Remote Monitoring (RMON)

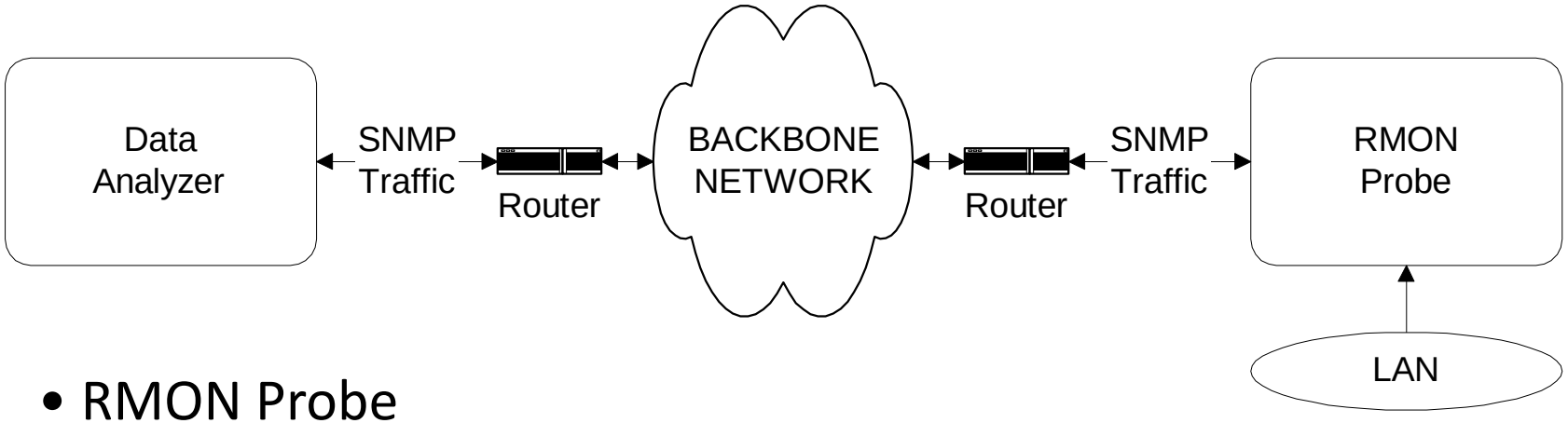
Ing. Pedro Escudero

Telf: 0994667184
Mail: pedro.escudero@unach.edu.ec
Web: https://www.researchgate.net/profile/Pedro-Escudero-3/research

Mayo - 2024

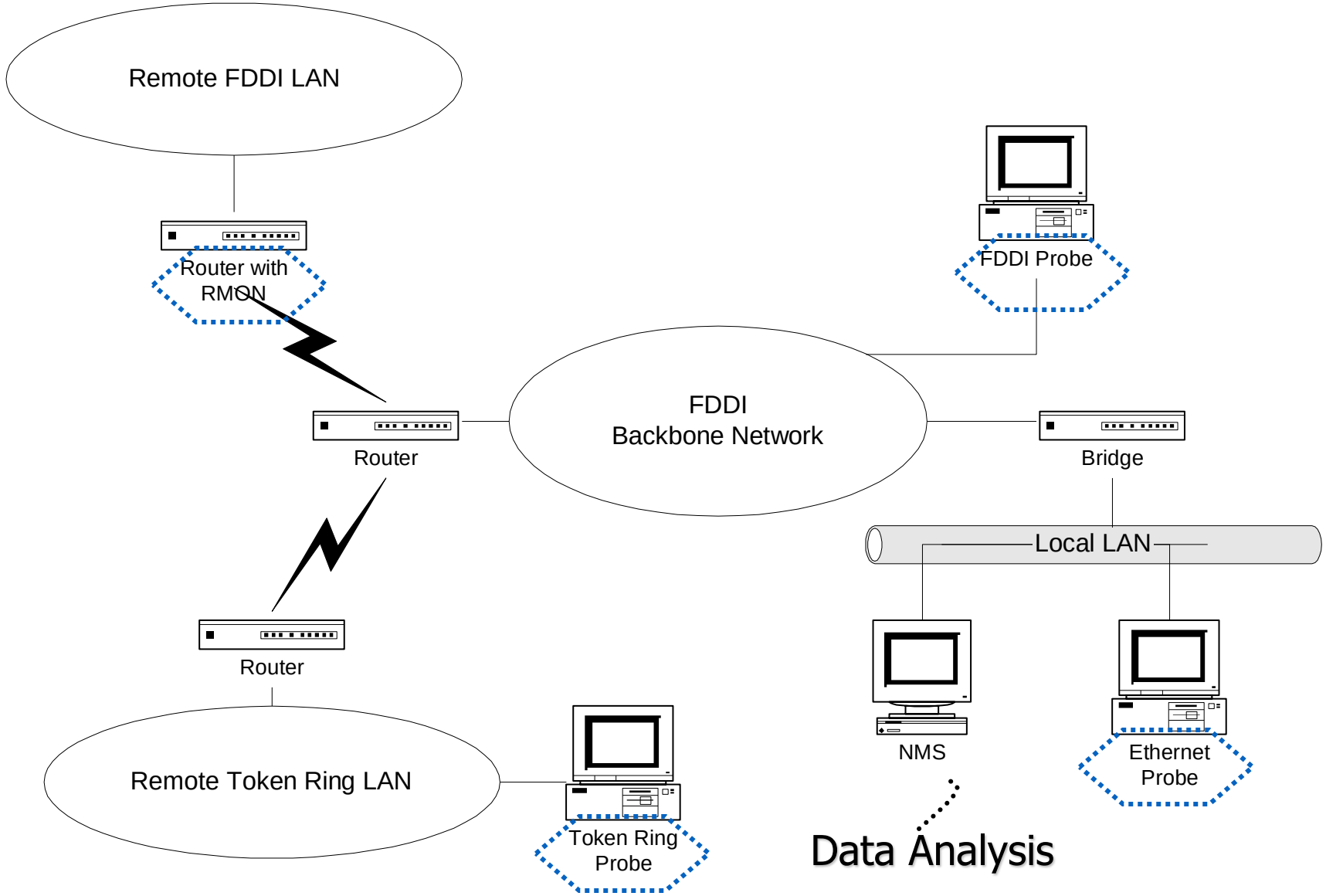
- **RMON Components**

RMON: Remote Network Monitoring



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

• Networks with RMONs



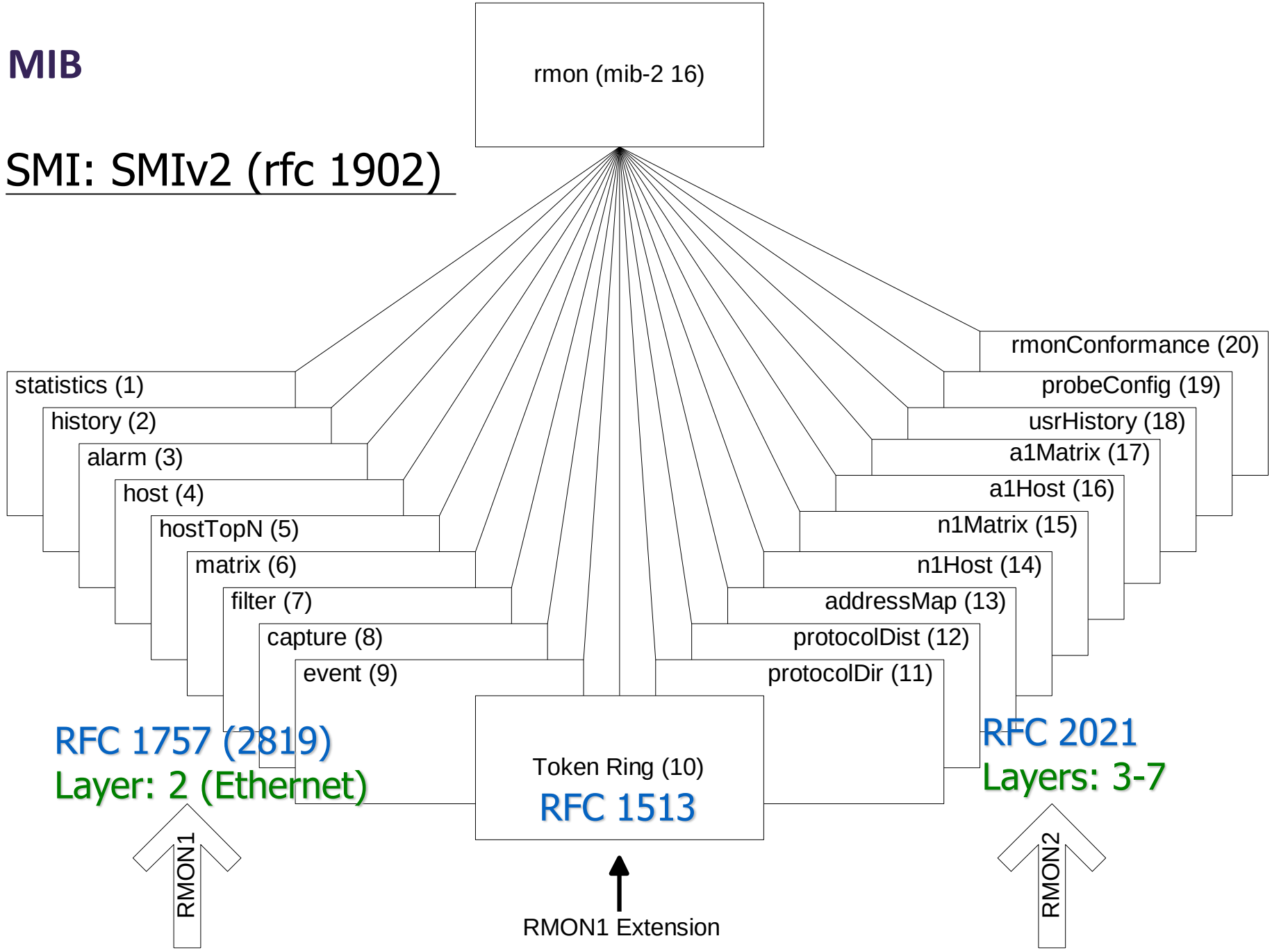
• Remote NM Goals

- Offline Operation
  - Perform diagnostics and to collect statistics continuously, even when communication with the management station may not be possible or efficient.
- Proactive Monitoring
  - Continuously run diagnostics and log network performance.
- Problem Detection and Reporting
  - Given conditions, the probe continuously to check for them.
  - If there any condition occurs, notify the manager.
- Value Added Data
  - Who generate the most traffic or errors, …
- Multiple Managers

