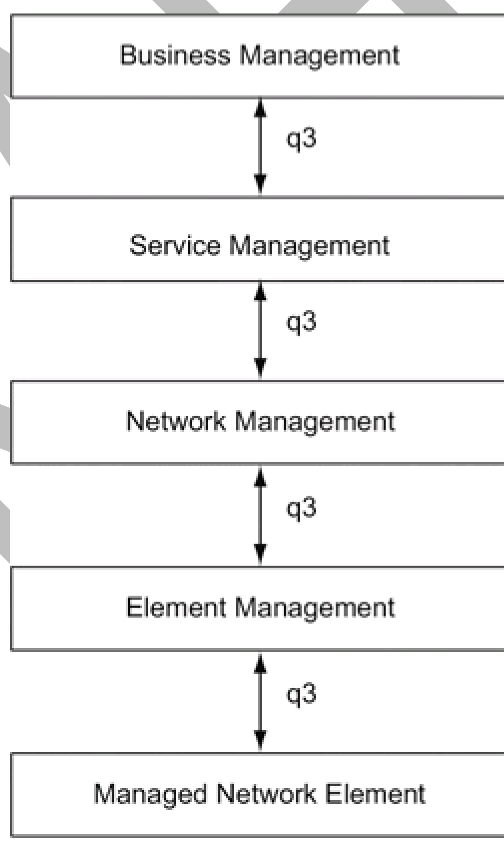
Figure TMN Architecture



Management Service Architecture

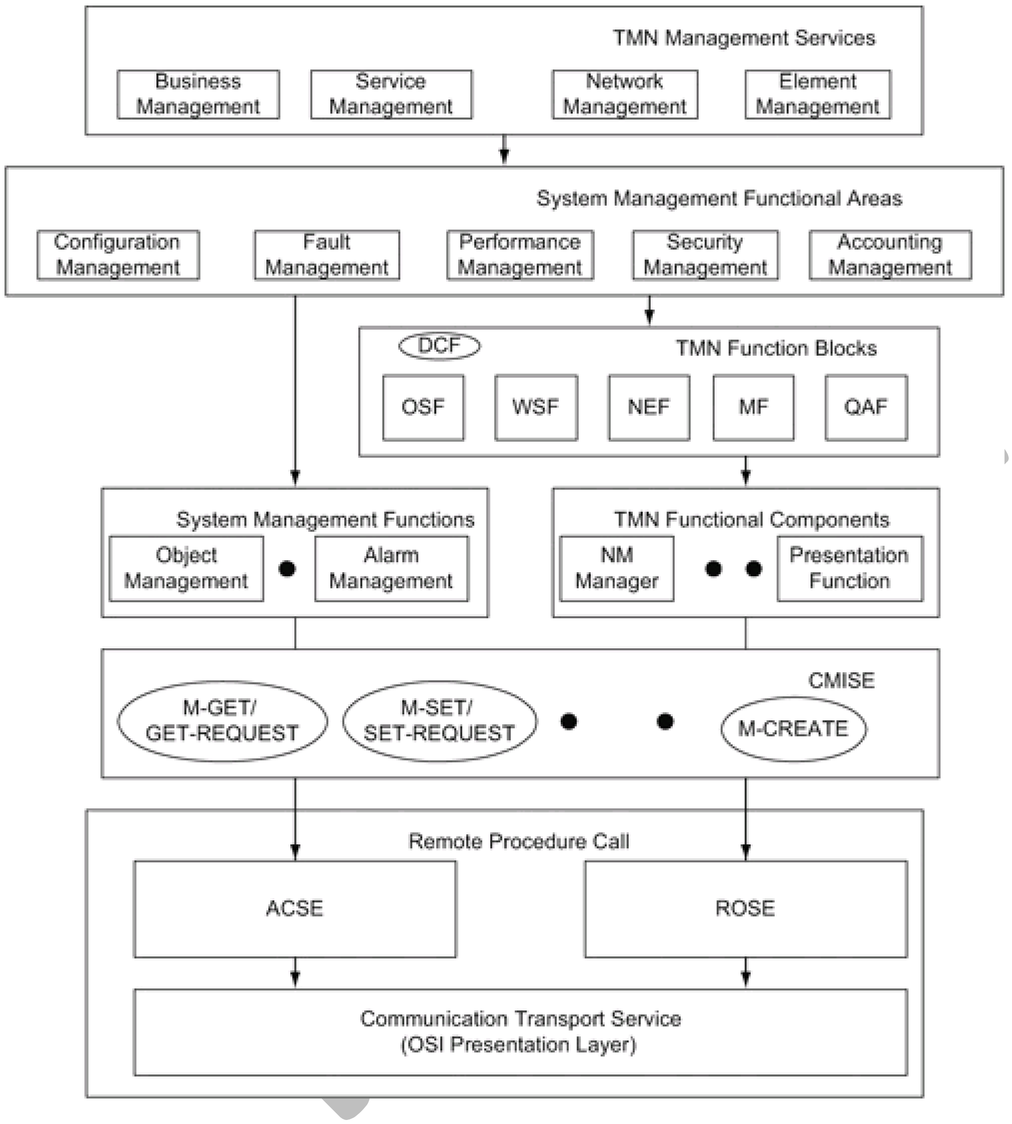
Another functional model of TMN is based on the services provided in a TMN environment. The TMN services are grouped and presented as TMN layered architecture [M.3400]. This layered architecture is not the same in the strict sense of protocol layered architecture, in that communication can occur between nonadjacent layers.

