FINAL – IT340 **1,3 – 9**

Chapter 1

- Internet is based on TCP/IP
- IP is Internet protocol at the network layer level
- TCP is connection-oriented transport protocol and ensures end-to-end connection
- UDP is connectionless transport protocol and provides datagram service
- The Internet Control Message Protocol (ICMP) part of TCP/IP suite

Data link layer consist of two sublayers: Logical link control **AND** Media access control

- ○ (LLC)**:** Formats the data to go on the medium; performs error control and flow control
- ○ (MAC): Controls data transfer to and from LAN; resolves conflicts with other data on LAN

- Protocol Data Unit (PDU) Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data.

Common Network Problems:

- Loss of connectivity
- Duplicate IP address
- Intermittent (interrupted) problems
- Network configuration issues
- Non-problems
- Performance problems

Chapter 3

Network Models

- OSI
- Internet
- TMN
- IEEE 802
- Web-based

Management communication protocols

- SNMP
- CMIP
- XML
- CORBA

ASN.1 language

- Syntax
- Macro

SMI describes how the management information is structured and MIB deals with the relationship and storage of management information.

The two primary communications protocols are CMIP in **OSI** and SNMP in the **Internet**.

OSI Architecture and Model	SNMP Architecture and Model
• **Organization** • Network management components • Functions of components • Relationships	• **Organization** • Network management components • Functions of components • Relationships
• **Information** • **Structure of management information (SMI)** • Syntax and semantics • **Management information base (MIB)** • Organization of management information • **Object-oriented**	• **Information** • **Structure of management information (SMI)** • Syntax and semantics • **Management information base (MIB)** • Organization of management information • **Object-oriented** • **(but scalar)**
• **Communication** • Transfer syntax with bidirectional messages • Transfer structure (**PDU**)	• **Communication** • Messages less complex than OSI and unidirectional • Transfer structure (PDU)
• **Functions** • Application functions • Configure components • Monitor components • Measure performance • Secure information • Usage accounting	• **Functions** • **Application functions** • Fault management • Configuration management • Account management • Performance management • Security management

Manager	Agent	Managed object
• Sends requests to agents • Monitors alarms • Houses applications • Provides user interface	• Gathers information from objects • Configures parameters of objects • Responds to managers' requests • Generates alarms and sends them to managers	• Network element that is managed • Houses management agent • All objects are not managed / manageable

MIB: It is a *virtual* database that is compiled into management module
MDB: physical database

Keyword Example:

- CHOICE
- SET
- SEQUENCE
- OF
- NULL

Chapter 4

5 Massages between Manager and Agent: First 3 for Manager and last 2 for Agent.

- Get-Request
  - Sent by manager requesting data from agent
- Get-Next-Request
  - Sent by manager requesting data on the **next** MO to the one specified
- Set-Request
  - Initializes or changes the value of network element
- Get-Response
  - Agent responds with data for get and set requests from the manager
- Trap
  - Alarm generated by an agent

SEQUENCE and SEQUENCE OF They are used to build lists and tables.

Chapter 5

There are **three** types of traps — **generic-trap**, **specific-trap**, and **time-stamp**, which are application specific.

- The **generic-trap** type consists of coldStart, warmStart, linkDown, linkUp, authentication Failure, egpNeighborLoss, and enterpriseSpecific.

Chapter 6

Textual Conventions are designed to help define new data types.

SNMPv2 New Massages:

- inform-request
  - manager-to-manager message
- get-bulk-request
  - transfer of large data
- report
  - not used

createAndGo AND createAndWait →

Table 6.4 RowStatus Textual Convention

State	Enumer-ation	Description
active	1	Row exists and is operational
notInService	2	Operation on the row is suspended
notReady	3	Row does not have all the columnar objects needed
createAndGo	4	This is a one-step process of creation of a row; immediately goes into active state
createAndWait	5	Row is under creation and should not be commissioned into service
destroy	6	Same as Invalid in EntryStatus. Row should be deleted

Chapter 7

SNMPv3 formally defines five types of applications.
They are command generator, command responder, notification originator, notification receiver, and proxy forwarder.

Chapter 8

Remote monitoring is monitoring the network using remotely positioned probes in various segments in the network.
RMON1 was initially defined for data link level parameters of Ethernet LAN. It was then extended to token-ring LAN.
RMON2 development followed to monitor and produce statistics for parameters associated with the upper layers, from the network to the application level.