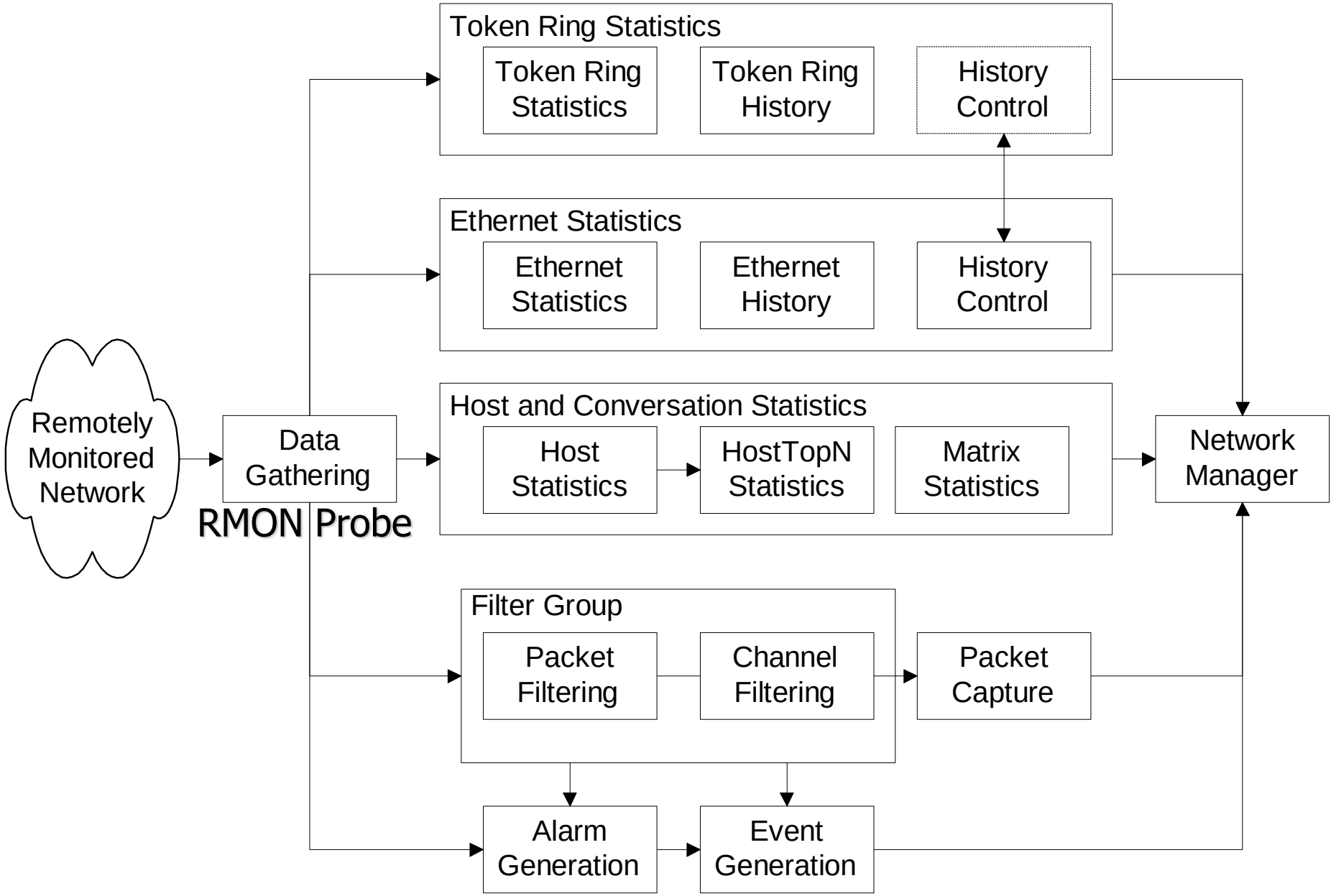
• RMON Benefits

- 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

- **RMON MIB**


rmon (mib-2 16)
SMI: SMIv2 (rfc 1902)
statistics (1)
history (2)
alarm (3)
host (4)
hostTopN (5)
matrix (6)
filter (7)
capture (8)
event (9)
rmonConformance (20)
probeConfig (19)
usrHistory (18)
a1Matrix (17)
a1Host (16)
n1Matrix (15)
n1Host (14)
addressMap (13)
protocolDist (12)
protocolDir (11)
RFC 1757 (2819)
Layer: 2 (Ethernet)
Token Ring (10)
RFC 1513
RFC 2021
Layers: 3-7
RMON1
RMON1 Extension
RMON2

- **RMON Groups and Functions**



• RMON1 MIB Groups & Tables

- 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

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

- **RMON1 MIB Groups & Tables**

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

• Textual Convention: Row Creation & Deletion

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

- **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.

TimeTicks

RFC 2021: RMON2

- **TimeFilter**

```
fooTable  {
  SYNTAX SEQUENCE Of FooEntry
  ...
}
fooEntry {
  SYNTAX FooEntry
  INDEX { fooTimeMark, fooIndex }
  ...
}
FooEntry {
            fooTimeMark   TimeFilter
            fooIndex      INTEGER,
            fooCounts     Counter
}
...
```

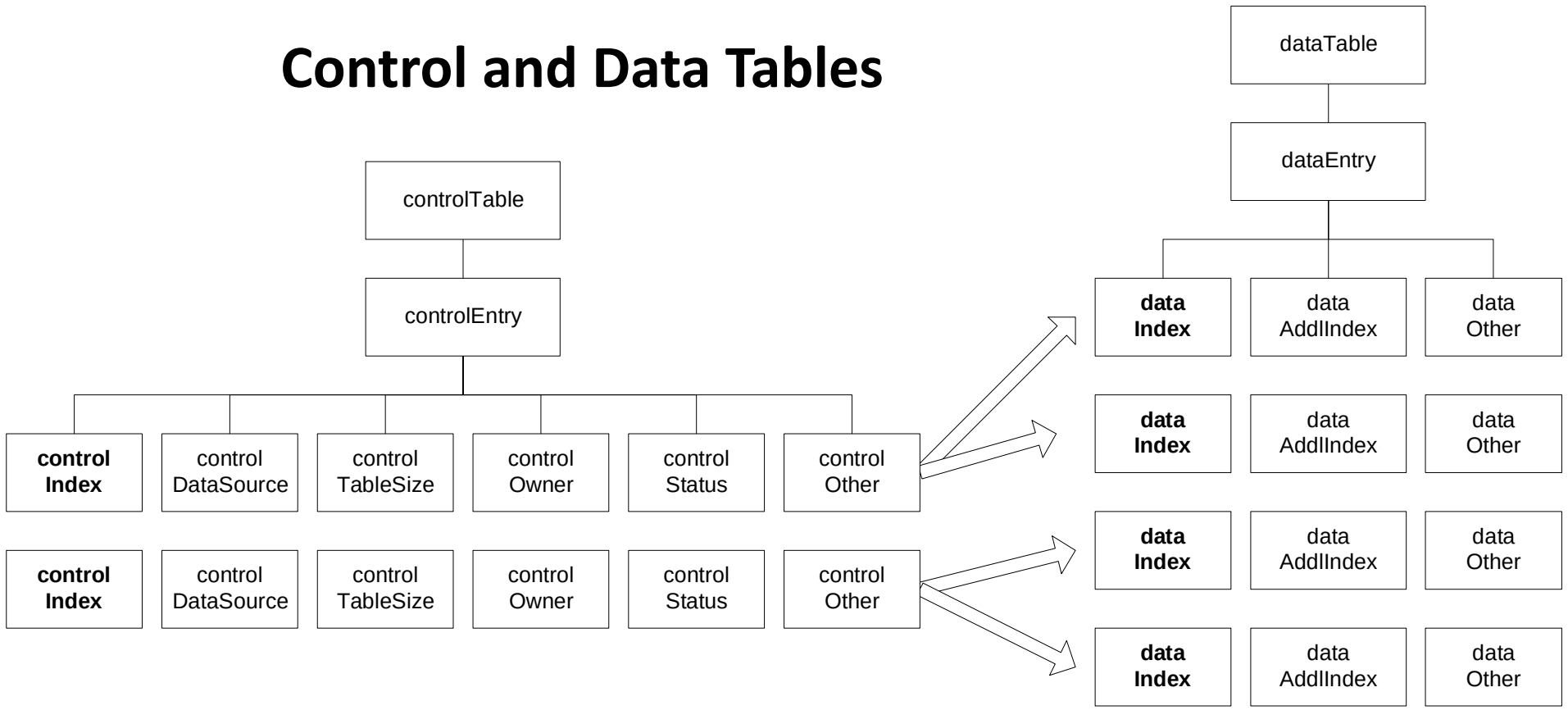
fooTable

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
fooCounts.5.2 9

fooCounts of (fooIndex = 1) was updated at time 5
fooCounts of (fooIndex = 2) was updated at time 9

• Control of Remote Network Monitoring Devices



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

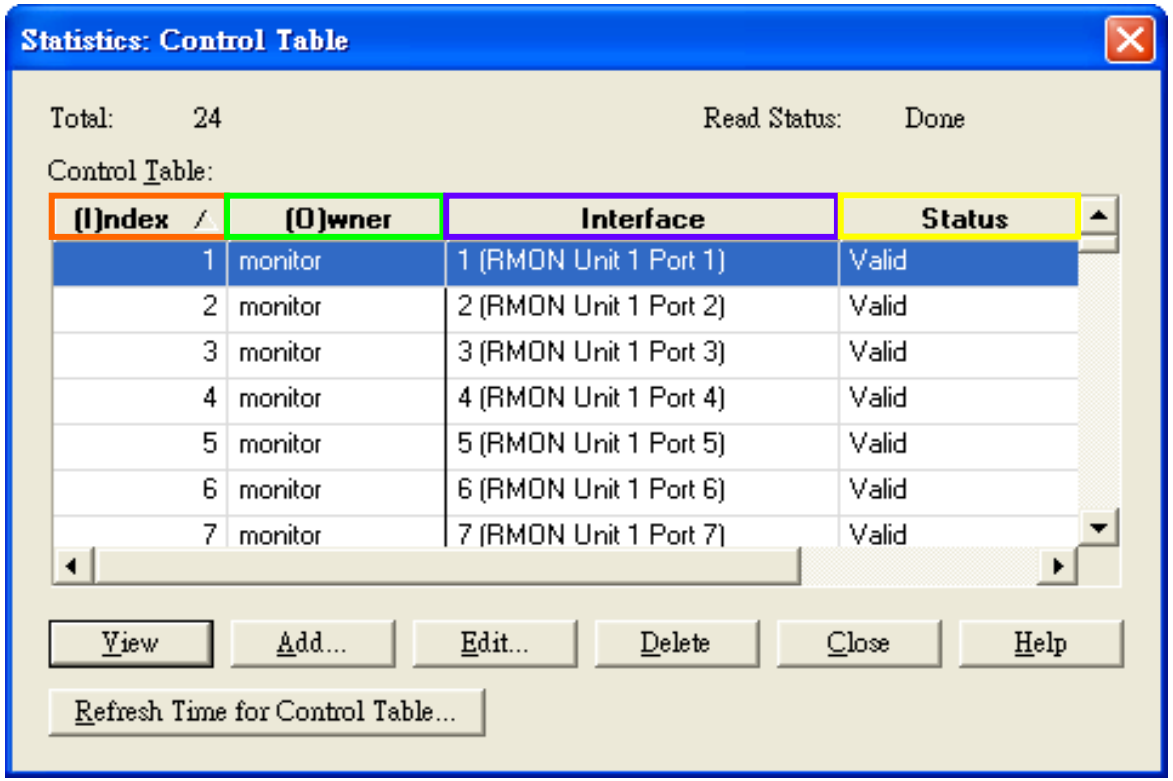
- **Statistics**

rmon 1

etherStatsTable
etherStatsEntry
etherStatsIndex
etherStatsDataSource
etherStatsDropEvents
etherStatsOctets
etherStatsPkts
etherStatsBroadcastPkts
etherStatsMulticastPkts
etherStatsCRCAlignErrors
etherStatsUndersizePkts
etherStatsOversizePkts
etherStatsFragments
etherStatsJabbers
etherStatsCollisions
etherStatsPkts64Octets
etherStatsPkts65to127Octets
etherStatsPkts128to255Octets
etherStatsPkts256to511Octets
etherStatsPkts512to1023Octets
etherStatsPkts1024to1518Octets
etherStatsOwner
etherStatsStatus