Figure TMN Service Architecture



TMN Integrated View

Now that we have discussed various aspects and perspectives of TMN architecture, let us look at the overall picture of how all these fit together. A representation of this is shown in Figure 10.13. Figure 10.13. TMN Services and Functions



TMN Implementation

Although the TMN concept was proposed in the early 1980s, it has not found wide acceptance for several reasons [Glitho and Hayes, 1995; Raman, 1998]. Some of these are its strong dependency on exclusive OSI network management, high resource requirement, technical complexity, lack of complete standards, popularity and simplicity of SNMP management, and implementation difficulties.

Industry and computer technology were not quite ready in the 1980s to fully implement (or even partially implement) the object-oriented OSI network management due to its complexity. The object-oriented and layered OSI protocol stack demanded processor resources that were beyonssd the capability of the technology then. However, present-day hardware resources can handle such demands. OSI toolkits are currently available both commercially and as freeware. Using these tools, products have been developed for trouble ticket administration (TMN X interface) and Integrated Digital Loop Carrier (TMN Q3 interface) recently.

POSSIBLE QUESTIONS

UNIT-IV

PART-A **(20 MARKS)**

(Q.NO 1 TO 20 Online Examination)

PART –B **(5*6=30 MARKS)**

1. Discuss the Structure of Management Information.
2. What is Management Information Base?
3. Differentiate RMON1 – RMON2.
4. Explain the methodology of ATM Networks.
5. Discuss in detail about network operating systems.
6. Explain the Integrated view of TMN.

PART – C

CASE STUDY (COMPULSORY) **(1*10=10 MARKS)**

1. Discuss in detail about implementation issues in system architecture.
2. Explain about Conceptual model.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Subject:Network architecture and Management
Subject Code:17CSP304
Class: II-M.Sc(CS) SEM:III
Objective type questions
UNIT-IV

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	____________ is used to define an information module.	OBJECT-TYPE	MODULE_IDENTITY	NOTIFICATION-TYPE	ENTITY-TYPE	**MODULE_IDENTITY**
2	______macros define the syntax and semantics of a managed object.	MODULE_IDENTITY	NOTIFICATION-TYPE	ENTITY-TYPE	OBJECT-TYPE	**OBJECT-TYPE**
3	Trap is also termed notification and defined by _______ macro.	NOTIFICATION-TYPE	OBJECT-TYPE	MODULE_IDENTITY	ENTITY-TYPE	**NOTIFICATION-TYPE**
4	The expansion of SMI	structure of management information	structure of manager information	segmentation of manage informant	segmentation of management information	**structure of management information**
5	The first is the ability to request and receive bulk data using the _____message.	set-bulk	set-get bulk	get-bulk	set-get command	**get-bulk**
6	______are designed to help define new datatypes.	textual conventions	conformance statements	table enhancements	transport mapping	**textual conventions**
7	________help the customer objectively compare the features of the various products.	table enhancements	textual conventions	conformance statements	transport mapping	**conformance statements**
8	8.MIB has two sub groups _______ and ________.	secure and snmp	security and snmpv2	security and snmp	snmp and snmpv2	**security and snmpv2**
9	9.In _______are several changes to the communication model in SNMPv2.	transport mapping	textual conventions	table enhancements	conformance statements	**transport mapping**
10	10.The _____definitions describe the semantics of an informayion module .	textual	module	object	class	**module**

