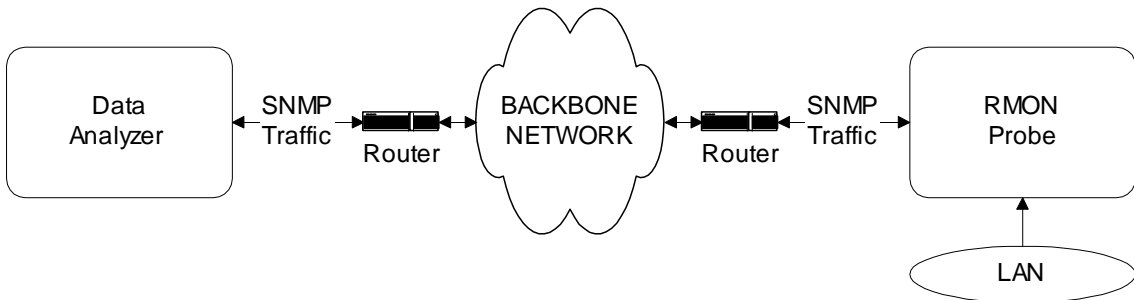# Network Management

Lecture 8

SNMP Management: RMON

Objectives

- Remote network monitoring, RMON
- RMON1: Monitoring Ethernet LAN and token-ring LAN
- RMON2: Monitoring upper protocol layers
- Generates and sends statistics close to subnetworks to central NMS
- RMON MIBs for RMON group objects

