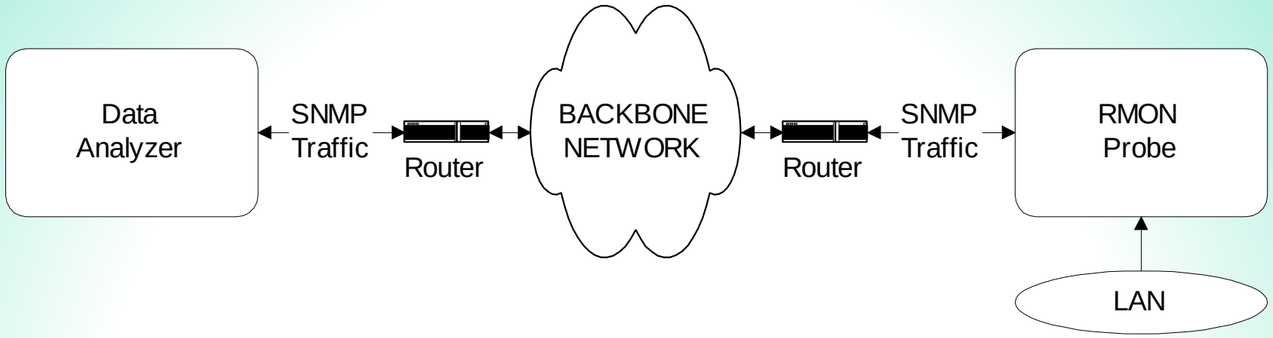
Chapter 8

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

Probes of different types according to the network

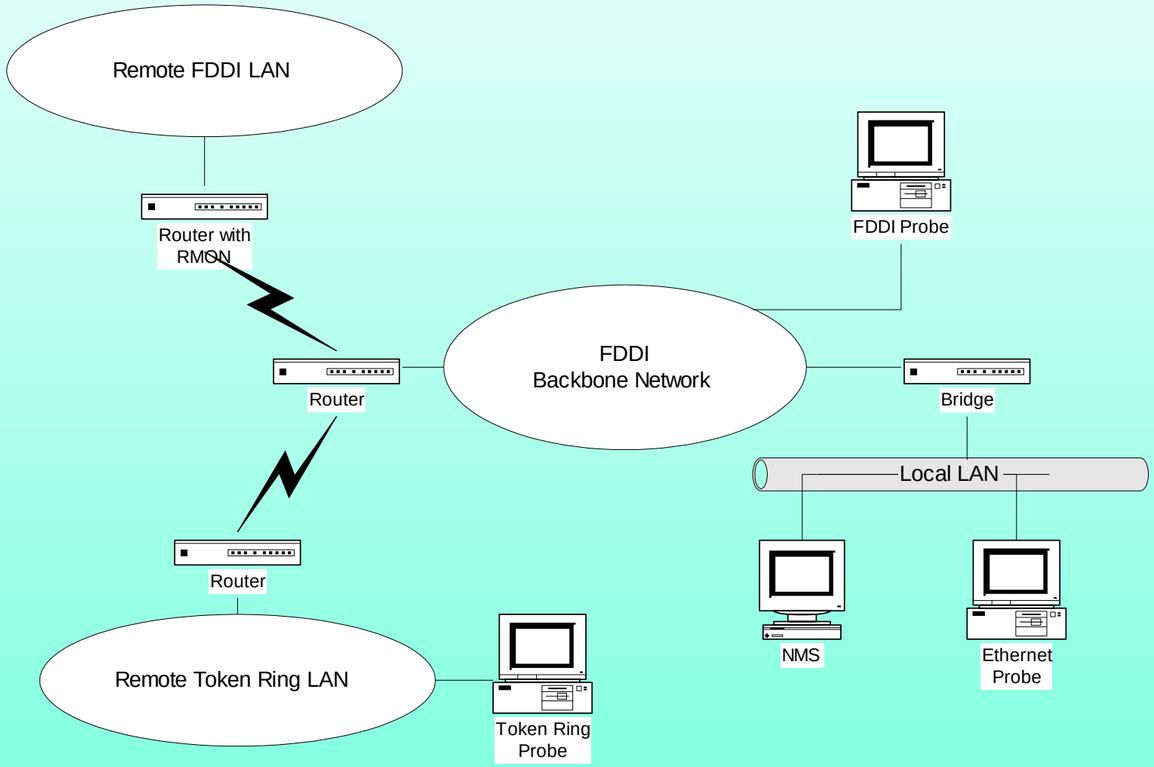


Figure 8.1 Network Configuration with RMONs

Notes

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

RMON Benefits

- Monitors and (partially) analyzes data locally and relays it to the data analyzer/NMS : this results in less load on the network