11	COTS stands for___________.	connectionless oriented transport service	connection oriented transport service	connectivity of transfer service	connectivity of transport service	**connection oriented transport service**
12	An________trap event known in version 1.	SMNP	SNMP	SNMPv2	SMTP	**SNMPv2**
13	________in SMIv2 is equivalent to trap in SMIv1.	object	notification	identity	class	**notification**
14	________definitions are used to describe managed objects.	class	UDP	object	notification	**object**
15	The snmpV2 has _______subnodes.	1	2	3	4	**3**
16	_______defines information modules.	RFC	RFC 180	RFC 1902	RPC	**RFC 1902**
17	There are _______modules under MIBObjects.	2	1	3	6	**2**
18	18.______extends the SNMP standards to send management messages over transmission protocols.	SNMP domains	UDP domains	SNMPv2	UDP	**SNMP domains**
19	19.The SNMPv2 module has ______sub modules.	2	3	4	5	**3**
20	20.The MIB module __________addresses the new objects intoduced in SNMPv2	MIBobjects	snmp objects	snmpMIBobjects	objects	**snmpMIBobjects**
21	21.The lowest layer is the _________layer .	network	transport	network element	application	**network element**
22	22.The second layer is the ___________layer.	session	datalink	element management	physical	**element management**
23	23.The third layer is the________layer,which manages the network.	network	network management	element management	datalink	**network management**
24	24.The network management functions in this layer include_____	bandwidth, Qos	performance	flow conntrol	all the above	**all the above**
25	25.The _______is concerned with managing the sertvice provided by a network service provider.	service management	network management	element management	all the above	**service management**
26	26.TMN management services are classified by____	tcp	ip	OSI	Tcp/ip	**OSI**
27	27.The OSI application functions are of _______ types.	2	5	6	7	**5**
28	28.TMN functional components such as the _____and ______.	NMF and TMN	NMF and MIB	NMF	all the above	**NMF and MIB**

29	29.OSI toolkits are currently available both commercial and as_________	software	hardware	freeware	all the above	**freeware**
30	30.The ____and _______ protocol stack demanded processor resources that were beyond the technology at the time.	object-oriented and layered OSI	TCP/IP and OSI	OSI and UDP	UDP and TCP/IP	**object-oriented and layered OSI**
31	31.The terminology used in the telephone industry,has been changed to ________.	OS	OAM	OAM&P	OS and OAM	**OS**
32	32.The OS does not play a direct role in information transfer,but it does help in________.	OAM&P	OPM	OFM	OS and OAM	**OAM&P**
33	33.The interfaces associated with the various _____and_____.	functions and objects	object and class	function and services	protocaol and stack	**function and services**
34	34.The CMISE stands for____.	common management information service element	connection management information service element	connectionless manager information service element	common manager informant service element	**common management information service element**
35	35.The ________identifies functional modules ,or blocks in the TMN environment.	information architecture	physical architecture	functional architecture	network architecture	**functional archtecture**
36	36.The ___________defines the physical blocks and interfaces between them.	physical architecture	network architecture	information architecture	functional architecture	**physical architecture**
37	37.The _______deals with the information exchange between managed objects and management syatem.	information architecture	information architecture	network architecture	physical architecture	**information architecture**
38	38.communication between function blocks is itself a fuction,but not a function block and is defined as the __________.	DCF	TMN	TMNDCF	Tcp/ip	**TMNDCF**
39	39.The TMN __________is implemented in Operations sytem.	OSF	OPF	DCF	TMN	**OSF**
40	40.The TMN _________ concerned with managed network elements.	OSF	NEF	DCF	TMN	**NEF**