RMON Components

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

Notes

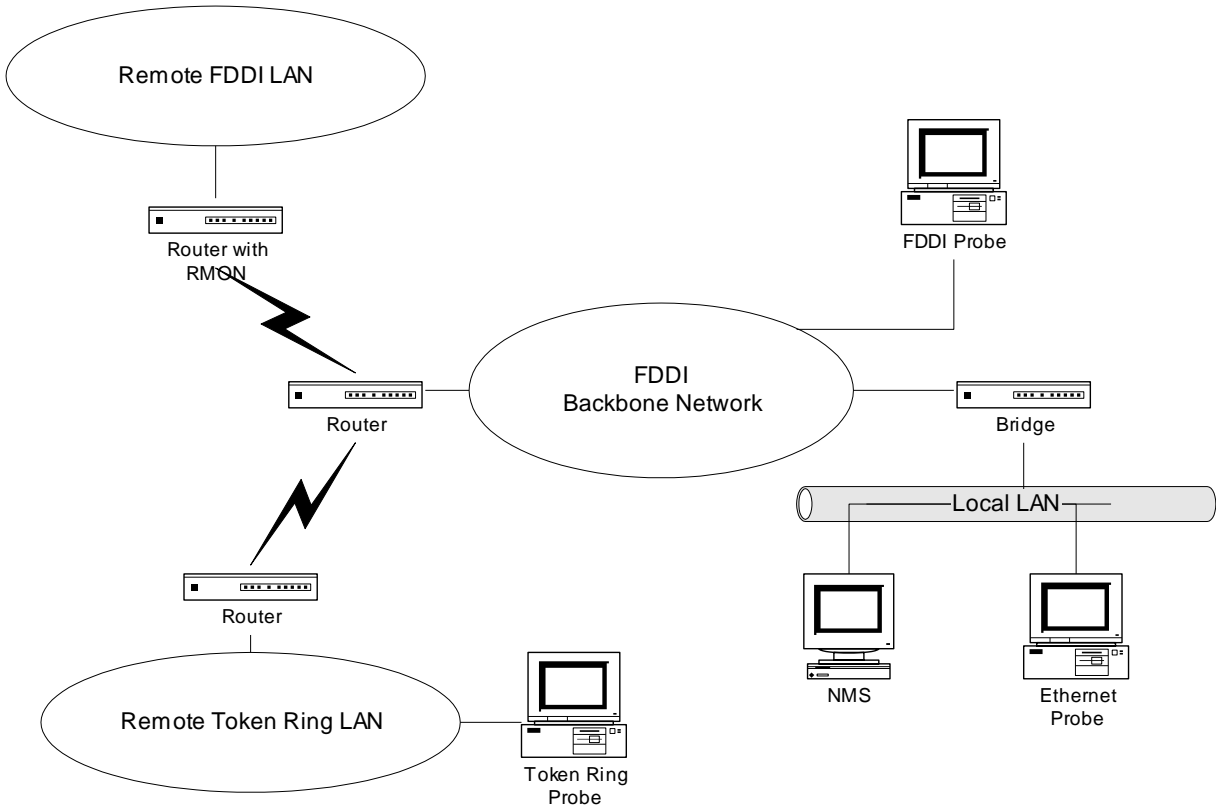- RMON Remote Network Monitoring

Network with RMONs

Figure 8.1 Network Configuration with RMONs

Notes

- Note that RMON is embedded monitoring remote FDDI LAN
- Analysis done in NMS

RMON Benefits

- Monitors and analyzes locally and relays data;
  Less load on the network
- Needs no direct visibility by NMS;
  More reliable information
- Permits monitoring on a more frequent basis
  and hence faster fault diagnosis
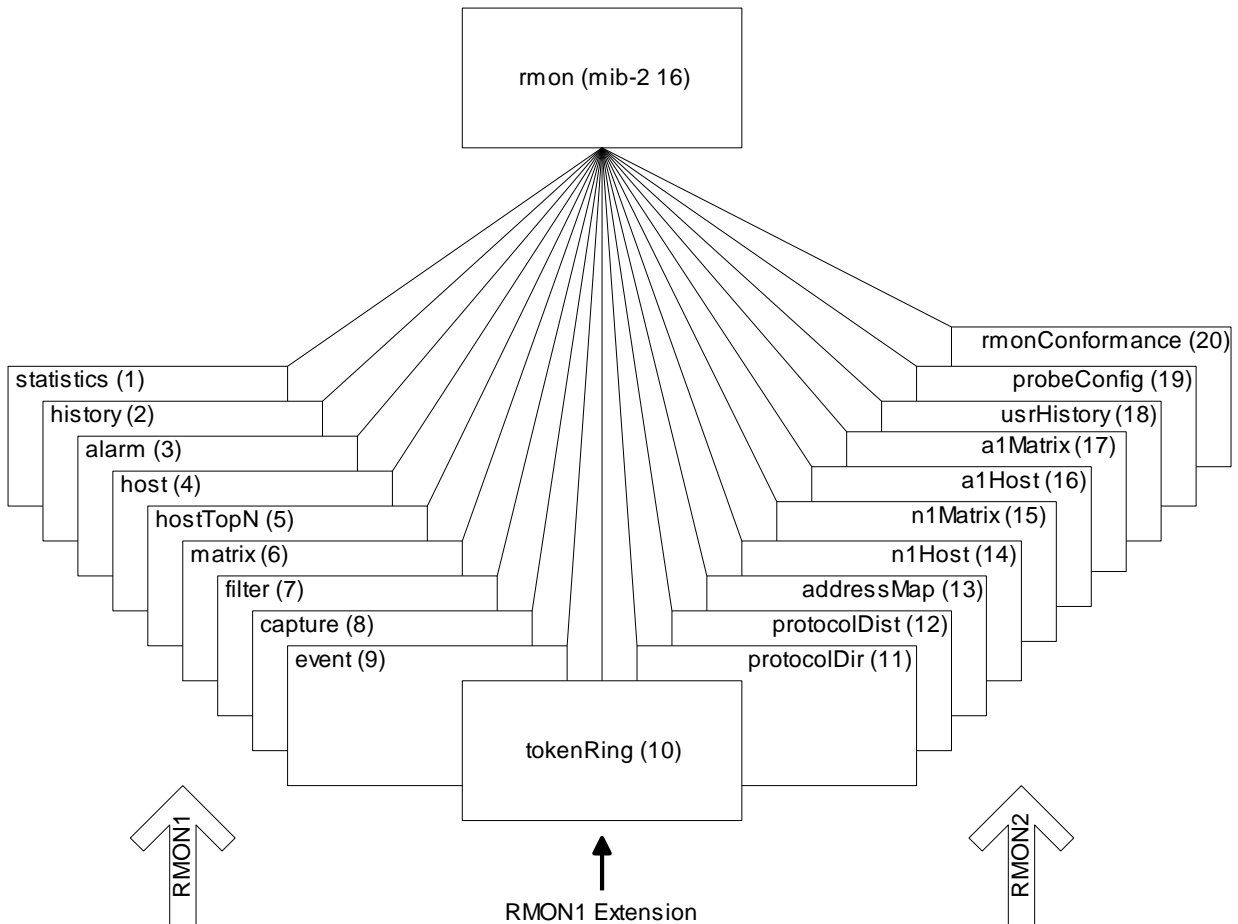- Increases productivity for administrators

Notes

RMON MIB

Figure 8.2 RMON Group

Notes

- RMON1: Ethernet RMON groups (rmon 1 - rmon 9)

- RMON1: Extension: Token ring extension (rmon 10)

- RMON2: Higher layers (3-7) groups (rmon 11 - rmon 20)