- RMON1: Monitoring Ethernet LAN and token-ring LAN
- RMON2: Monitoring upper protocol layers

Functions For RMON

- Statistics on Ethernet, token ring, and hosts / conversations
- Filter group filters data prior to capture of data
- Generation of **alarms** and **events**

Ten groups divided into three categories

- **Statistics groups** (rmon 1, 2, 4, 5, 6, and 10)
- **Event reporting groups** (rmon 3 and 9)
- **Filter and packet capture gro**ups (rmon 7 and 8)

RMON Components

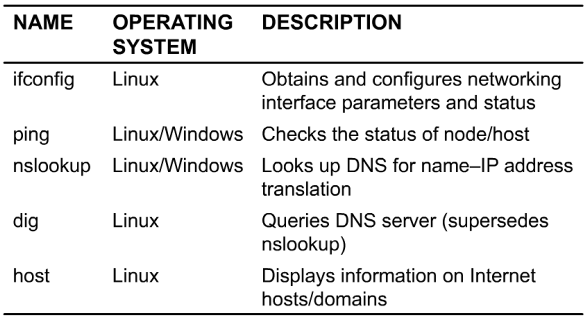
1. RMON Probe
   - Data gatherer - a physical device
2. Data analyzer
   - Processor that analyzes data

Chapter 9

Basic Network Software Tools

- Status monitoring tools
- Traffic monitoring tools
- Route monitoring tools

Table 9.1 Status-Monitoring Tools



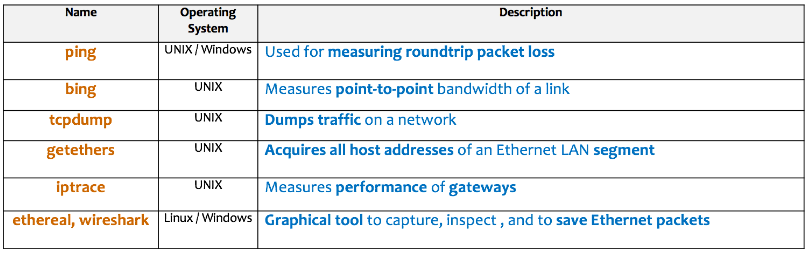
NAME	OPERATING SYSTEM	DESCRIPTION
ifconfig	Linux	Obtains and configures networking interface parameters and status
ping	Linux/Windows	Checks the status of node/host
nslookup	Linux/Windows	Looks up DNS for name–IP address translation
dig	Linux	Queries DNS server (supersedes nslookup)
host	Linux	Displays information on Internet hosts/domains

nslookup: An interactive program for querying Internet Domain Name System servers.
Converts a hostname into an IP address and vice versa querying DNS
Useful to identify the subnet a host or node belongs to.
dig: Used to gather lots of information on hosts from DNS

Ping:

- Useful for measuring connectivity
- Useful for measuring packet loss

Table 9.2 Traffic monitoring tools



Name	Operating System	Description
ping	UNIX / Windows	Used for **measuring roundtrip packet loss**
bing	UNIX	Measures **point-to-point** bandwidth of a link
tcpdump	UNIX	**Dumps traffic** on a network
getethers	UNIX	**Acquires all host addresses** of an Ethernet LAN **segment**
iptrace	UNIX	Measures **performance** of **gateways**
ethereal, wireshark	Linux / Windows	**Graphical tool** to capture, inspect , and to **save Ethernet packets**

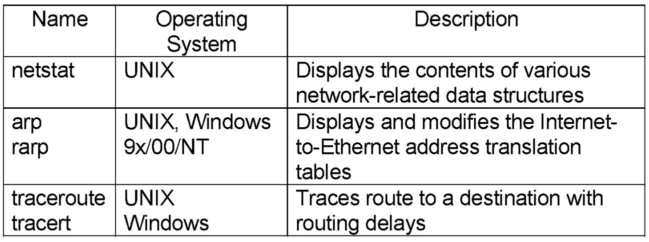
netstat is a useful diagnostic tool for troubleshooting.

traceroute (UNIX) or **tracert** (MS Windows), which is the basic tool used most extensively to diagnose routing problems. The tool discovers the route taken by packets from the source-to-destination through each hop.

snmpsniff: Linux/Free BSD based tool.
Reads PDUs. It captures SNMP packets going across the segment and stores them for later analysis.