41	41.The TMN________block addresses the operations performed on the information content passing between the element and OS.	DCF	MF	NEF	OSF	**MF**
42	42.The TMN_______provides an interface between human personnel and TMN activities.	MF	WSF	DCF	NEF	**WSF**
43	43.The ________blocks are connected with intefaces denoted by x,qx,and f.	function	services	switches	hub	**function**
44	44.The TMN interface between function blocks, is called a _______.	TMN reference point	TMN discrete point	TMN connection point	TMN work station	**TMN reference point**
45	45.The __________interfaces with a management application function.	q-class reference point	x-class refence point	f-class reference	x-class TMN reference	**q-class reference point**
46	46.An _______is an interface between the workstation function block and any other function block inTMN.	f-class reference point	x-class refence point	q-class reference point	x-class TMN reference	**f-class reference point**
47	47.An TMN________is an interface between two OS function blocks belonging to two different TMNs.	x-class refence point	q-class reference point	x-class TMN reference	f-class reference point	**x-class refence point**
48	48.TMN reference points are designed by the _____letters.	uppercase	numeric	lowercase	alphabet	**lowercase**
49	49.Physical interfaces are identified by the_______letters	numeric	uppercase	alphabet	lowercase	**uppercase**
50	50.The first standard is the definition of management information according to a_________.	MIF	DCF	MF	RCF	**MIF**
51	51.The term _________network has several interpretations.	broadband	multiband	single	bandwidth	**broadband**
52	52.There are three types of information technology services they are____,__________,_____.	voice	video	data	all the above	**all the above**
53	53.Those who provide multimedia services to customers are broadband servce providers and are referred to as ______.	MSO	MIMO	NSO	IMO	**MSO**

54	54.ISDN means_________.	basic integrated services digital network	base integrated selection of data network	basic integer services data network	base integrated selection of data network	**basic integrated services digital network**
55	55.ATM means_________.	automatic teller machine	automatic trap machine	asynchronous transfer mode	asynchronous transmit mode	**asynchronous transfer mode**
56	56.The _____group collects basic statistics.	portselect groups	atmmatrix	atmstatstable	atmstats	**atmstats**
57	57.The pertinent data are stored in the ________and _______.	SerialConfigTable and Serial Connection Table	SerialConnection and Serial Table	History Table and Object Table	trap Dest Table and netConfig table	**SerialConfig Table and Serial Connection Table**
58	58.The __________contains the network configuration parameter.	trap Dest Table and netConfig table	netConfigTable	SerialConnection and Serial Table	History Table and Object Table	**netConfigTable**
59	59.The ____________defines the destination addresses for the traps.	netConfigTable	atmmatrix	trap Dest Table	atmstats	**trap Dest Table**
60	60.LCD means______	Local control device	loss of cell delineation	local cost division	loose of cell division	**loss of cell delineation**

SYLLABUS

UNIT V

Network Management Tools and Systems: Network management tools – Network statistics measurement system – Network Management Systems – System Management; Network Management Applications: Configuration Management - Fault Management - Performance Management – Security Management – Accounting Management – Report Management - Policy Based Management – Service Level Management.

Network Management Tools, Systems, and Engineering

SNMP standards for IP network management. This includes protocols and Management Information Bases (MIBs). Assorted tools and techniques that can be used for the management of networks using SNMP and other management protocols. Commonly available utilities that can be used for management. This is followed by a discussion of tools for gathering network. Examine the design of MIBs (MIB Engineering), which is important for any vendor of networking equipment. We turn to the design of a typical network management system (NMS) server for a large telecom network.

System Utilities for Management

A significant amount of network management can be done using operating system (OS) utilities and some freely downloadable SNMP tools. These can be put together quickly using simple scripting languages such as Perl. Some of these tools are described below.

Basic Tools

Numerous basic tools are either a part of the OS or are available as add-on applications that aid in obtaining network parameters or in the diagnosis of network problems. We will describe some of the more popular ones here under the three categories of status monitoring, traffic monitoring, and route monitoring.

Network Statistics Measurement Systems

One key aspect of network management is traffic management. Let us consider performance management as one of the application functions. However, let's first consider how the basic tools are used to gather network statistics in the network at various nodes and segments. We will then cover an SNMP tool, Multi Router Traffic Grapher (MRTG), which can be used to monitor traffic.

One of the best ways to gather network statistics is to capture packets traversing network segments or across node interfaces in a promiscuous mode. Thus, they are good tools to gather network statistics. Another way to gather network statistics is to develop a simple application using a function similar to **tcpdump**, using a high-performance network interface card and processor, and analyze the data for the required statistics.

Tasks and operational details

An NMS manages the network elements, also called managed devices. Device management includes faults, configuration, accounting, performance, and security (FCAPS) management. Management tasks include discovering network inventory, monitoring device health and status, providing alerts to conditions that impact system performance, and identification of problems, their source(s) and possible solutions.

Protocols

An NMS employs various protocols to accomplish these tasks. For example, SNMP protocol can be used to gather the information from devices in the network hierarchy.

Network statistics

The NMS collects device statistics and may maintain an archive of previous network statistics including problems and solutions that were successful in the past. If faults recur, the NMS can search the archive for the possible solutions.