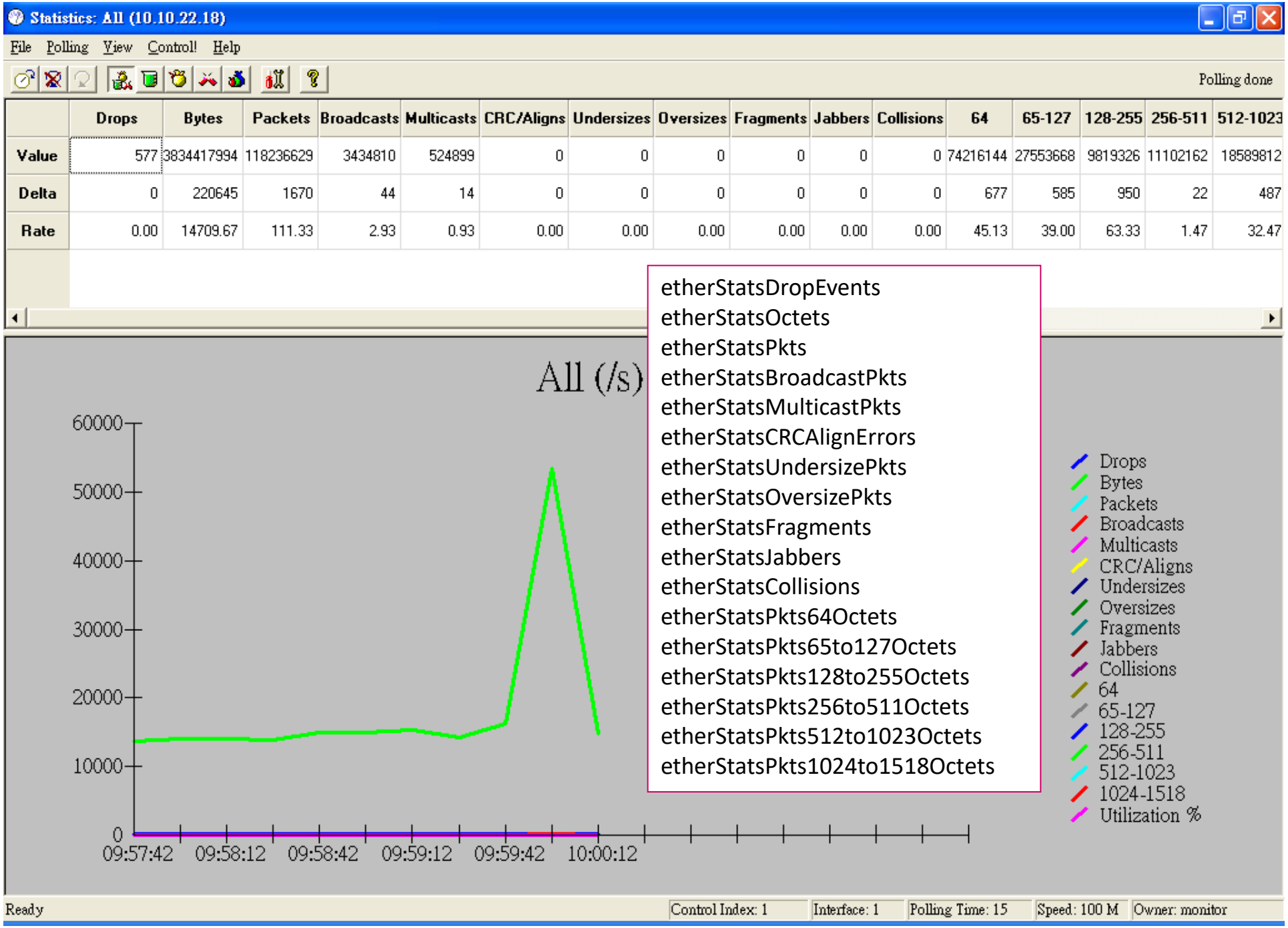
ifIndex.1.

- **Statistics**

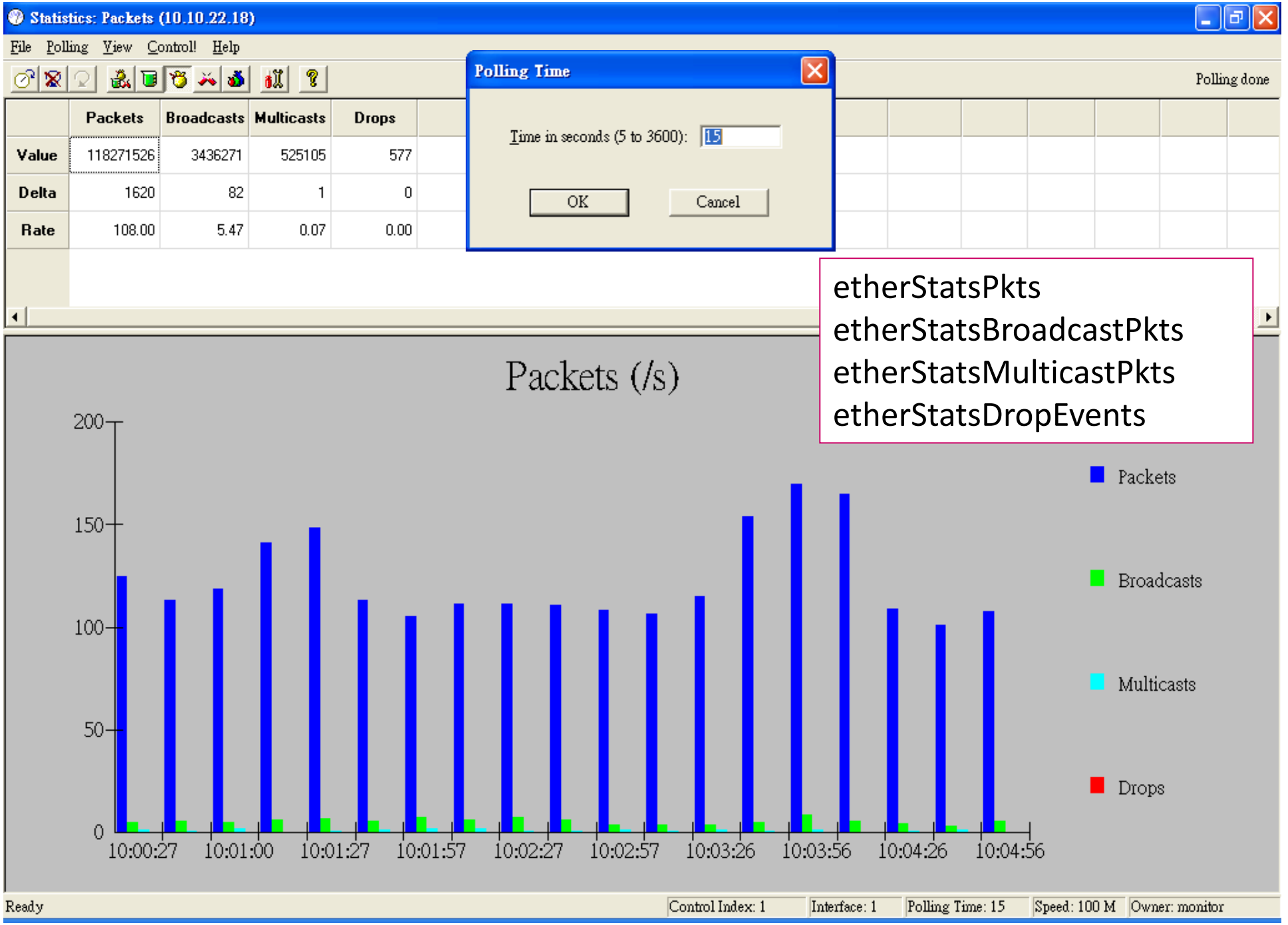


- etherStatsIndex
- etherStatsOwner
- ifDesrc.*x* (etherStatsDataSource) = *x*
- etherStatsStatus