Row Creation & Deletion

Table 8.1   EntryStatus Textual Convention

State	Enume-ration	Description
valid	1	Row exists and is active. It is fully configured and operational
createRequest	2	Create a new row by creating this object
underCreation	3	Row is not fully active
invalid	4	Delete the row by disassociating the mapping of this entry

- EntryStatus data type introduced in RMON
- EntryStatus (similar to RowStatus in SNMPv2) used to create and delete conceptual row
- Only 4 states in RMON compared to 6 in SNMPv2

Notes
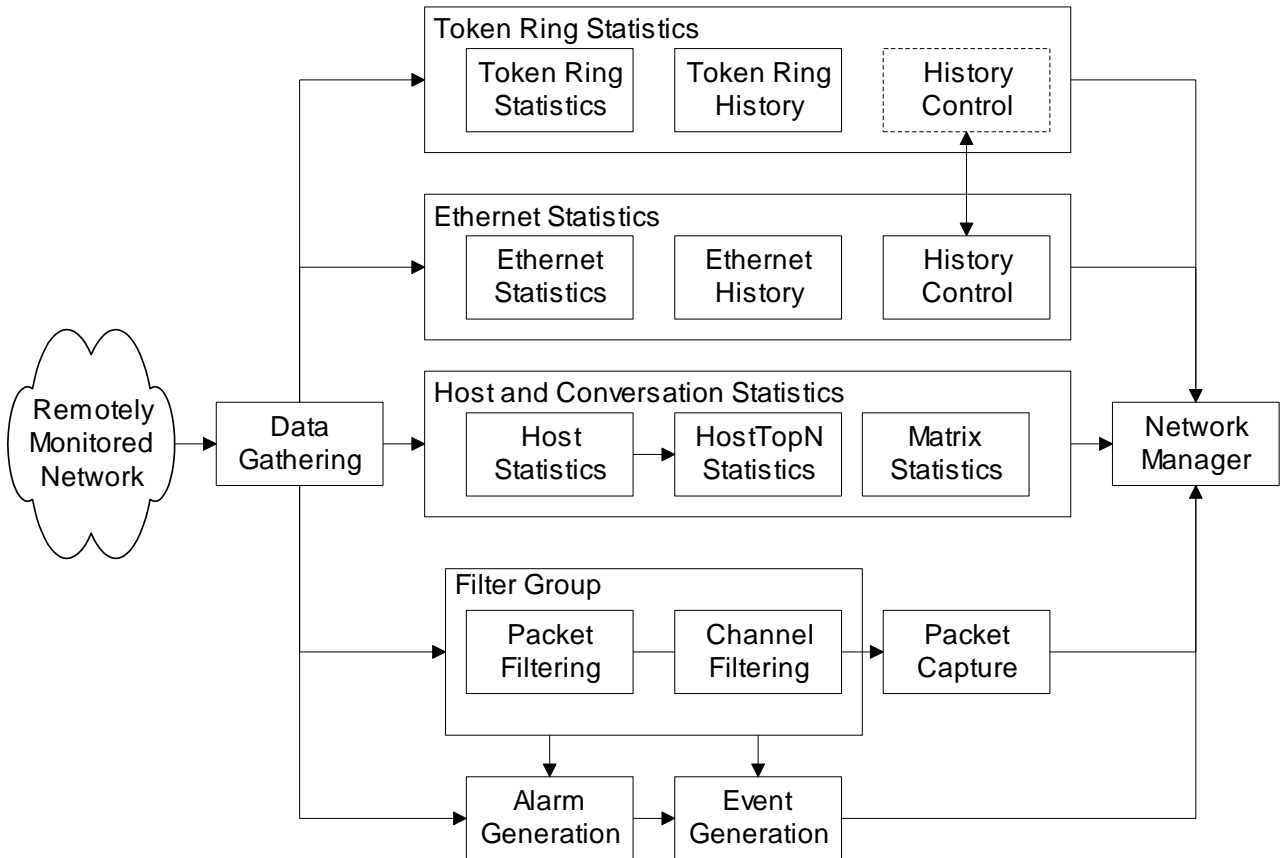
RMON Groups and Functions

Figure 8.3 RMON1 Groups and Functions

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

RMON1 MIB Groups & Tables

Group	OID	Function	Tables
Statistics	rmon 1	Link level statistics	-etherStatsTable -etherStats2Table
History	rmon 2	Periodic statistical data collection and storage for later retrieval	-historyControlTable -etherHistoryTable -historyControl2Table -etherHistory2Table
Alarm	rmon 3	Generates events when the data sample gathered crosses pre-established thresholds	-alarmTable
Host	rmon 4	Gathers statistical data on hosts	-hostControlTable -hostTable -hostTimeTable -hostControl2Table
HostTopN	rmon 5	Computes the top N hosts on the respective categories of statistics gathered	-hostTopNcontrolTable
Matrix	rmon 6	Statistics on traffic between pair of hosts	-matrixControlTable -matrixSDTable -matrixDSTable -matrixControl2Table
Filter	rmon 7	Filter function that enables capture of desired parameters	-filterTable -channelTable -filter2Table -channel2Table
Packet Capture	rmon 8	Packet capture capability to gather packets after they flow through a channel	-buffercontrolTable -captureBufferTable
Event	rmon 9	Controls the generation of events and notifications	-eventTable
Token Ring	rmon 10	See Table 8.3	See Table 8.3