Network Management Systems

Simple system utilities and tools for management. This was followed by a detailed examination of the design of a high-end NMS server.. We start with the management of networks, and then cover management of systems and applications. This is followed by enterprise management and telecommunications network management.

Network Management

A network consists of routers, switches, and hubs connected by network links. Servers, workstations, and PCs are connected to LANs in the network. Various access technologies may be used. In network management, we are primarily interested in the health and performance of the routers, switches, and links. We may also monitor the health of servers.

Summary

A number of utilities that are available on commonly used operating systems such as Linux, UNIX, and Windows. These are invaluable tools in the repertoire of any network manager, and support a significant amount of troubleshooting and traffic monitoring. Some of these tools are based on SNMP, others use assorted protocols such as ICMP or proprietary messages over TCP. We discussed techniques used for monitoring of statistics and the use of MRTG for collecting router traffic statistics.Focusing on SNMP-enabled devices, the vendor needs to design an MIB that supports remote management of the device.

System Management

Systems management refers to enterprise-wide administration of distributed systems including and commonly in practice computer systems, Systems management is strongly influenced by network management initiatives in telecommunications. The application performance management (APM) technologies are now a subset of Systems management. Maximum productivity can be achieved more efficiently through event correlation, system automation and predictive analysis which is now all part of APM. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being used:

- For a small business startup with ten computers, automated centralized processes may take more time to learn how to use and implement than just doing the management work manually on each computer.
- A very large business with thousands of similar employee computers may clearly be able to save time and money, by having IT staff learn to do systems management automation.
- A small branch office of a large corporation may have access to a central IT staff, with the experience to set up automated management of the systems in the branch office, without need for local staff in the branch office to do the work.

System management may involve one or more of the following tasks:

- Hardware inventories.
- Server availability monitoring and metrics.
- Software inventory and installation.

- Anti-virus and anti-malware management.
- User's activities monitoring.
- Capacity monitoring.
- Security management.
- Storage management.
- Network capacity and utilization monitoring.
- Anti-manipulation management

Network Management Applications

The management of networked information services involves management of network and system resources. OSI defines network management as a five-layer architecture. We have extended the model to include system management and have presented the integrated architecture. At the highest level of TMN are the functions associated with managing the business, business management. This applies to all institutions, be it a commercial business, educational institute, telecommunications service provider, or any other organization that uses networked systems to manage their business.

Configuration Management

Configuration management in network management is normally used in the context of discovering network topology, mapping the network, and setting up the configuration parameters in management agents and management systems. Network management in the broad sense also includes network provisioning. Network provisioning includes network planning and design and is considered part of configuration management.

Network Provisioning

Network provisioning, also called circuit provisioning in the telephone industry, is an automated process. The design of a trunk (circuit from the originating switching center to the destination switching center) and a special service circuit (customized for customer specifications) is done by application programs written in operation systems. Planning systems and inventory systems are integrated with design systems to build a system of systems. Thus, a circuit designed for the future automatically derives its turn-up date from the planning system and ensures that the components are available in the inventory system. when a circuit is to be disconnected, it is coordinated with the planning system and the freed-up components are added to the inventory system. Thus, the design system is made aware of the availability of components for future designs.

Fault Management

Fault in a network is normally associated with failure of a network component and subsequent loss of connectivity. Fault management involves a five-step process: (1) fault detection, (2) fault location, (3) restoration of service, (4) identification of root cause of the problem, and (5) problem resolution. The fault should be detected as quickly as possible by the centralized management system, preferably before or at about the same time as when the users notice it. Fault location involves identifying where the problem is located. We distinguish this from problem isolation, although in practice it could be the same. The reason for doing this is that it is important to restore service to the users as quickly as possible, using alternative means.

The restoration of service takes a higher priority over diagnosing the problem and fixing it. However, it may not always be possible to do this. Identification of the root cause of the problem could be a complex process, which we will go into greater depth soon. After identifying the source of the problem, a trouble ticket can be generated to resolve the problem. In an automated network operations center, the trouble ticket could be generated automatically by the NMS.

Fault Detection

Fault detection is accomplished using either a polling scheme (the NMS polling management agents periodically for status) or by the generation of traps (management agents based on information from the network elements sending unsolicited alarms to the NMS). An application program in NMS generates the ping command periodically and waits for response. Connectivity is declared broken when a pre-set number of consecutive responses are not received. The frequency of pinging and the preset number for failure detection may be optimized for balance between traffic overhead and the rapidity with which failure is to be detected.