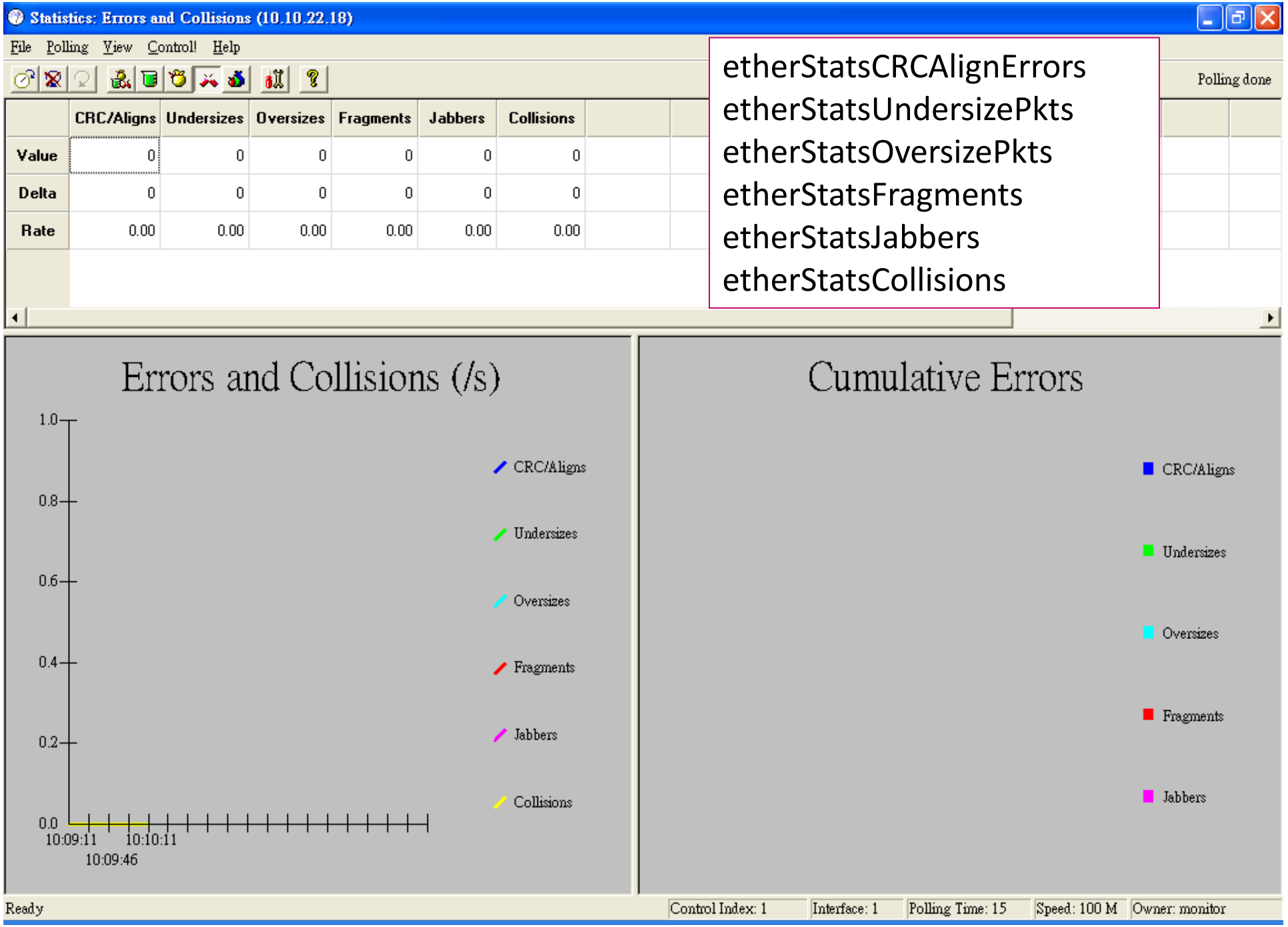
- **Statistics**


Statistics: All (10.10.22.18)
File Polling View Control! Help
Polling done
Drops Bytes Packets Broadcasts Multicasts CRC/Aligns Undersizes Oversizes Fragments Jabbers Collisions 64 65-127 128-255 256-511 512-1023
Value 577 3834417994 118236629 3434810 524899 0 0 0 0 0 0 74216144 27553668 9819326 11102162 18589812
Delta 0 220645 1670 44 14 0 0 0 0 0 0 677 585 950 22 487
Rate 0.00 14709.67 111.33 2.93 0.93 0.00 0.00 0.00 0.00 0.00 0.00 45.13 39.00 63.33 1.47 32.47
etherStatsDropEvents
etherStatsOctets
etherStatsPkts
etherStatsBroadcastPkts
etherStatsMulticastPkts
etherStatsCRCAlignErrors
etherStatsUndersizePkts
etherStatsOversizePkts
etherStatsFragments
etherStatsJabbers
etherStatsCollisions
etherStatsPkts64Octets
etherStatsPkts65to127Octets
etherStatsPkts128to255Octets
etherStatsPkts256to511Octets
etherStatsPkts512to1023Octets
etherStatsPkts1024to1518Octets
All (/s)
60000
50000
40000
30000
20000
10000
0
09:57:42
09:58:12
09:58:42
09:59:12
09:59:42
10:00:12
Drops
Bytes
Packets
Broadcasts
Multicasts
CRC/Aligns
Undersizes
Oversizes
Fragments
Jabbers
Collisions
64
65-127
128-255
256-511
512-1023
1024-1518
Utilization %
Ready
Control Index: 1
Interface: 1
Polling Time: 15
Speed: 100 M
Owner: monitor

- **Statistics**


Statistics: Packets (10.10.22.18)
File Polling View Control! Help
Polling done
Packets Broadcasts Multicasts Drops
Value 118271526 3436271 525105 577
Delta 1620 82 1 0
Rate 108.00 5.47 0.07 0.00
Polling Time
Time in seconds (5 to 3600): 15
OK
Cancel
etherStatsPkts
etherStatsBroadcastPkts
etherStatsMulticastPkts
etherStatsDropEvents
Packets (/s)
200
150
100
50
0
10:00:27
10:01:00
10:01:27
10:01:57
10:02:27
10:02:57
10:03:26
10:03:56
10:04:26
10:04:56
Packets
Broadcasts
Multicasts
Drops
Ready
Control Index: 1
Interface: 1
Polling Time: 15
Speed: 100 M
Owner: monitor

- **Statistics**


Statistics: Errors and Collisions (10.10.22.18)
File Polling View Control! Help
Polling done
CRC/Aligns Undersizes Oversizes Fragments Jabbers Collisions
Value 0 0 0 0 0 0
Delta 0 0 0 0 0 0
Rate 0.00 0.00 0.00 0.00 0.00 0.00
etherStatsCRCAlignErrors
etherStatsUndersizePkts
etherStatsOversizePkts
etherStatsFragments
etherStatsJabbers
etherStatsCollisions
Errors and Collisions (/s)
1.0
0.8
0.6
0.4
0.2
0.0
10:09:11
10:10:11
10:09:46
CRC/Aligns
Undersizes
Oversizes
Fragments
Jabbers
Collisions
Cumulative Errors
CRC/Aligns
Undersizes
Oversizes
Fragments
Jabbers
Ready
Control Index: 1
Interface: 1
Polling Time: 15
Speed: 100 M
Owner: monitor

- **Statistics**

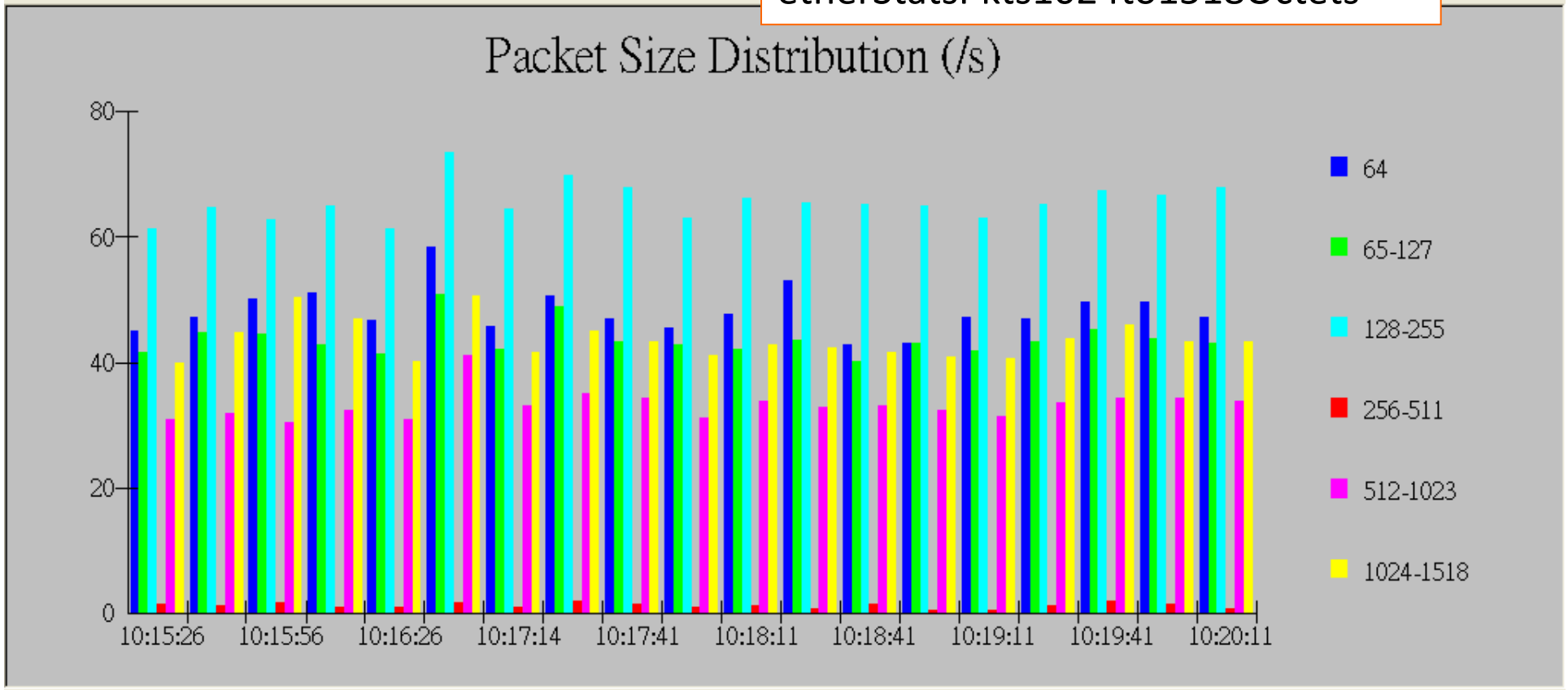
Statistics: Packet Size Distribution (10.10.22.18)

File Polling View Control! Help

Polling done

	64	65-127	128-255	256-511	512-1023	1024-1518
Value	74501116	27606947	9899940	11103520	18630202	93945605
Delta	710	646	1020	11	509	651
Rate	47.30	43.04	67.95	0.73	33.91	43.37

etherStatsPkts64Octets
etherStatsPkts65to127Octets
etherStatsPkts128to255Octets
etherStatsPkts256to511Octets
etherStatsPkts512to1023Octets
etherStatsPkts1024to1518Octets



Ready | Control Index: 1 | Interface: 1 | Polling Time: 15 | Speed: 100 M | Owner: monitor