- Needs no direct visibility by NMS; More reliable information

- Permits monitoring on a more frequent basis (because data is gathered locally) and hence faster fault diagnosis

- Increases productivity for administrators

Notes

RMON MIB

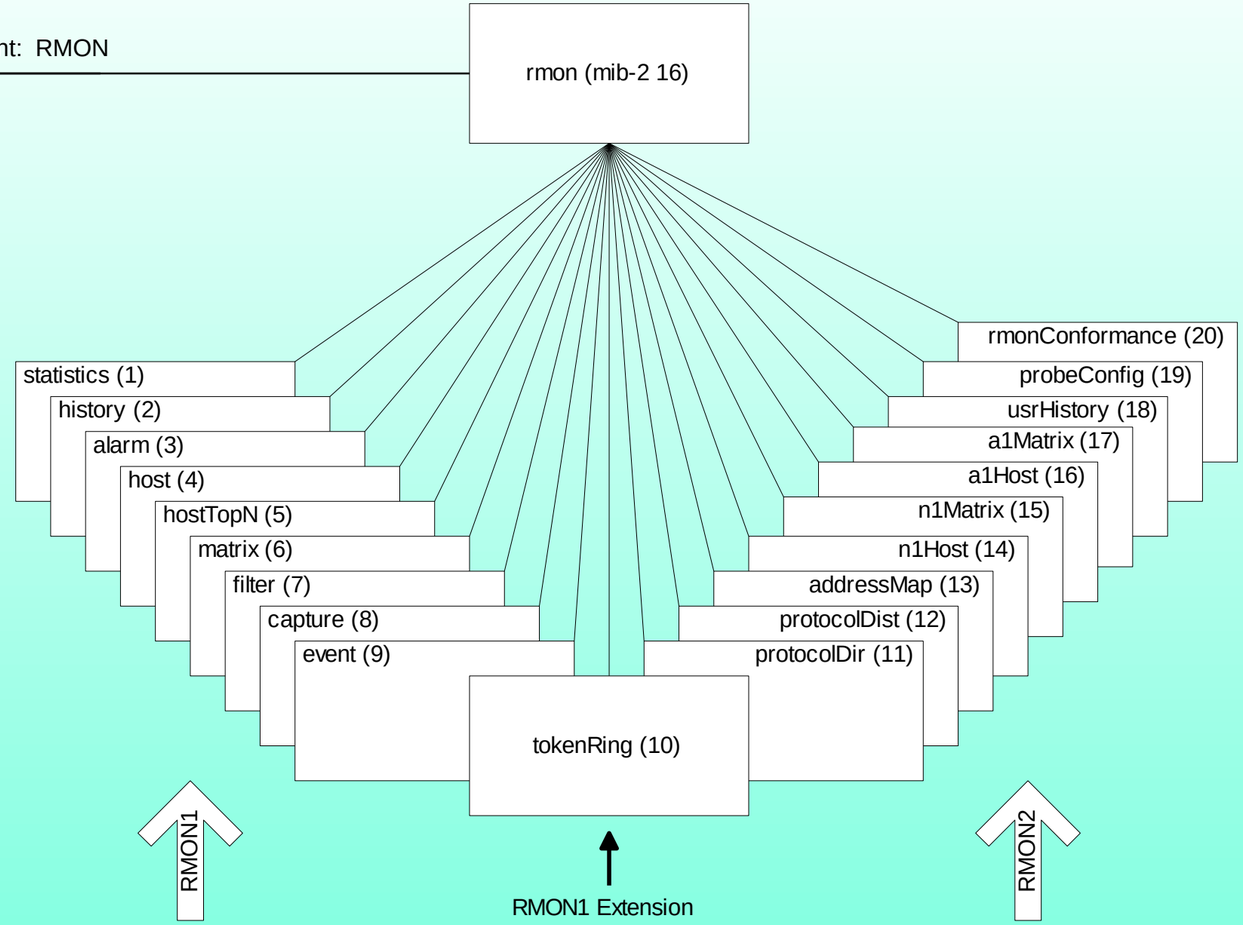


Figure 8.2 RMON Group

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), as shown in Figure 8.2.