Performance Management

In addressed performance management applications directly and indirectly under the various headings. Two popular protocol analyzers, Sniffer and Net Metrix,. The protocol analyzer as a system tool, to measure traffic monitoring on Ethernet LANs, which is in the realm of performance management. We know that at load monitoring based on various parameters such as source and destination addresses, protocols at different layers, etc. We addressed traffic statistics collected over a period of from hours to a year using the Multi Router Traffic Grapher

(MRTG) tool. The statistics obtained using a protocol analyzer as a remote monitoring (RMON) tool was detailed in the case study. We noticed how we were able to obtain the overall trend in Internet-related traffic and the type of traffic.

Performance of a network is a nebulous term, which is hard to define or quantify in terms of global metrics. The purpose of the network is to carry information and thus performance management is really (data) traffic management. It involves the following: data monitoring, problem isolation, performance tuning, analysis of statistical data for recognizing trends, and resource was planning.

The goal is to both prepare the network for the future, as well as to determine the efficiency of the current network. Performance management is focused on ensuring that network performance remains at acceptable levels. This area is concerned with gathering regular network performance data such as network response times, packet loss rates, link utilization, and so forth. This information is usually gathered through the implementation of an SNMP management system, either actively monitored, or configured to alert administrators when performance move above or below predefined thresholds. Actively monitoring current network performance is an important step in identifying problems before they occur, as part of a proactive network management strategy

Security Management

Security management is both a technical and an administrative issue in information management. It involves securing access to the network and information flowing in the network, access to data stored in the network, and manipulating the data that are stored and flowing across the network. The scope of network and access to it not only covers enterprise intranet network, but also the Internet that it is connected to.

Another area of great concern in secure communication is communication with mobile stations. There was an embarrassing case of a voice conversation from the car-phone of a politician being intercepted by a third party traveling in an automobile. Of course, this was an analog signal. However, this could also happen in the case of a mobile digital station such as a hand-held stock trading device. An intruder could intercept messages and alter trade transactions either to benefit by it or to hurt the person sending or receiving them.

The goal of security management is to control access to assets in the network. Security management is not only concerned with ensuring that a network environment is secure, but also that gathered security-related information is analyzed regularly. Security management functions include managing network authentication, authorization, and auditing, such that both internal and external users only have access to appropriate network resources. Other common tasks include the configuration and management of network firewalls, intrusion detection systems, and security policies such as access lists.

Accounting Management

Accounting management is probably the least developed function of network management application. We have discussed the gathering of statistics using RMON. Accounting management could also include the use of individual hosts, administrative segments, and external traffic.

Accounting of individual hosts is useful for identifying some hidden costs. For example, the library function in universities and large corporations consumes significant resources and may need to be accounted for functionally. This can be done by using the RMON statistics on hosts.

The goal is to gather usage statistics for users. Accounting management is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. While this may not be applicable to all companies, in many larger organizations the IT department is considered a cost center that accrues revenues according to resource utilization by individual departments or business units.

Report Management

Report management as a special category, although it is not assigned a special functionality in the OSI classification. Reports for various application functions, configuration, fault, performance, security, and accounting could normally be addressed in those sections. The reasons for us to deal with reports as a special category are the following. A well-run network operations center goes unnoticed. Attention is paid normally only when there is a crisis or apparent poor service. It is important to generate, analyze, and distribute various reports to the appropriate groups, even when the network is running smoothly.We can classify such reports into three categories: (1) planning and management reports, (2) system reports, and (3) user reports.

Report management includes the following tasks:

- Organize the reporting environment by adding new folders to store collections of reports.
- Enable features such as My Reports, report history, and e-mail report delivery.
- Adjust the default security model as necessary to secure access to folders and reports by using role-based security.
- Build shared schedules and shared data sources that you want to make available for general use.

Policy-Based Management

we need to define a policy and preferably build that into the system, i.e., implement policy management. For example, network operations center personnel may observe an alarm on the NMS, at which time they need to know what action they should take. This depends on what component failed, severity or criticality of the failure, when the failure happened, etc. In addition, they need to know who should be informed and how, and that depends on when the failure occurred and what SLAs have been contracted with the user. We illustrated this with an example of CBR, where a policy restraint was used to increase the bandwidth as opposed to reducing load in resolving a trouble ticket. Based on security management, policy plays an equally important, if not greater, role as the technical area. Without policy establishment and enforcement, security management is not of much use.