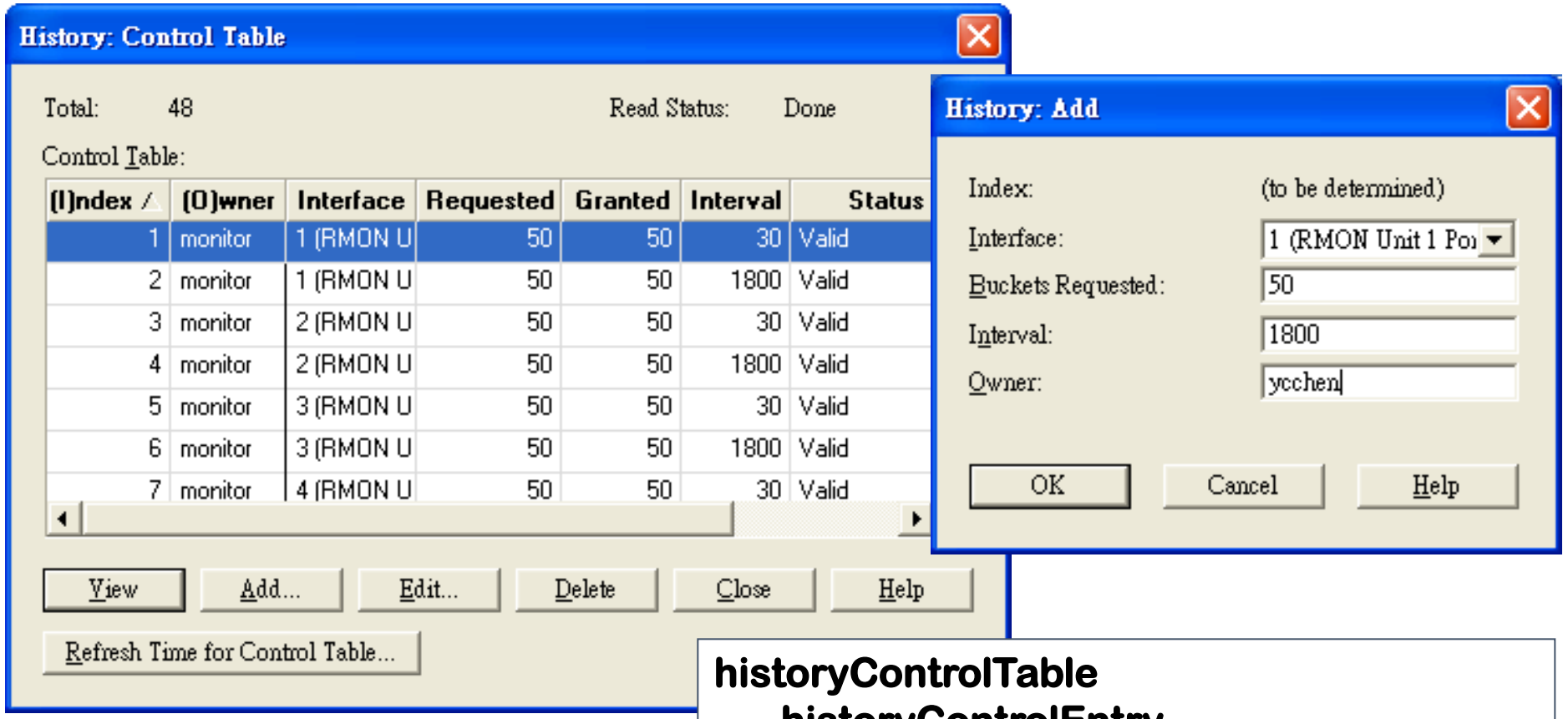
- **History**

historyControlTable
historyControlEntry
historyControlIndex
historyControlDataSource
historyControlBucketsRequested
historyControlBucketsGranted
historyControlInterval
historyControlOwner
historyControlStatus

etherHistoryTable
etherHistoryEntry
etherHistoryIndex →
etherHistorySampleIndex
etherHistoryIntervalStart
etherHistoryDropEvents
etherHistoryOctets
etherHistoryPkts
etherHistoryBroadcastPkts
etherHistoryMulticastPkts
etherHistoryCRCAlignErrors
etherHistoryUndersizePkts
etherHistoryOversizePkts
etherHistoryFragments
etherHistoryJabbers
etherHistoryCollisions
etherHistoryUtilization

rmon 2

- **History**



historyControlTable
- **historyControlEntry**
  - **historyControlIndex**
  - **historyControlDataSource**
  - **historyControlBucketsRequested**
  - **historyControlBucketsGranted**
  - **historyControlInterval**
  - **historyControlOwner**
  - **historyControlStatus**

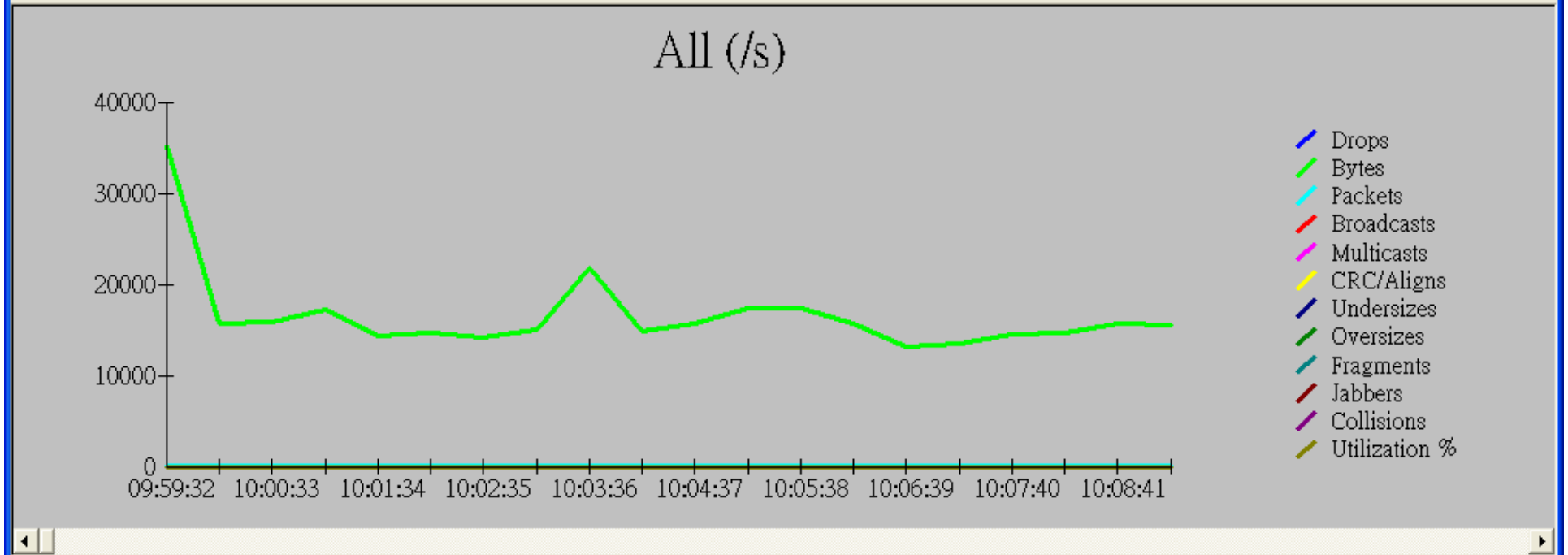
- **History**

History: All (10.10.22.18)

File Polling View Control! Help

Polling done

	Sample Idx	Interval Start	Drops	Bytes	Packets	Broadcasts	Multicasts	CRC/Aligns	Undersizes	Oversizes	Fragments	Jabbers	Collisions	Utilization %
47	25308	2006/5/28 10:22:54	0	753986	3764	137	11	0	0	0	0	0	0	1.00
48	25309	2006/5/28 10:23:24	0	474277	3638	129	38	0	0	0	0	0	0	1.00
49	25310	2006/5/28 10:23:55	0	468994	3740	122	21	0	0	0	0	0	0	1.00
50	25311	2006/5/28 10:24:25	1	508399	3889	123	24	0	0	0	0	0	0	1.00
51	25312	2006/5/28 10:24:55	6	550023	3915	133	23	0	0	0	0	0	0	1.00
52	25313	2006/5/28 10:25:26	2	614678	4855	172	19	0	0	0	0	0	0	1.00
53	25314	2006/5/28 10:25:55	0	799162	6829	156	14	0	0	0	0	0	0	1.00
54	25315	2006/5/28 10:26:27	0	633183	5264	220	11	0	0	0	0	0	0	1.00
55	25316	2006/5/28 10:26:56	0	550460	3961	138	41	0	0	0	0	0	0	21.00
56	25317	2006/5/28 10:27:28	0	249780	1731	102	13	0	0	0	0	0	0	1.00
57	25318	2006/5/28 10:27:57	0	287844	1714	157	12	0	0	0	0	0	0	1.00
58														



Ready | Control Index: 1 | Interface: 1 | Interval: 30 | Speed: 100 M | Owner: monitor

- **etherHistoryUtilization**

  - 10-Megabit ethernet utilization:

$$\text{Utilization} = \frac{\text{Pkts} * (9.6 + 6.4) + (\text{Octets} * .8)}{\text{Interval} * 10{,}000}$$

$$\text{Utilization} = \frac{\text{Pkts} * (96 + 64) + (\text{Octets} * 8)}{\text{Interval} * 10{,}000{,}000} \times 100\%$$

- **Alarm Group**

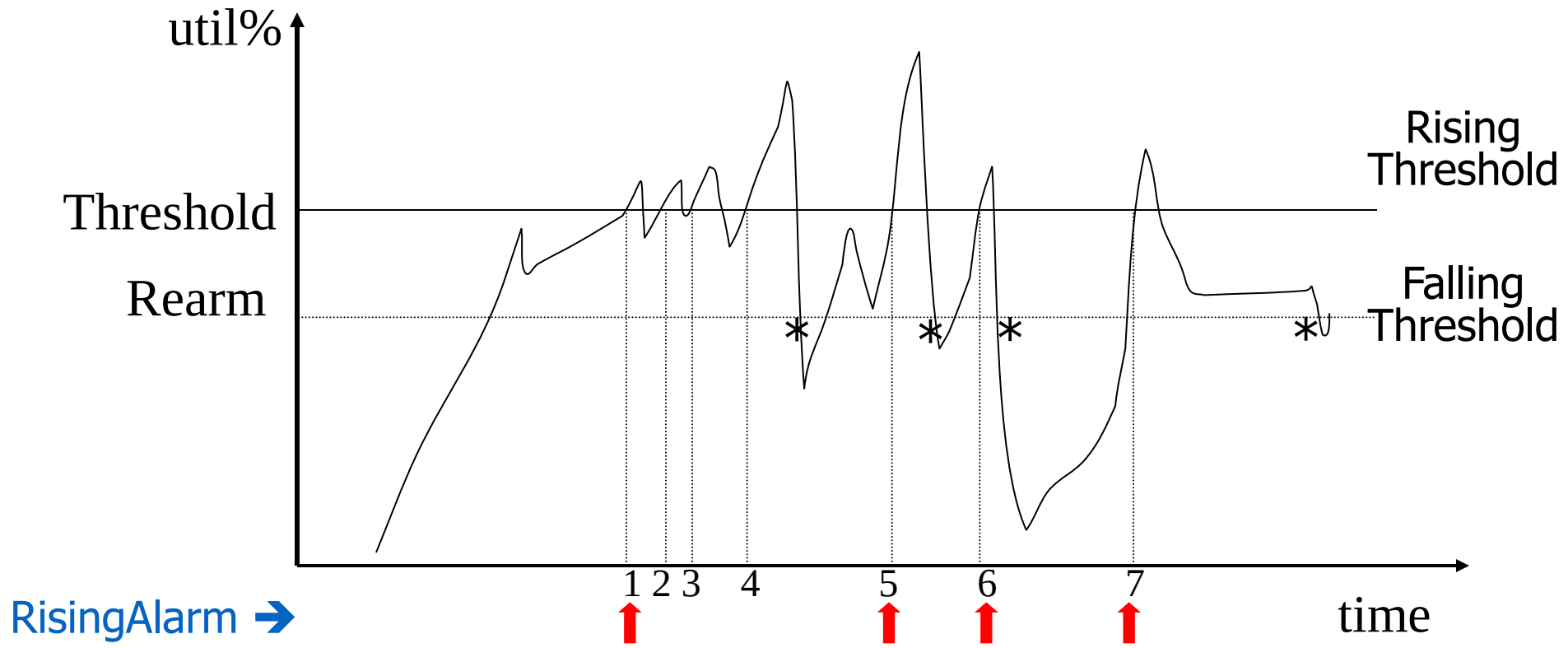
rmon 3

- Set thresholds on a variety of items affecting network performance
- When the thresholds are crossed, events are reported.
- In general, the values of thresholds are determined according to past experience.