- 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

Textual Convention: LastCreateTime and TimeFilter

Enhancements to RMON1 include :

•LastCreateTime: a standard textual convention that tracks changes of data and control

• Timefilter : a standard textual convention enables an application to download only those rows that changed since a particular time.

An additional descriptive label which may associated to some management information, these textual conventions can be applied to rows of tables

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.1.2	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

RMON Groups and Functions

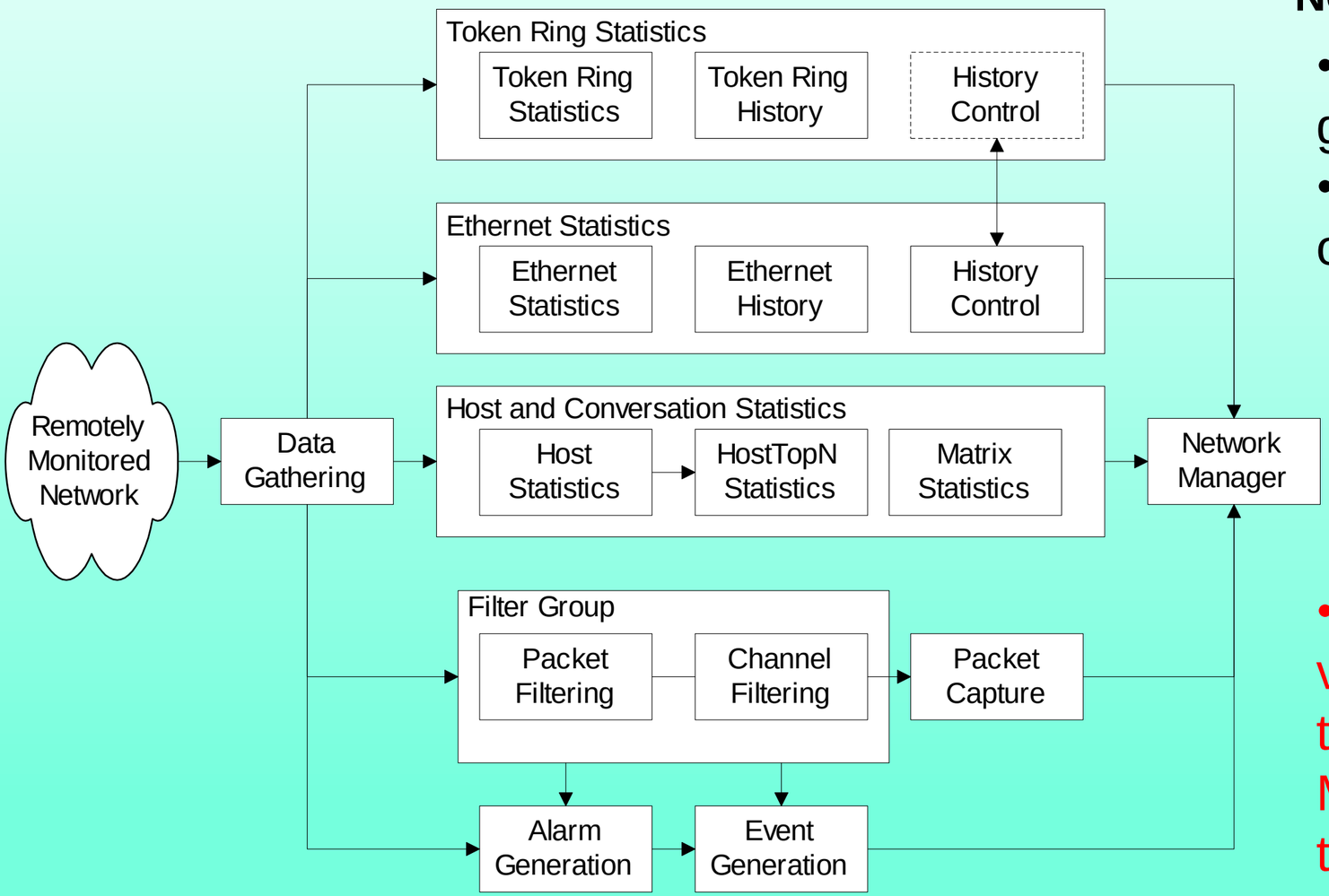


Figure 8.3 RMON1 Groups and Functions

Notes

- Probes on remotely monitored networks gather data
- The data can serve as inputs to five sets of functions
  - Statistics on Ethernet, token ring, and hosts / conversations
  - Filter group filters data prior to capture of data
  - Generation of alarms and events
- The above functions associated with the various groups are accomplished using ten groups associated with the RMON1 MIB. The first nine groups are applicable to common data and to Ethernet LAN, and the tenth group extends it to token-ring LAN.