Service Level Management

Building a superstructure of telecommunications management to bring us up to date on the technology. We addressed policy management in the last section that ensures the optimal and enterprise-wide consistent use of the network and system management systems. However, the establishment of corporate policy does not stop at the best and consistent use of management tools. The network, systems, and business applications that run on them are there to serve customers, and customer satisfaction is essential for the success of the business. Hence, policy management should be driven by service level management, which is the second to the top layer in the TMN model.

Implementing service level management on TMN with operations systems. An operations system, in general, does an exclusive or special-purpose function. With the availability of element management and NMSs, it is time for the arrival of a generalized service level management. Service level management is defined as the process of (1) identifying services and characteristics associated with them, (2) negotiating an SLA, (3) deploying agents to monitor and control the performance of network, systems, and application components, and (4) producing service level reports. Lewis compares the definition of service level management to quality of service (QoS) management defined by the Object Modeling Group (OMG).

POSSIBLE QUESTIONS

UNIT-V

PART-A **(20 MARKS)**

(Q.NO 1 TO 20 Online Examination)

PART –B **(5*6=30 MARKS)**

1. Explain about Network management tools.
2. Discuss the architecture of Network Management Systems.
3. What are the applications of Network Management.
4. Write a brief note on Fault Management.
5. How to improve performance of a network?
6. Discuss about Accounting Management.

PART – C

CASE STUDY (COMPULSORY) **(1*10=10 MARKS)**

1. Write about Network statistics measurement system.
2. Discuss about Policy Based Management.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Subject:Network architecture and Management
Subject Code:17CSP304
Class: II-M.Sc(CS) SEM:III
Objective type questions
UNIT-V

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	Tools catalog generated byt the IETF working group on______	Network operations center tools	Network operations center techniques	Network other center tools	Network operations cell tools	**WSF**
2	Noc stands for ________	Network operations center tools	Network operations center techniques	Network other center tools	Network operations cell tools	**Network operations center tools**
3	What are the types of characterize used in tools catalog__________	10	8	5	2	**5**
4	ARP stands for___________	Address Research Protocol	Address Record Protocol	Address Resource Protocol	Address Resolution Protocol	**Address Resolution Protocol**
5	The Kyword NFS indicates a network file system debugging tool such as_______	protocol	tcp dump	ethernet	ARP	**tcp dump**
6	BERT_______	Bit Error Run Time	Bit Error Rate Tester	Byte Error Rate Tester	Byte Error Run time	**Bit Error Rate Tester**
7	CRC stands for	cyclic Redundancy check	client rcord check	client resource check	cyclic report check	**cyclic Redundancy check**

8	As the noise level increases forward error correction keeps the error rate________	Low	high	medium	none	**Low**
9	Basic s/w tools has ______types of categories of status	1	2	3	4	**3**
10	MIB structure is	Array	tree	stack	queue	**tree**
11	MRTG stands for	Multiple router transper grap	Multi router traffic grapher	Mono router traffic grapher	Multipurpose router traffic graph	**Multi router traffic grapher**
12	which of the following is automoted system tool	Network Management system	Network Management services	Network Management tools	Network Management snmp	**Network Management system**
13	N/w Management functional components are divided in to ___ types	2	3	4	5	**5**
14	MOM	Message of Message	Mail of Mail	Multiple of message	Managers of Managers	**Managers of Managers**
15	The security function is required and built into all_____	Network Management system	Network Management services	Network Management tools	Network Management snmp	**Network Management system**
16	MIS	Management of Information snmp	Management of Interchange system	Management of Information service	Management of Information system	**Management of Information system**

17	system management tools monitor the _____of computer system	networking	quality	service	performance	**performance**
18	The network provisioning also called________	sequence Provisioning	service Provisioning	Circuit Provisioning	Application Provisioning	**Circuit Provisioning**
19	TIRKS	Trunk Isolation Record Keeping system	Trunk Integrated Rows Keeping system	Trunk Integrated Record Keeping system	Trunk Integrated Result Keeping system	**Trunk Integrated Record Keeping system**
20	PVC stands for	Permanent virtual circuit	Performance virtual circuit	physical virtual circuit	Port virtual circuit	**Permanent virtual circuit**
21	SVC stands for	Switched vision circuit	Switched valid circuit	Switched virtual circuit	System virtual circuit	**Switched virtual circuit**
22	Network management is based on knowledge of network_____	IP address	topology	interface	package	**topology**
23	Fault management involves a _____step process	2	3	4	5	**5**
24	SLA stands for	software level agreement	service level agreement	server level agreement	sender level agreement	**service level agreement**
25	NCSC	National computer security center	National corp security center	National cost security center	Network computer security center	**National computer security center**
26	Which was originally called SNMP	SNMPV1	SNMPV2	SNMPV3	SNMPV4	**SNMPV1**
27	BERT stands for ______	Bit Error Rate Tester	Binary Error Rate Tester	Bit Enhanced Rate Tester	Binary Enhanced Rate Tester	**Bit Error Rate Tester**