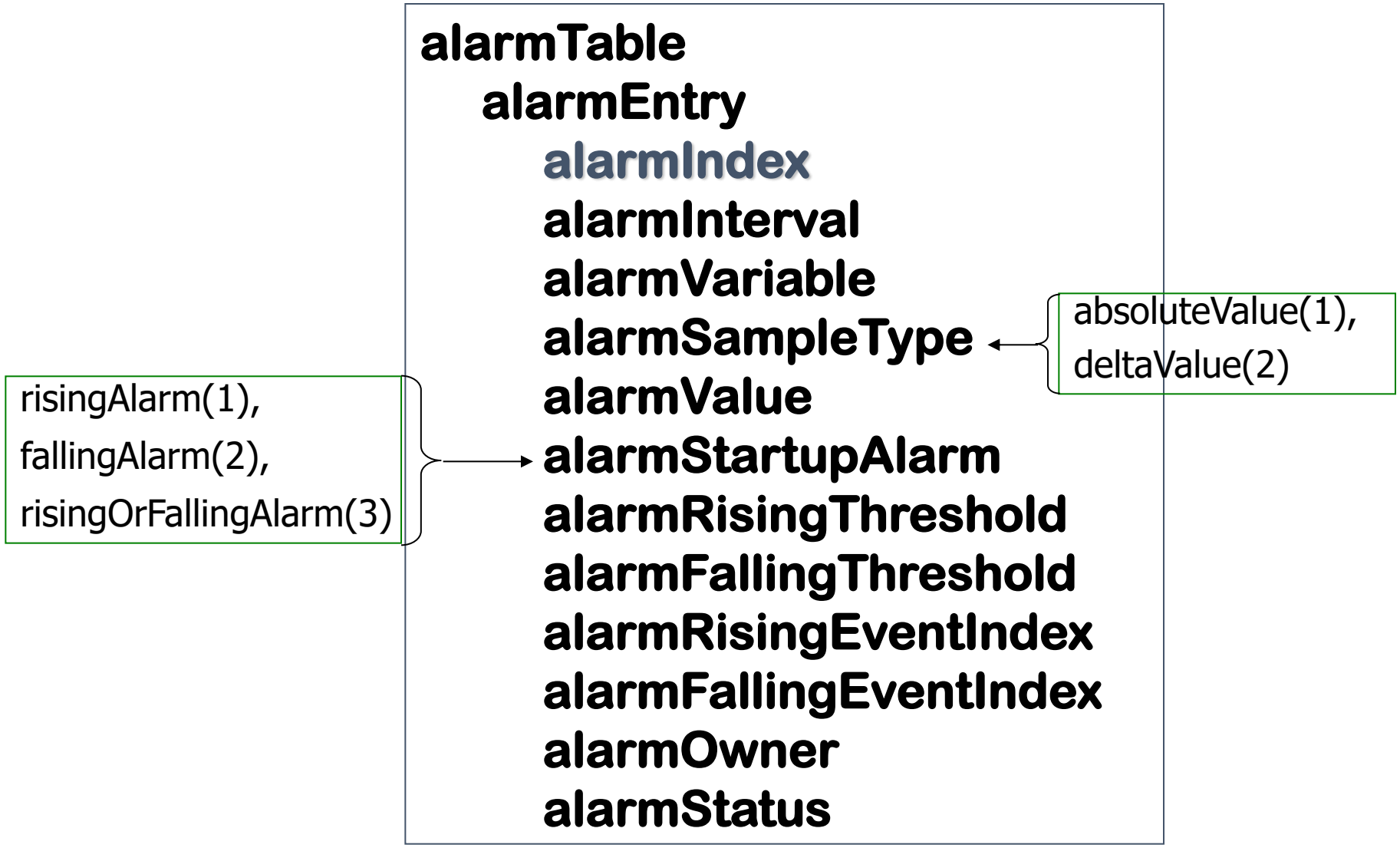
- **Thresholds**

- Threshold Priority
  - In general, priority: low, medium, high
  - Multiple threshold values for the same item
  - Thresholds for multiple items
  - RMON doesn't support multiple thresholds.
- Use ***rearm*** mechanism to avoid frequent threshold events
  - alarmRisingThreshold, alarmFallingThreshold

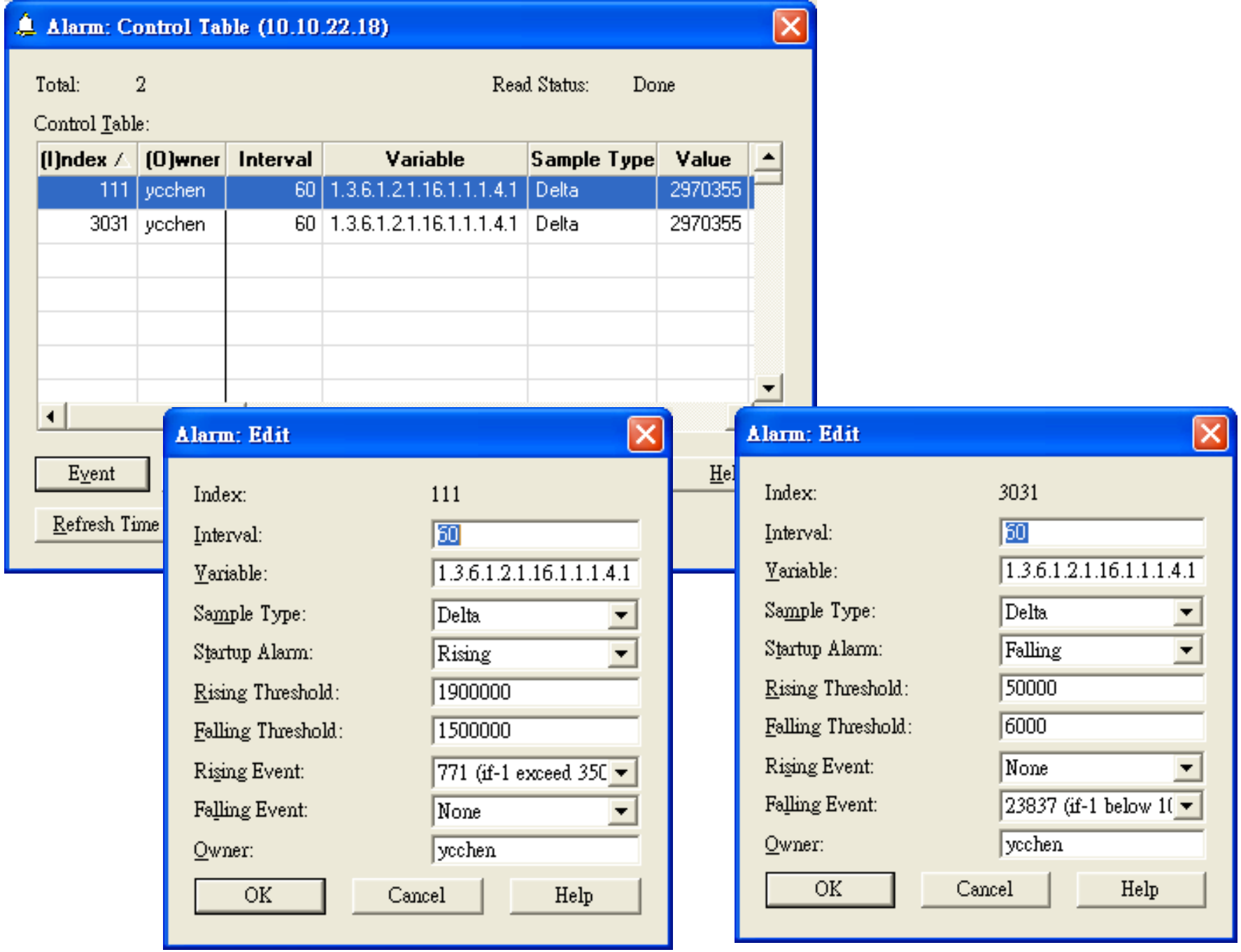
- **Alarms**


util%
Threshold
Rearm
Rising
Threshold
Falling
Threshold
1 2 3 4 5 6 7
time
RisingAlarm ➔

- **Alarms**



Alarm Index	Alarm Interval	Alarm Variable	Alarm SampleType	Alarm Value	Alarm StartupAlarm	Alarm Rising Threshold	Alarm Falling Threshold	Alarm Rising EventIndex	Alarm Falling EventIndex	Alarm Owner	Alarm Status
111	60	etherStatsOctets.1	deltaValue(2)	2489342	risingAlarm(1)	1900000	1500000	771	0	ycchen	valid(1
3031	60	etherStatsOctets.1	deltaValue(2)	2489342	fallingAlarm(2)	50000	6000	0	23837	ycchen	valid(1


Alarm: Control Table (10.10.22.18)
Total: 2
Read Status: Done
Control Table:
(I)ndex / (O)wner Interval Variable Sample Type Value
111 ycchen 60 1.3.6.1.2.1.16.1.1.1.4.1 Delta 2970355
3031 ycchen 60 1.3.6.1.2.1.16.1.1.1.4.1 Delta 2970355
Event
Refresh Time
Alarm: Edit
Index: 111
Interval: 30
Variable: 1.3.6.1.2.1.16.1.1.1.4.1
Sample Type: Delta
Startup Alarm: Rising
Rising Threshold: 1900000
Falling Threshold: 1500000
Rising Event: 771 (if-1 exceed 35(
Falling Event: None
Owner: ycchen
OK
Cancel
Help
Alarm: Edit
Index: 3031
Interval: 30
Variable: 1.3.6.1.2.1.16.1.1.1.4.1
Sample Type: Delta
Startup Alarm: Falling
Rising Threshold: 50000
Falling Threshold: 6000
Rising Event: None
Falling Event: 23837 (if-1 below 1(
Owner: ycchen
OK
Cancel
Help