RMON1 MIB Groups & Tables

Table 8.2 RMON1 MIB Groups and Tables

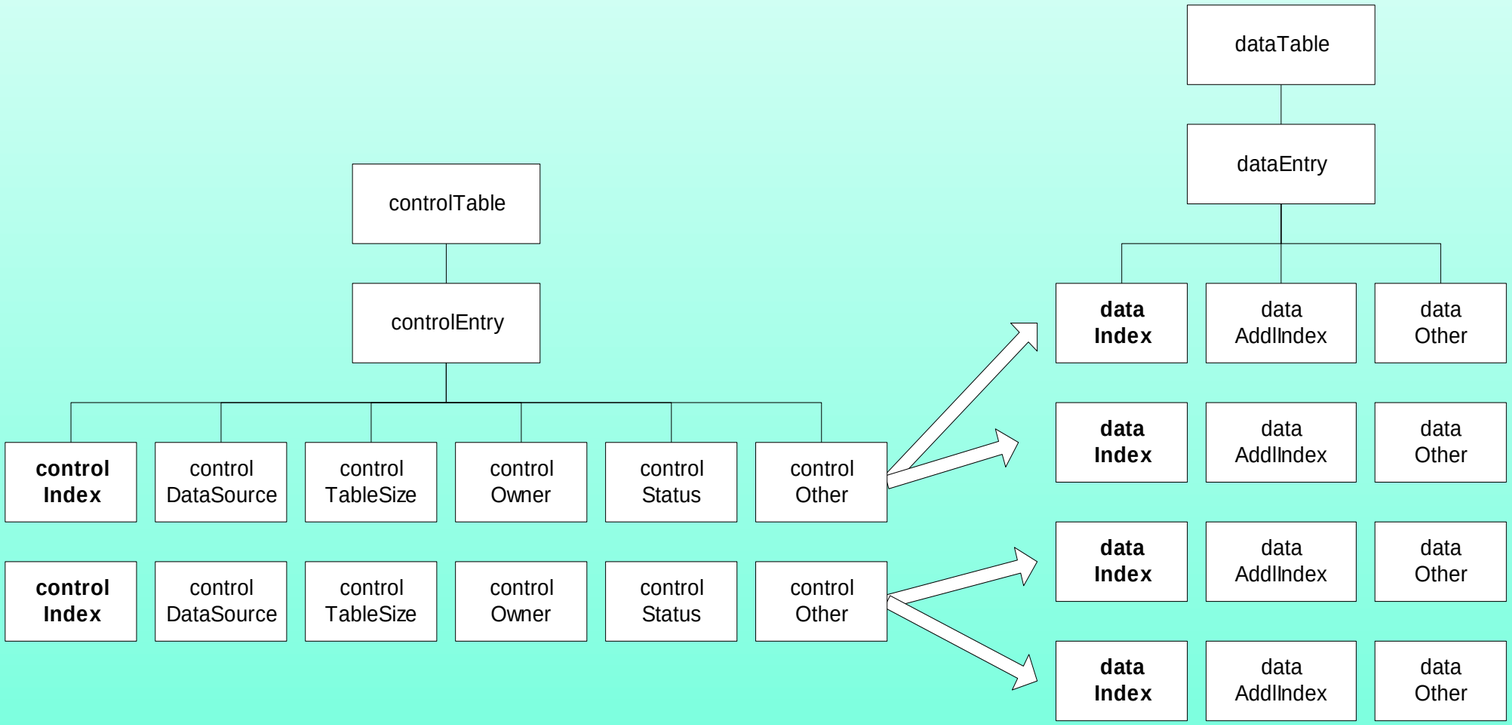
GROUP	OID	FUNCTION	TABLES
Statistics	rmon 1	Provides link-level statistics	–etherStatsTable
			–etherStats2Table
History	rmon 2	Collects periodic statistical data and stores for later retrieval	–historyControlTable
			–etherHistoryTable
			–historyControl2Table
			–etherHistory2Table
Alarm	rmon 3	Generates events when the data sample gathered crosses pre-established thresholds	–alarmTable
Host	rmon 4	Gathers statistical data on hosts	–hostControlTable
			–hostTable
			–hostTimeTable
			–hostControl2Table
Host Top N	rmon 5	Computes the top N hosts on the respective categories of statistics gathered	–hostTopNcontrolTable
Matrix	rmon 6	Gathers statistics on traffic between pairs of hosts	–matrixControlTable
			–matrixSDTable
			–matrixDSTable
			–matrixControl2Table
Filter	rmon 7	Performs filter function that enables capture of desired parameters	–filterTable
			–channelTable
			–filter2Table
			–channel2Table
Packet capture	rmon 8	Provides 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
- **Table 8.2, notice several of the groups have a data table and a control table.**