- Similar to *tcpdump*

Table 9.3 Route-Monitoring Tools



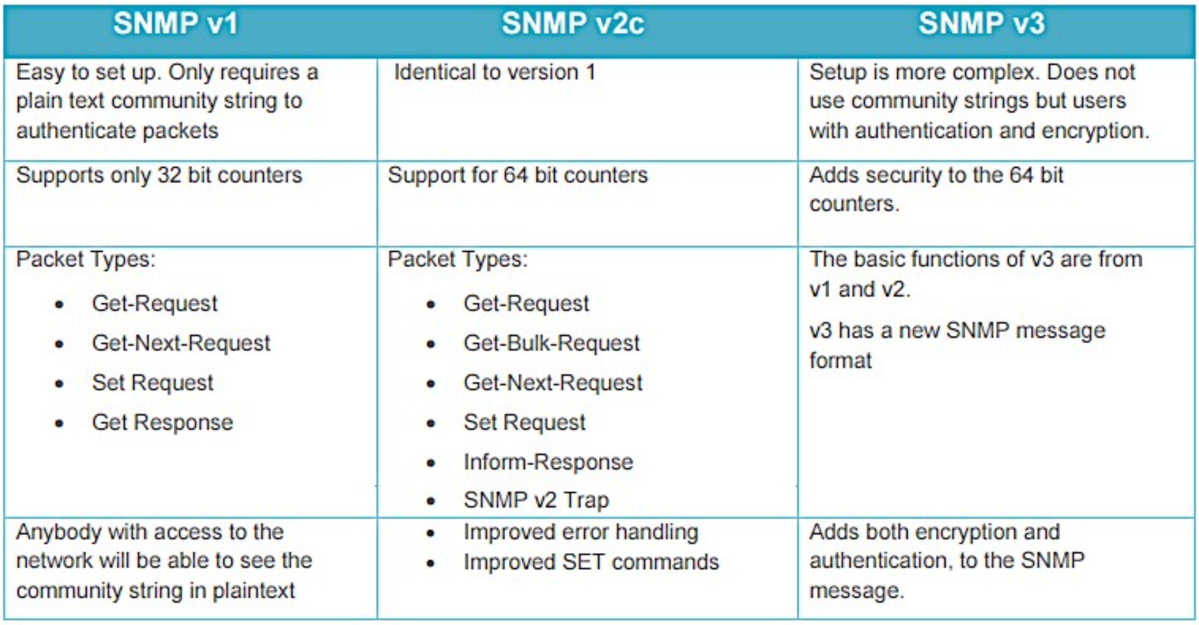
Name	Operating System	Description
netstat	UNIX	Displays the contents of various network-related data structures
arp rarp	UNIX, Windows 9x/00/NT	Displays and modifies the Internet-to-Ethernet address translation tables
traceroute tracert	UNIX Windows	Traces route to a destination with routing delays

SNMP Command Tools

- snmp**test**
- snmp**get:** This command communicates with a network object using the SNMP gef-reguest message
- snmp**getnext:** This command is especially useful to get the values of variables in an aggregate object
- snmp**set:** sends the SNMP set-request message and receives the get-response command.
- snmp**trap**
- snmp**walk**
- snmp**netstat:** Useful for finding status of network connections

MRTG is a **tool** that **monitors traffic load** on network links, It generates a live **visual representation** of traffic data by reading the SNMP traffic counters on routers and creates **graphs** that are embedded into Web pages.

Differences between SNMP versions:



SNMP v1	SNMP v2c	SNMP v3
Easy to set up. Only requires a plain text community string to authenticate packets	Identical to version 1	Setup is more complex. Does not use community strings but users with authentication and encryption.
Supports only 32 bit counters	Support for 64 bit counters	Adds security to the 64 bit counters.
Packet Types: • Get-Request • Get-Next-Request • Set Request • Get Response	Packet Types: • Get-Request • Get-Bulk-Request • Get-Next-Request • Set Request • Inform-Response • SNMP v2 Trap	The basic functions of v3 are from v1 and v2. v3 has a new SNMP message format
Anybody with access to the network will be able to see the community string in plaintext	• Improved error handling • Improved SET commands	Adds both encryption and authentication, to the SNMP message.