Notes

• 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 groups(romon 7 and 8)
• Groups with "2" in the name are enhancements with RMON2

Textual Convention: LastCreateTime and TimeFilter

- LastCreateTime tracks change of data with the changes in control in the control tables
- Timefilter used to download only those rows that changed after a particular time

FooTable (bold indicating the indices):

fooTimeMark	*fooIndex*	*fooCounts*
fooCounts.0.1	5	
fooCounts.0.2	9	
fooCounts.1.1	5	
fooCounts.1.2	9	
fooCounts.2.1	5	
fooCounts.2.2	9	
fooCounts.3.1	5	
fooCounts.3.2	9	
fooCounts.4.2	9	-- (Note that row #1 does not exist for times 4 & 5 since the last update occurred at time-mark 3.)
fooCounts.5.2	9	

(Both rows #1 and #2 do not exist for time-mark greater than 5.)

Notes

- Bold objects (fooTimeMark and fooIndex) are indices

Control and Data Tables
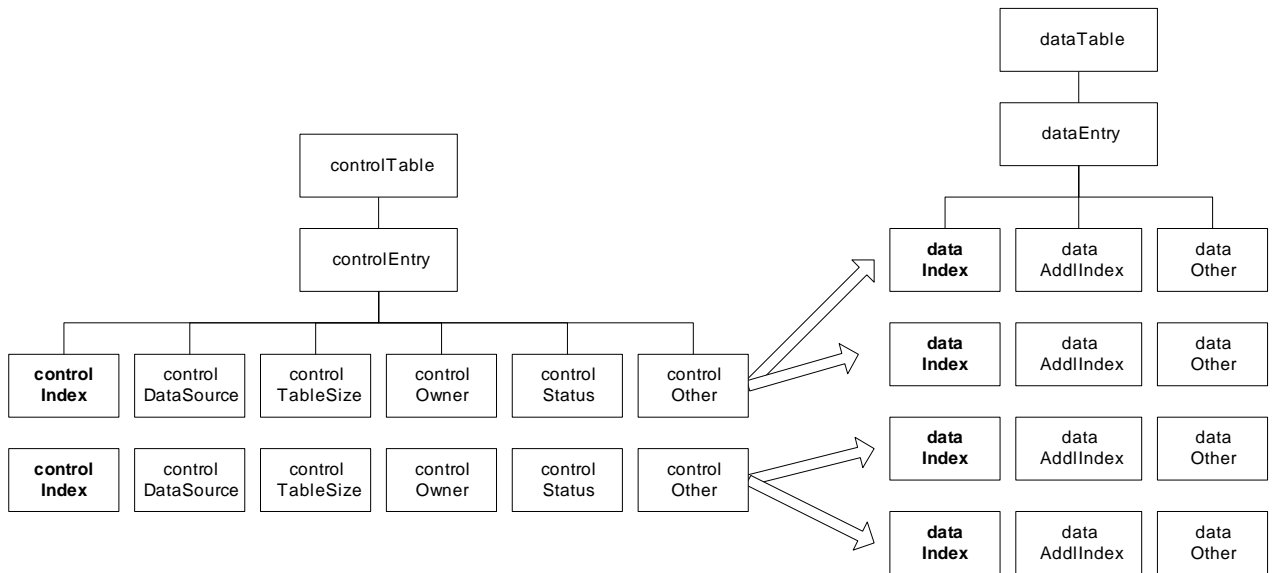
Note on Indices:
 Indices marked in bold letter
 Value of dataIndex same as value of controlIndex

Figure 8.4 Relationship between Control and Data Tables

Notes

• Control table used to set the instances of data
rows in the data table
• Values of data index and control index are the
same