Relationship between Control and Data Tables

Here a generic representation of the relationship



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

Notes

•The data table contains rows (instances) of data.

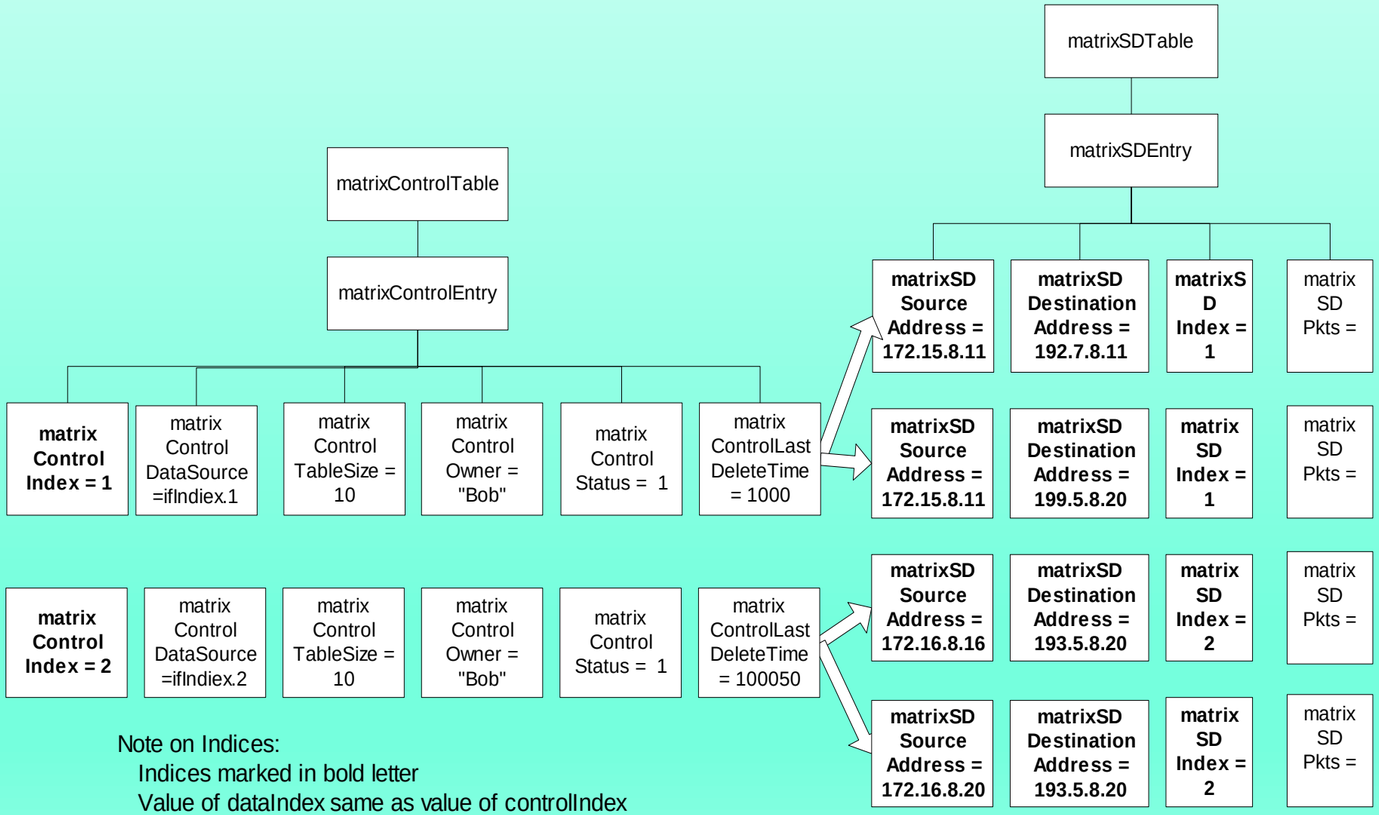
•The control table defines the instances of the data rows in the data table and is settable to gather and store different instances of data.