28	Ping stands for ____	packet information group	packet internet group	packet information grouper	packet internet grouper	**packet internet grouper**
29	The Command _____ discovers all the host and the Ethernet address pairs on the LAN segment	ping	iptrace	getethers	shoop	**getethers**
30	SNMP MIBtools are of ______ types	2	3	4	5	**3**
31	MRTG stands for _____	Multi router traffic grapher	multi router traffic generator	multi range traffic group	multi range terminal group	**Multi router traffic grapher**
32	_______ is a tool that monitors the traffic load on the network links.	SNMP	MRTG	shoop	RMON MIB	**MRTG**
33	A ____ is the automated system tool that helps networking personal perform their functions efficiently.	Network monitoring system	Network message system	network management system	Local area network of the above	**network management system**
34	Network management can be classified into _____ functional components.	3	4	5	6	**5**
35	_______ management is used in discovering network topology, mapping the network.	Configuration	fault	performance	Local area network of the above	**Configuration**

36	Fault management involves _____ step process	4	5	6	7	**5**
37	Network Provisioning is considered to be part of _____	fault	performance	accounting	configuratio n	**configurati on**
38	TIRKS stands for ___	Traffic information record keeping System	Traffic integrated record keeping System	Trunk information record keeping System	Traffic integrated record keeping System	**FALSE**
39	The _____ tool uses the NETMON program in a UNIX kernal	iptrace	netstat	ping	trace route	**iptrace**
40	The Command ____ in unix display the content of various network related data structutre	iptrace	iptrace	netstat	ping	**netstat**
41	The Non SNMP components can be managed by an_____ by using proxy server.	SNMP	SNMP NMS	SNMP NNS	SMTP	**SNMP NMS**
42	____ management deals with the managing system resources which complements network management	Network monitoring system	resource	System	Information	**System**

43	An efficient database system is an essential part of ___ management	System	performance	network	inventory	**inventory**
44	Network management is based on ___ topology	network	system	computer	internet	**network**
45	DIG stands for _______	Data information group	Domain information group	Data information grouper	Domain information grouper	**Domain information grouper**
46	______ in unix is used to capture and inspects network packets	ping	snoop	getethers	bing	**getethers**
47	_______ is used to query to a domain name server & gather information it .	ping	host	dig	snoop	**dig**
48	______ is a powerful and versatile network management tool.	protocol analyser	functional role	acquisition	SMTP of the above	**protocol analyser**
49	Performance management application both ______&______under the various handings	directly and indirectly	internal and exteral	input and output	syncronous and asyncronous	**directly and indirectly**
50	The architecture defines_______entities for traffic flow masurements	5	2	3	4	**3**

51	Performance statistics are used in______a network	tuning	scaling	routing	large	**tuning**
52	ststistical data on traffic are collected and ____reports generated on use trends and to project needs	periodic	generic	logical	physical	**periodic**
53	RBR_______	Routing-based Reasoning	Rule-based Reasoning	Real-based Reasoning	Report-based Reasoning	**Rule-based Reasoning**
54	The basic Rule based Reasoning paradigm_____level	2	4	3	6	**3**
55	Security management goes beyond the realm of _______management	UDP	SNMP	TCP/IP	IP	**SNMP**
56	USM stands for ______	User-Based Security Management	User-Based Security Model	User-Based Security Method	User-Based Security Member	**User-Based Security Model**
57	NCSC stands for ______	National computer security center	National Counter Security center	National Computer Service center	physical	**National Counter Security center**

58	The main purpose of a firewall is to protect a natwork from_____attacks	internal	dynamic	external	physical	**external**
59	packet filtering is based on_______ specific criteria	planning	applicatiion	performance	protocal	**protocal**
60	IDEA stands for ______	India dat encyption Algorithm	india data encryption algorithm	input data encryption algorithm	DES	**India dat encyption Algorithm**