- **Alarms**

```
Got a trap from: 10.10.22.18
Enterprise:     .1.3.6.1.2.1.16
Agent-Address:  10.10.22.18
Generic-Trap:   6
Specific-Trap:  1
Timestamp:      85114030
VariableBindings: (5)
  .1.3.6.1.2.1.16.3.1.1.1.111: 111
  .1.3.6.1.2.1.16.3.1.1.3.111: .1.3.6.1.2.1.16.1.1.1.4.1
  .1.3.6.1.2.1.16.3.1.1.4.111: 2
  .1.3.6.1.2.1.16.3.1.1.5.111: 2791697
  .1.3.6.1.2.1.16.3.1.1.7.111: 1900000
```

```
risingAlarm NOTIFICATION-TYPE
   OBJECTS  { alarmIndex, alarmVariable, alarmSampleType,
            alarmValue, alarmRisingThreshold }
   STATUS   current
   DESCRIPTION
      "The SNMP trap that is generated when an alarm
      entry crosses its rising threshold and generates
      an event that is configured for sending SNMP
      traps."
   ::= { rmonEventsV2 1 }

fallingAlarm NOTIFICATION-TYPE
   OBJECTS { alarmIndex, alarmVariable, alarmSampleType,
            alarmValue, alarmFallingThreshold }
   STATUS    current
   DESCRIPTION
      "The SNMP trap that is generated when an alarm
      entry crosses its falling threshold and generates
      an event that is configured for sending SNMP
      traps."
   ::= { rmonEventsV2 2 }
```

- **Event**

rmon 9

eventTable
- **eventEntry**
  - **eventIndex**
  - **eventDescription**
  - **eventType**
  - **eventCommunity**
  - **eventLastTimeSent**
  - **eventOwner**
  - **eventStatus**

none(1),
log(2),
snmptrap(3),
logandtrap(4)

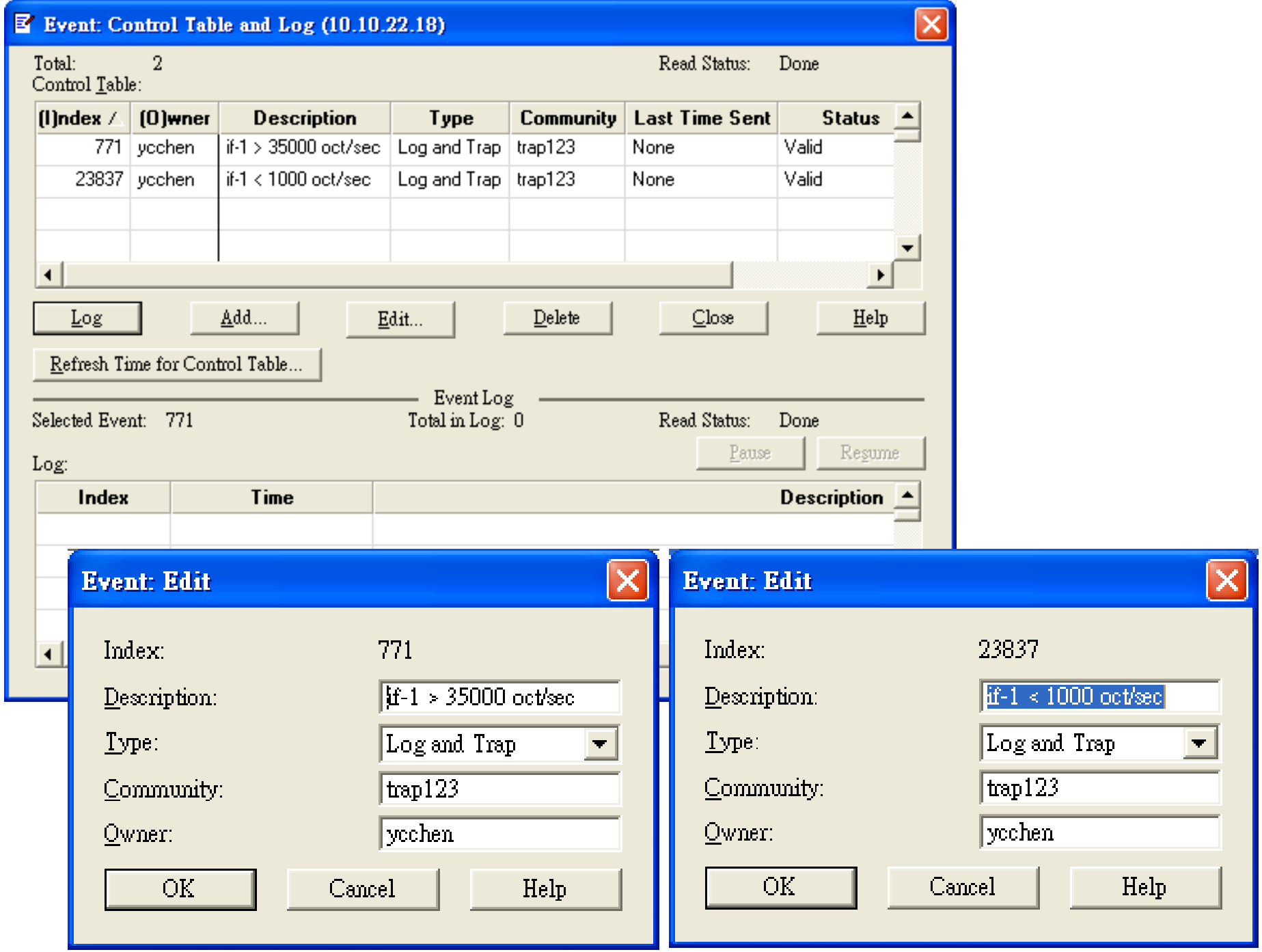
logTable
- **logEntry**
  - **logEventIndex**
  - **logIndex**
  - **logTime**
  - **logDescription**

eventTable

Event Index	Event Description	Event Type	Event Community	Event LastTimeSent	Event Owner	Event Status
771	if-1 exceed 35000 octets/sec	logandtrap(4)	trap123	11 days, 0 hours, 40 minutes, 12 seconds.	ycchen	valid(1)
23837	if-1 below 1000 oct/sec	logandtrap(4)	trap123	0 hours, 0 minutes, 0 seconds.	ycchen	valid(1)

logTable

Index	Log EventIndex	Log Index	Log Time	logDescription
771.1	771	1	9 days, 20 hours, 25 minutes, 40 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2791697, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.2	771	2	9 days, 20 hours, 46 minutes, 59 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 5221004, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.3	771	3	9 days, 20 hours, 52 minutes, 1 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2755232, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.4	771	4	9 days, 21 hours, 52 minutes, 23 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2142307, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.5	771	5	9 days, 23 hours, 14 minutes, 33 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2323511, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.6	771	6	9 days, 23 hours, 27 minutes, 14 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2062203, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.7	771	7	9 days, 23 hours, 32 minutes, 18 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 1914068, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"
771.8	771	8	9 days, 23 hours, 34 minutes, 51 seconds.	.1.3.6.1.2.1.16.1.1.1.4.1 (delta = 2165422, Rising Threshold = 1900000, interval = 60)[alarmIndex.111][trap] "if-1 exceed 35000 octets/sec"


Event: Control Table and Log (10.10.22.18)
Total: 2
Read Status: Done
Control Table:
(I)ndex / (O)wner Description Type Community Last Time Sent Status
771 ycchen if-1 > 35000 oct/sec Log and Trap trap123 None Valid
23837 ycchen if-1 < 1000 oct/sec Log and Trap trap123 None Valid
Log
Add...
Edit...
Delete
Close
Help
Refresh Time for Control Table...
Event Log
Selected Event: 771
Total in Log: 0
Read Status: Done
Pause
Resume
Log:
Index Time Description
Event: Edit
Index: 771
Description: if-1 > 35000 oct/sec
Type: Log and Trap
Community: trap123
Owner: ycchen
OK
Cancel
Help
Event: Edit
Index: 23837
Description: if-1 < 1000 oct/sec
Type: Log and Trap
Community: trap123
Owner: ycchen
OK
Cancel
Help

- **Hosts**

rmon 4

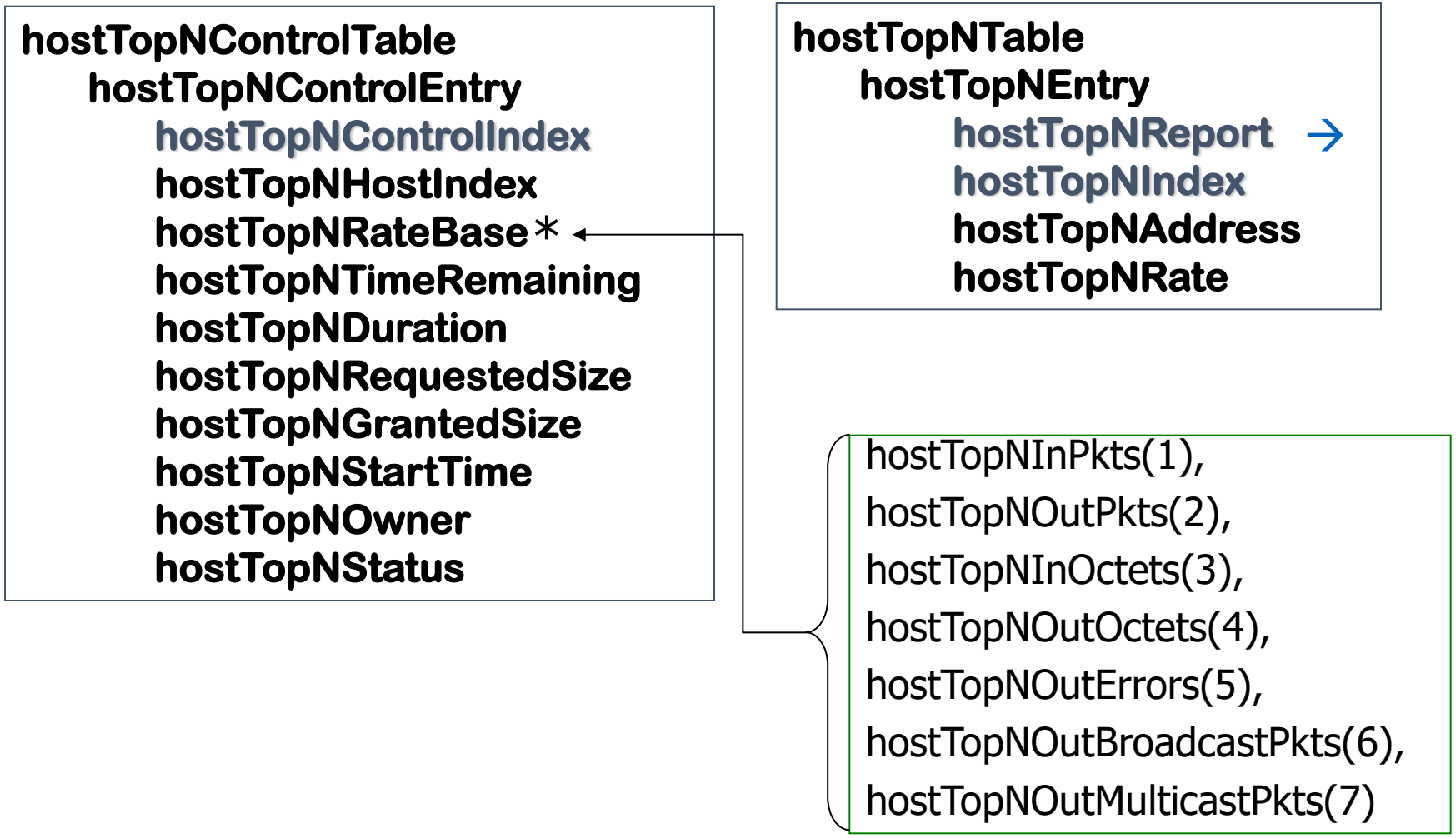
hostControlTable
- hostControlEntry
  - hostControlIndex
  - hostControlDataSource
  - hostControlTableSize
  - hostControlLastDeleteTime
  - hostControlOwner
  - hostControlStatus