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

Figure 8.4 Relationship between Control and Data Tables

Matrix Control and SD Tables

understand how the data table and the control table work together using the matrix group in Table 8.2



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

Notes

• We can collect data based on source and destination addresses appearing in the packets on a given interface using the matrixSDTable (matrix source–destination table).

- The control index is an integer uniquely identifying the row in the control table. It would have a value of 1 for the first interface of a managed entity.
- The value of the columnar object, controlDataSource, identifies the source of the data that is being collected. In our example, if the interface #1 belongs to the interfaces group, then controlDataSource is ifIndex.1.

•controlTableSize identifies entries associated with the data source In our MSD table example, this would be the source–destination pair in each row of the table.

•ThecontrolOwner columnar object is the entity or person who created the entry. The entity could be either the agent or NMS, or a management person.
•The controlStatus is one of the entries listed in Table 8.1.

Host Group

- The host group contains information about the hosts on the network. It compiles the list of hosts by looking at the good packets traversing the network and extracting the source and destination
- MAC addresses. It maintains statistics on these hosts.

- There are three tables in the group: hostControl-Table,hostTable, and hostTimeTable.

- The hostControlTable controls the interfaces on which data gathering is done.

- The other two tables depend on this information. The hostTable contains statistics about the host.

- The hostTimeTable contains the same data as the host table, but is stored in the time order in which the host entry was discovered. This helps in the fast discovery of new hosts in the system.

- The entries in the two data tables are synchronized with respect to the host in the hostControlTable. We can obtain statistics on a host using this MIB.