Matrix Control and SD Tables

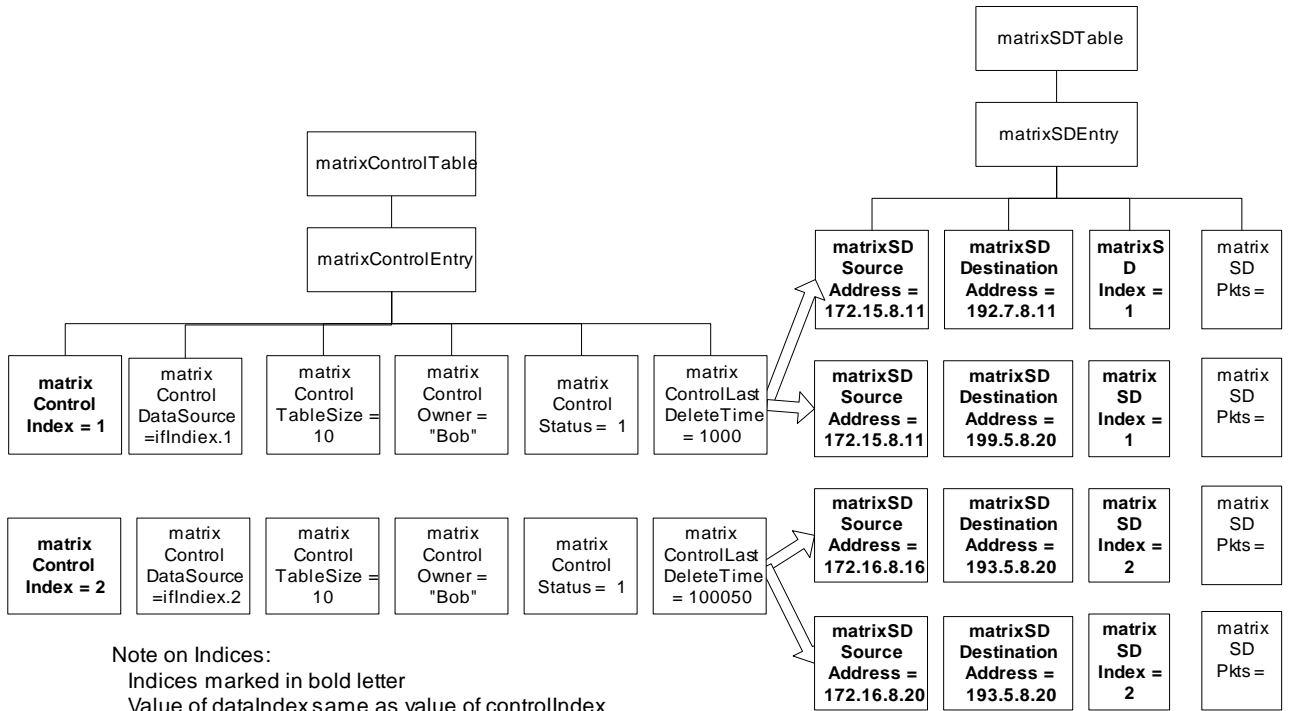| matrixSDTable			
matrixSDEntry			
matrixSD Source Address = 172.15.8.11	**matrixSD Destination Address = 192.7.8.11**	**matrixSD Index = 1**	matrix SD Pkts =
matrixSD Source Address = 172.15.8.11	**matrixSD Destination Address = 199.5.8.20**	**matrix SD Index = 1**	matrix SD Pkts =
matrixSD Source Address = 172.16.8.16	**matrixSD Destination Address = 193.5.8.20**	**matrix SD Index = 2**	matrix SD Pkts =
matrixSD Source Address = 172.16.8.20	**matrixSD Destination Address = 193.5.8.20**	**matrix SD Index = 2**	matrix SD Pkts =

matrixControlTable

matrixControlEntry

matrix Control Index = 1	matrix Control DataSource =ifIndiex.1	matrix Control TableSize = 10	matrix Control Owner = "Bob"	matrix Control Status = 1	matrix ControlLast DeleteTime = 1000
matrix Control Index = 2	matrix Control DataSource =ifIndiex.2	matrix Control TableSize = 10	matrix Control Owner = "Bob"	matrix Control Status = 1	matrix ControlLast DeleteTime = 100050

Note on Indices:
Indices marked in bold letter
Value of dataIndex same as value of controlIndex