Host Top N Group Example

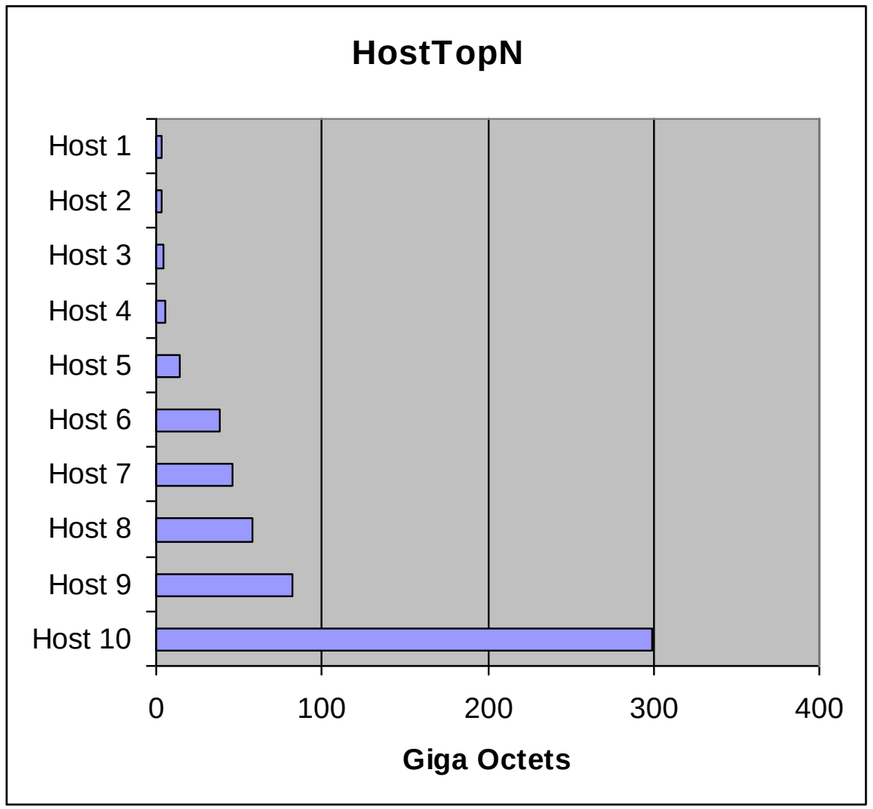


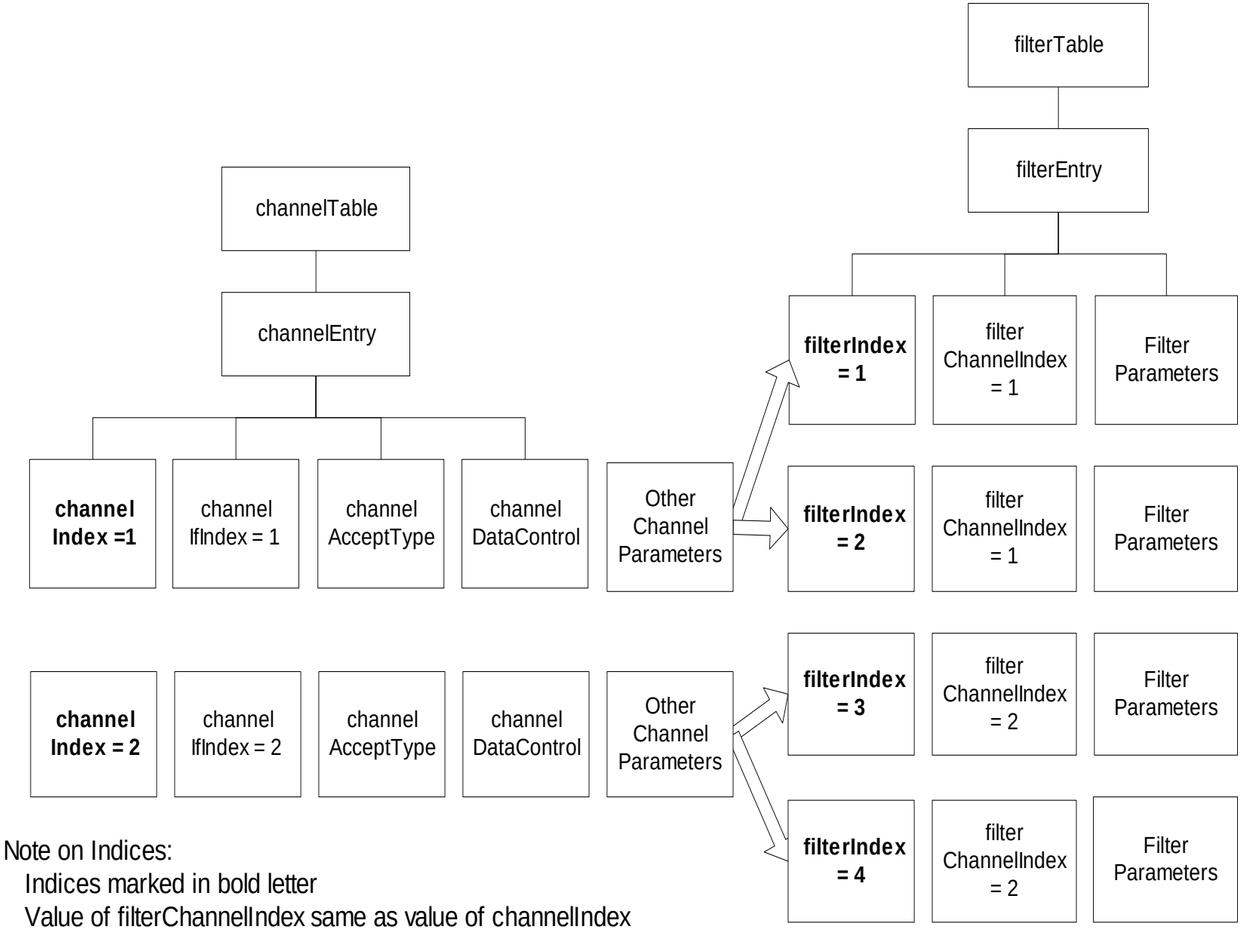
Figure 8.5 HostTop-10 Output Octets

The host top N group performs a report-generation function for ranking the top N hosts in the category of the selected statistics.

For example, we can rank–order the top ten hosts with maximum outgoing traffic. The HostTopNControlTable is used to initiate generation of such a report.

As an example of the type of data that can be acquired using an RMON probe, Figure 8.5 shows a chart derived using an RMON probe for the output octets of the top ten hosts in a network. The names of the hosts have been changed to generic host numbers for security reasons.

Filter Group



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

• The group contains a filter table and a channel table.

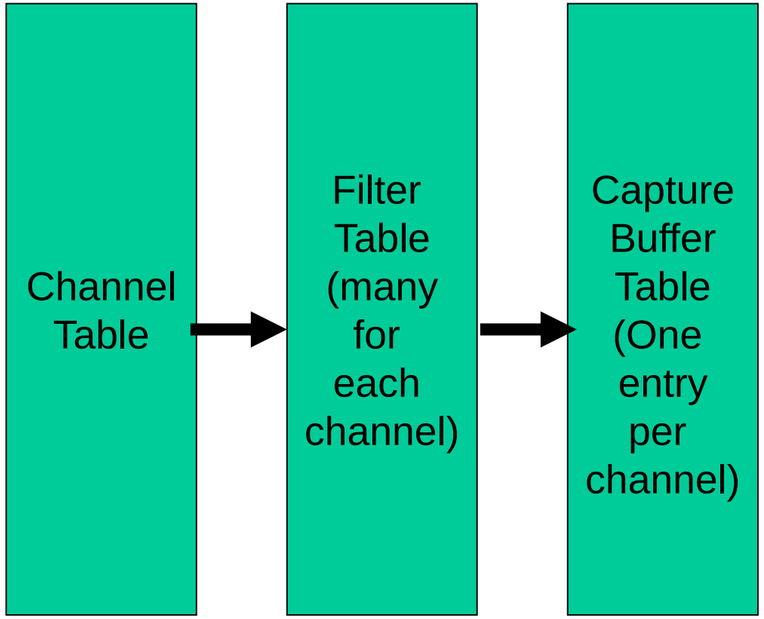
– Filter table allows packets to be filtered with an arbitrary filter expression, a set of filters associated with each channel. Each filter is defined by a row in the filter table.

– 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

– For each channel, the input packet is validated against each filter associated with that channel and is accepted if it passes any of the tests. A row in the channel table of the filter group includes the interface ID (same as ifIndex) with which the channel is associated, along with acceptance criteria. The combination of the filter and channel filtering provides enormous flexibility to select packets to be captured.

Packet Capture Group



- The packet capture group is a post-filter group. It captures packets from each channel based on the filter criteria of packet and channel filters in the filter group.
- The channel filter criteria for acceptance of the filter group output are controlled by the bufferControlTable
- Each packet captured is stored in the capture buffer table (captureBufferTable) as an instance.

Notes

•*Buffer control table used to select channels*

RMON Token-Ring Extension Groups

token-ring RMON MIB is an extension to RMON1 MIB and is specified in RFC 1513

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 (TR Statistics group) collects TR parameters: data on token-ring parameters such as token packets, errors in packets, bursts, polling, etc.
  - Promiscuous Statistics group addresses statistics on the number of packets of various sizes and the type of packets
  - There are two corresponding history statistics groups—current and promiscuous. Each of the four statistics groups has one data table associated with it.
- Three groups associated with the stations
  - The ring station group provides statistics on each station being monitored on the ring along with its status. The data are stored in the ringStationTable. The rings and parameters to be monitored are controlled by the ringStationControlTable.
  - The ring station order group provides the order of the station on the monitored rings and has only a data table.
  - The ring station configuration group manages the stations on the ring.
- The source-routing group . It is used to gather statistics on routing information in a pure source-routing environment.

RMON2

- Applicable to Layers 3 and above
- Functions similar to RMON1: Several of the groups and functions in RMON2 at higher layers are similar to that of the data link layer in RMON1.
- Enhancement to RMON1
- Defined conformance and compliance

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

- The architecture of RMON2 is the same as RMON1. RMON2 MIB is arranged into ten groups.
- The protocol directory group is an inventory of the protocols that the probe can monitor. The capability of the probe can be altered by reconfiguring the protocolDirTable. The protocols range from the data link control layer to the application layer.
- ….

A CASE STUDY ON INTERNET TRAFFIC USING RMON

- 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)

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%.