Notes
- matrixSDTable is the source-destination table
- controlDataSource identifies the source of the data
- controlTableSize identifies entries associated with the data source
- controlOwner is creator of the entry
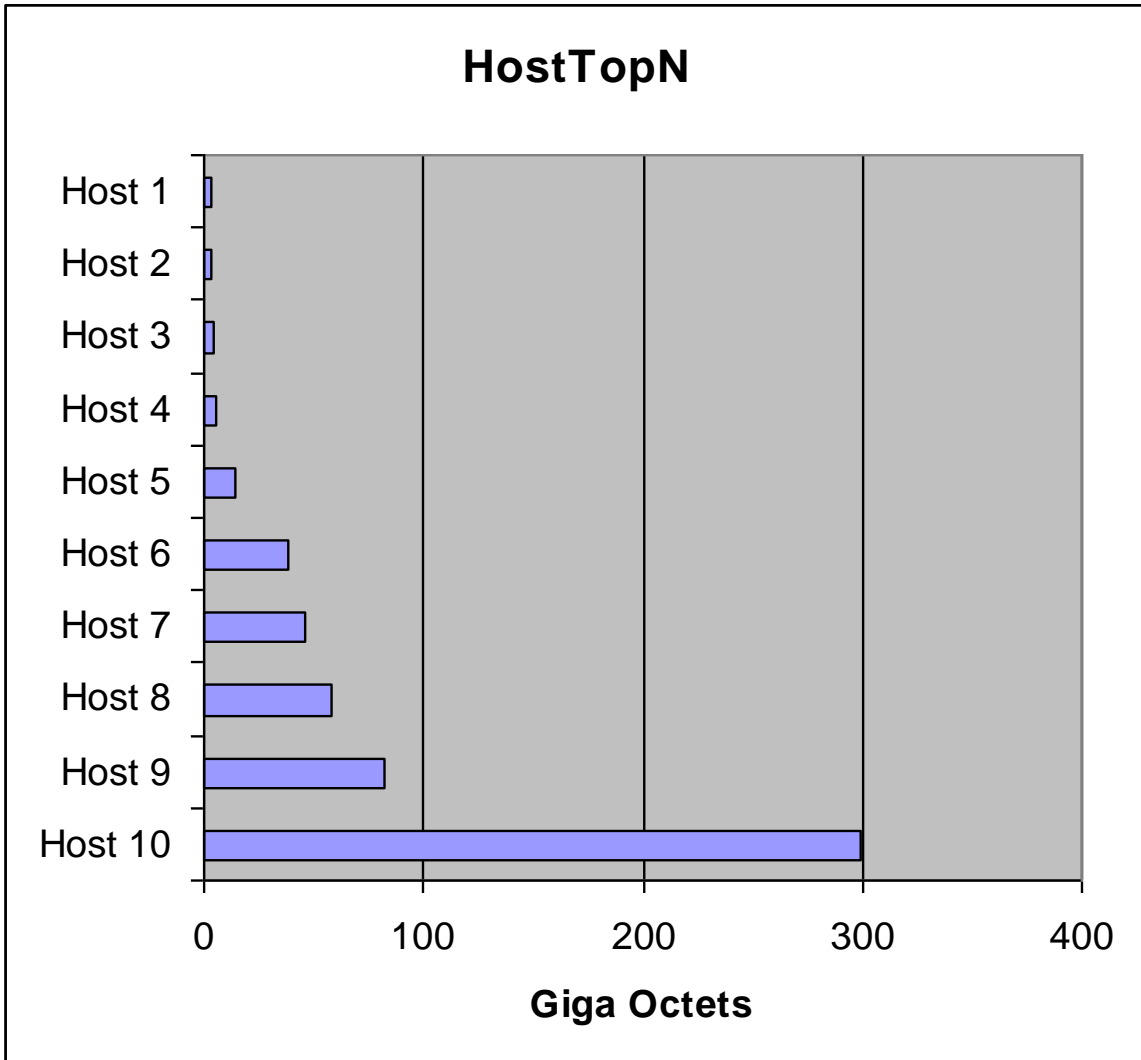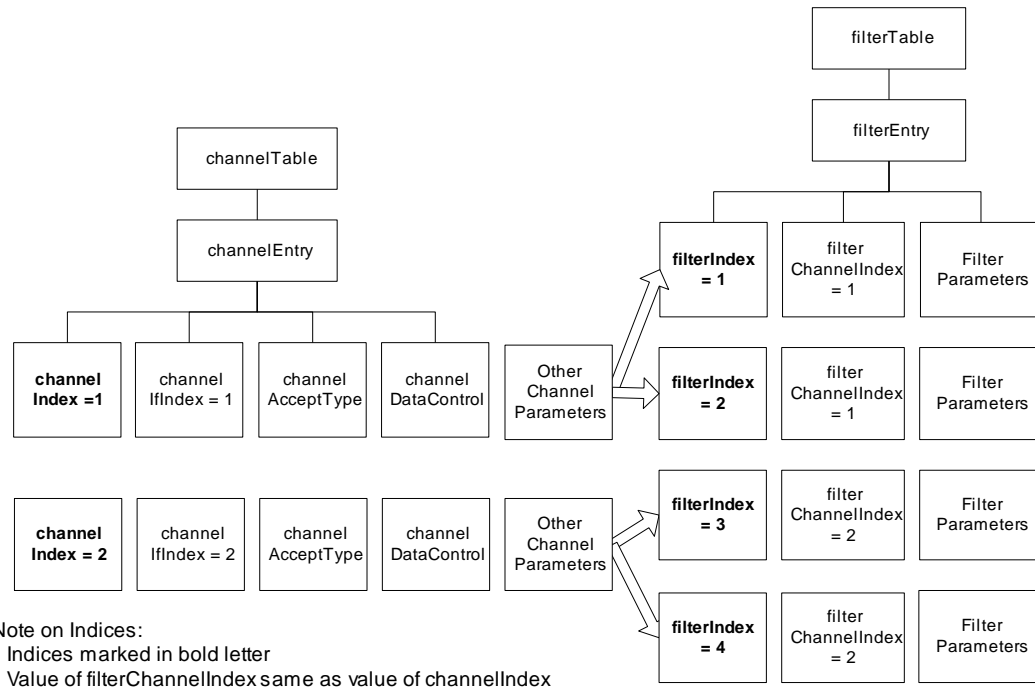
# Host Top N Group Example

Figure 8.5 HostTop-10 Output Octets

Notes

Filter Group

filterTable		
filterEntry		

channelTable → channelEntry

| channel Index =1 | channel IfIndex = 1 | channel AcceptType | channel DataControl | Other Channel Parameters |
| channel Index = 2 | channel IfIndex = 2 | channel AcceptType | channel DataControl | Other Channel Parameters |

filterIndex = 1	filter ChannelIndex = 1	Filter Parameters
filterIndex = 2	filter ChannelIndex = 1	Filter Parameters
filterIndex = 3	filter ChannelIndex = 2	Filter Parameters
filterIndex = 4	filter ChannelIndex = 2	Filter Parameters

Note on Indices:
 Indices marked in bold letter
 Value of filterChannelIndex same as value of channelIndex

Notes
- Filter group used to capture packets defined by logical expressions
- Channel is a stream of data captured based on a logical expression
- Filter table allows packets to be filtered with an arbitrary filter expression
- A row in the channel table associated with multiple rows in the filter table
- Capture table accepts data if test of any row in the filter table passes the test

Packet Capture Group

Channel Table	Filter Table (many for each channel)	Capture Buffer Table (One entry per channel)
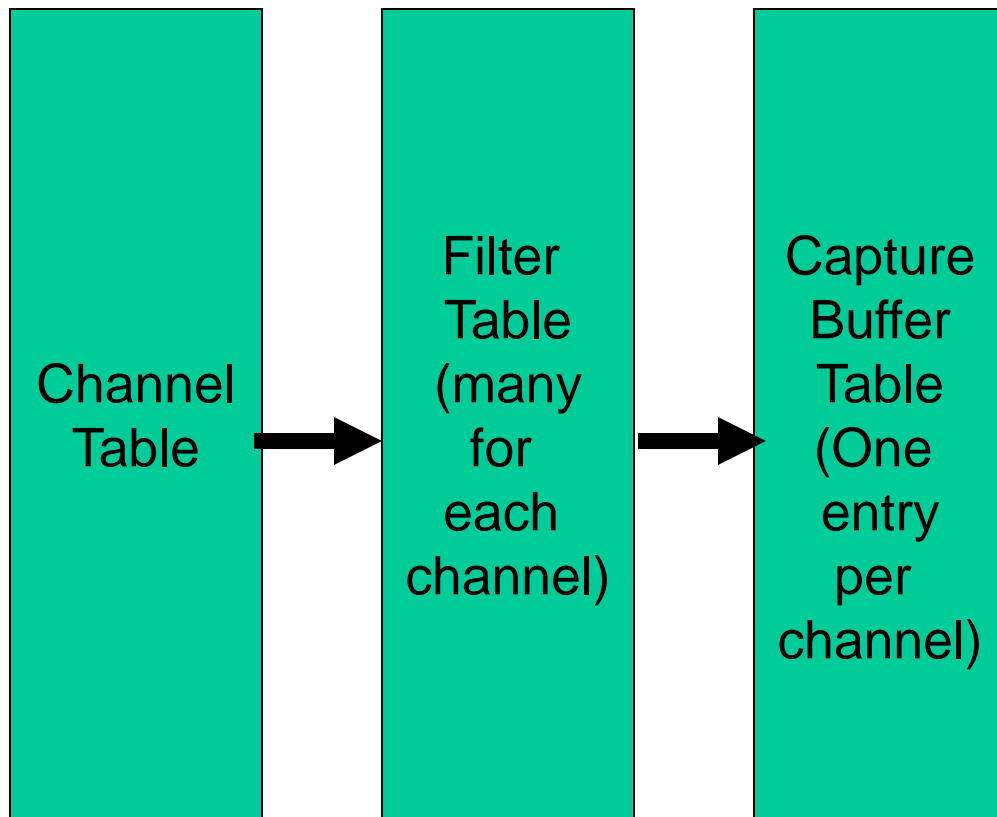
Notes

• Packet capture group is a post-filter group

• Buffer control table used to select channels

• Captured data stored in the capture buffer table

RMON TR Extension Groups

Table 8.3 RMON Token-Ring MIB Groups and Tables

Token Ring Group	Function	Tables
Statistics	Current utilization and error statistics of MAC Layer	tokenRingMLStatsTable tokenRingMLStats2Table
Promiscuous Statistics	Current utilization and error statistics of promiscuous data	tokenRingPStatsTable tokenRingPStats2Table
MAC -Layer History	Historical utilization and error statistics of MAC Layer	tokenRingMLHistoryTable
Promiscuous History	Historical utilization and error statistics of promiscuous data	tokenRingPHistoryTable
Ring Station	Station statistics	ringStationControlTable ringStationTable ringStationControl2Table
Ring Station Order	Order of the stations	ringStationOrderTable
Ring Station Configuration	Active configuration of ring stations	ringStationConfigControlTable ringStationConfigTable
Source-Routing	Utilization statistics of source routing information	sourceRoutingStatsTable sourceRoutingStats2Table

Notes

- Two statistics groups and associated history groups
    - MAC layer (Statistics group) collects TR parameters
    - Promiscuous Statistics group collects packets promiscuously on sizes and types of packets
- Three groups associated with the stations
- Routing group gathers on routing

16

RMON2

- Applicable to Layers 3 and above

- Functions similar to RMON1

- Enhancement to RMON1

- Defined conformance and compliance

Notes

RMON2 MIB

Table 8.4 RMON2 MIB Groups and Tables

Group	OID	Function	Tables
Protocol Directory	rmon 11	Inventory of protocols	protocolDirTable
Protocol Distribution	rmon 12	Relative statistics on octets and packets	protocolDistControlTable protocolDistStatsTable
Address Map	rmon 13	MAC address to network address on the interfaces	addressMapControlTable addressMapTable
Network-Layer Host	rmon 14	Traffic data from and to each host	n1HostControlTable n1HostTable
Network-Layer Matrix	rmon 15	Traffic data from each pair of hosts	n1MatrixControlTable n1MatrixSDTable n1MatrixDSTable n1MatrixTopNControlTable n1MatrixTopNTable
Application-Layer Host	rmon 16	Traffic data by protocol from and to each host	a1HostTable
Application-Layer Matrix	rmon 17	Traffic data by protocol between pairs of hosts	a1MatrixSDTable a1MatrixDSTable a1MatrixTopNControlTable a1MatrixTopNTable
User History Collection	rmon 18	User-specified historical data on alarms and statistics	usrHistoryControlTable usrHistoryObjectTable usrHistoryTable
Probe Configuration	rmon 19	Configuration of probe parameters	serialConfigTable netConfigTable trapDestTable serialConnectionTable
RMON Conformance	rmon 20	RMON2 MIB Compliances and Compliance Groups	See Section 8.4.2

Notes

Case Study

- A study at Georgia Tech on Internet traffic
- Objectives
    - Traffic growth and trend
    - Traffic patterns
- Network comprising Ethernet and FDDI LANs
- Tools used
    - HP Netmetrix protocol analyzer
    - Special high-speed TCP dump tool for FDDI LAN
- RMON groups utilized
    - Host top-n
    - Matrix group
    - Filter group
    - Packet capture group (for application level protocols)

Notes

Case Study Results

1. **Growth Rate**: Internet traffic grew at a significant rate from February to June at a monthly rate of 9% to 18%.

February to March	12%
March to April	9%
April to May	18%

   Note: There is sudden drop in June due to end of spring quarter and summer quarter starting.

2. **Traffic Pattern:**

- **Monthly / Weekly:** Only discernible variation is lower traffic over weekends

- **Daily:** 2/3 of the top 5% peaks occur in the afternoons

- **Users:**
  Top six domain of users (96%) are

Domain 1	20%
Domain 2	30%
Subdomain 1 (25%)	
Subdomain 2 (3%)	
Domain 3	34%
Domain 4	7%
Domain 5	3%
Domain 6	2%

Top three hosts sending or receiving data
  Newsgroups
  Mbone
  Linux host

What we have learned :

1. The three top groups of users contributing to 84% of the Internet traffic are students (surprise!), Newsgroup services, and Domain 1.

2. Growth rate of Internet during the study period in spring quarter is 50%.