hostTable
- hostEntry
  - hostAddress
  - hostCreationOrder
  - hostIndex →
  - hostInPkts
  - hostOutPkts
  - hostInOctets
  - hostOutOctets
  - hostOutErrors
  - hostOutBroadcastPkts
  - hostOutMulticastPkts

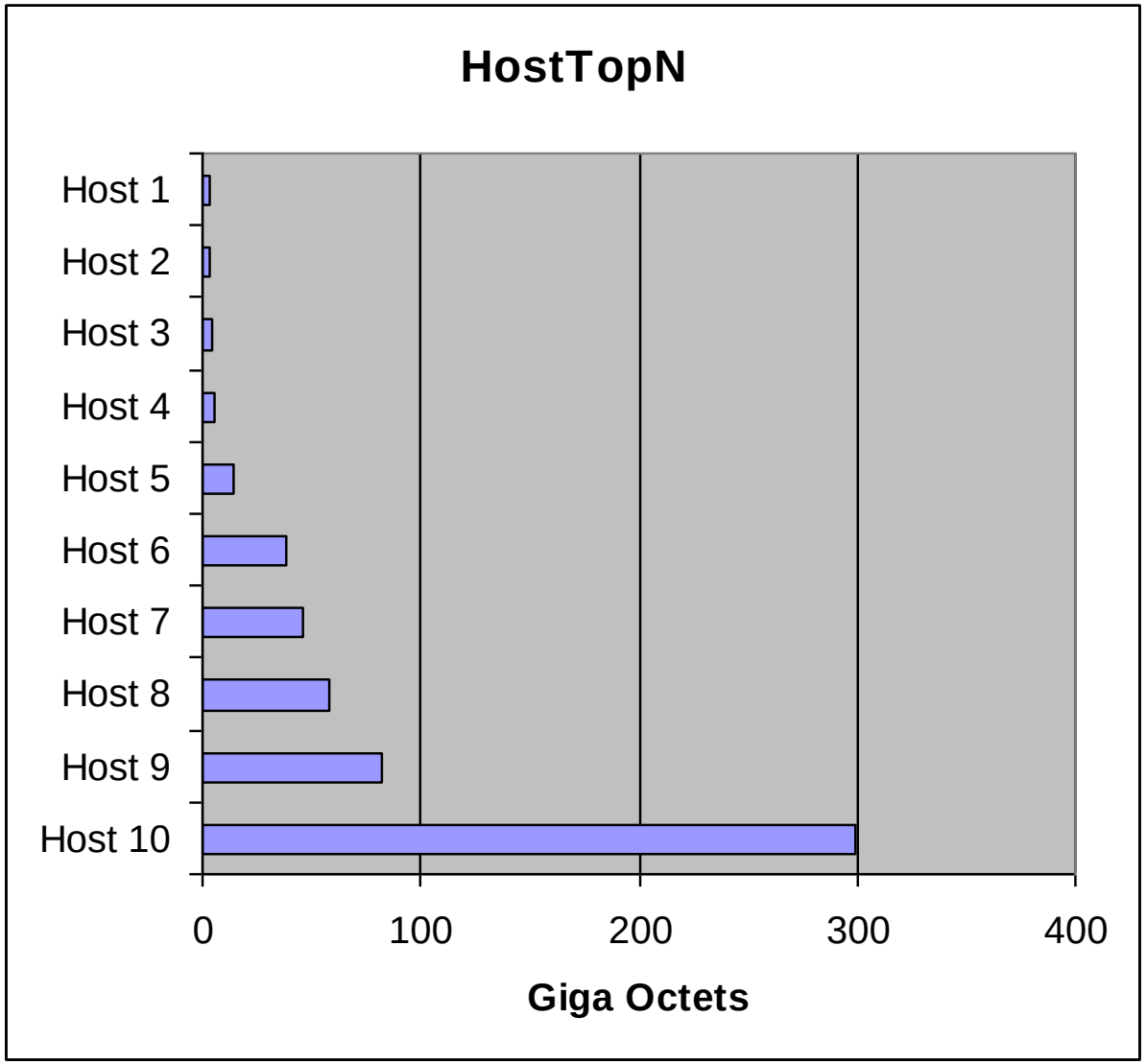
hostTimeTable
- hostTimeEntry
  - hostTimeAddress
  - hostTimeCreationOrder
  - hostTimeIndex →
  - hostTimeInPkts
  - hostTimeOutPkts
  - hostTimeInOctets
  - hostTimeOutOctets
  - hostTimeOutErrors
  - hostTimeOutBroadcastPkts
  - hostTimeOutMulticastPkts

- **hostTopN**

rmon 5



- **Host Top N Group Example**



- **Matrix**

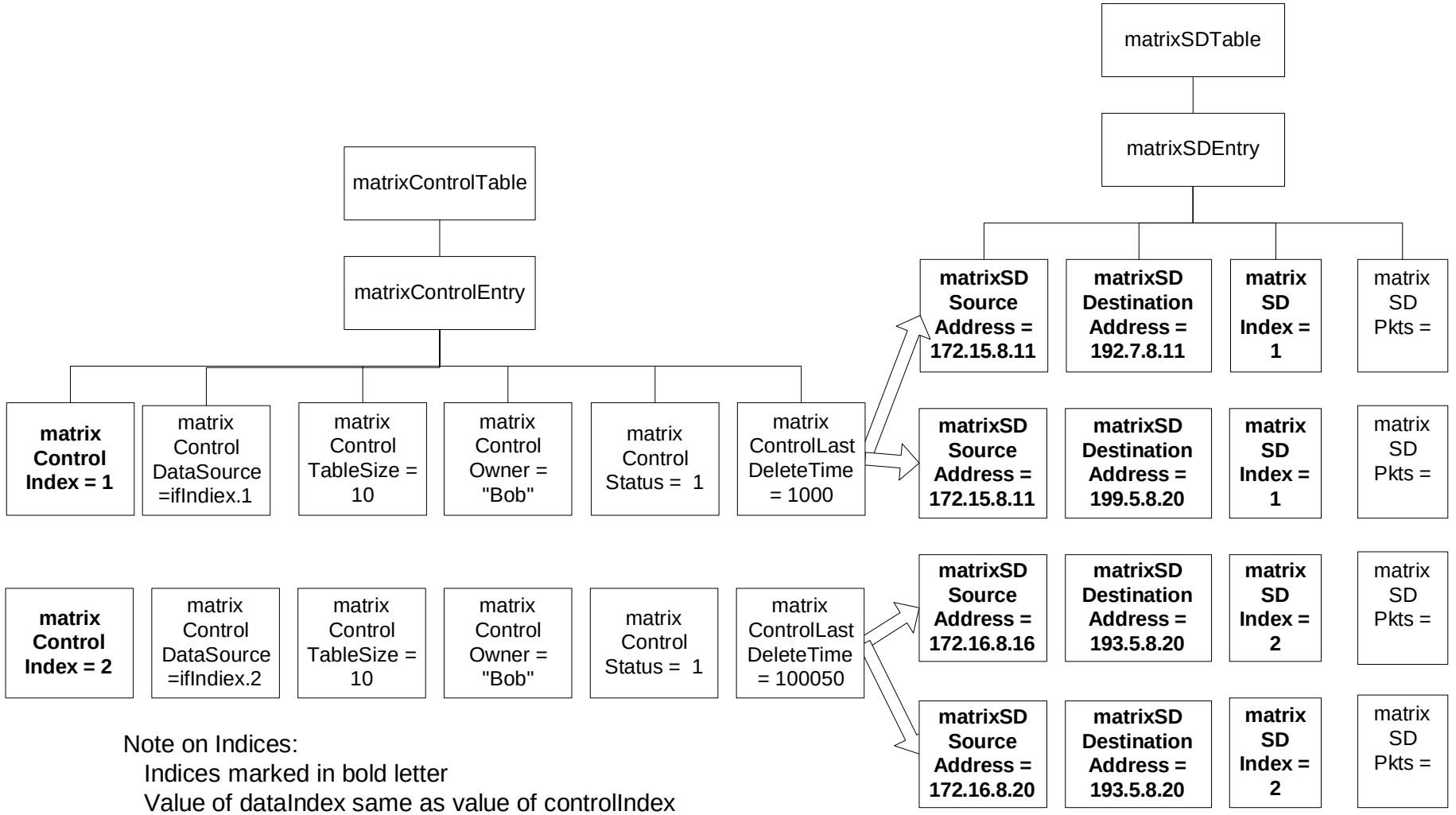
rmon 6

matrixControlTable
- matrixControlEntry
  - matrixControlIndex
  - matrixControlDataSource
  - matrixControlTableSize
  - matrixControlLastDeleteTime
  - matrixControlOwner
  - matrixControlStatus

matrixSDTable
- matrixSDEntry
  - matrixSDSourceAddress
  - matrixSDDestAddress
  - matrixSDIndex →
  - matrixSDPkts
  - matrixSDOctets
  - matrixSDErrors

matrixDSTable
- matrixDSEntry
  - matrixDSSourceAddress
  - matrixDSDestAddress
  - matrixDSIndex →
  - matrixDSPkts
  - matrixDSOctets
  - matrixDSErrors

• Matrix Control and SD Tables



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

- **Filter Group**

rmon 7

- 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

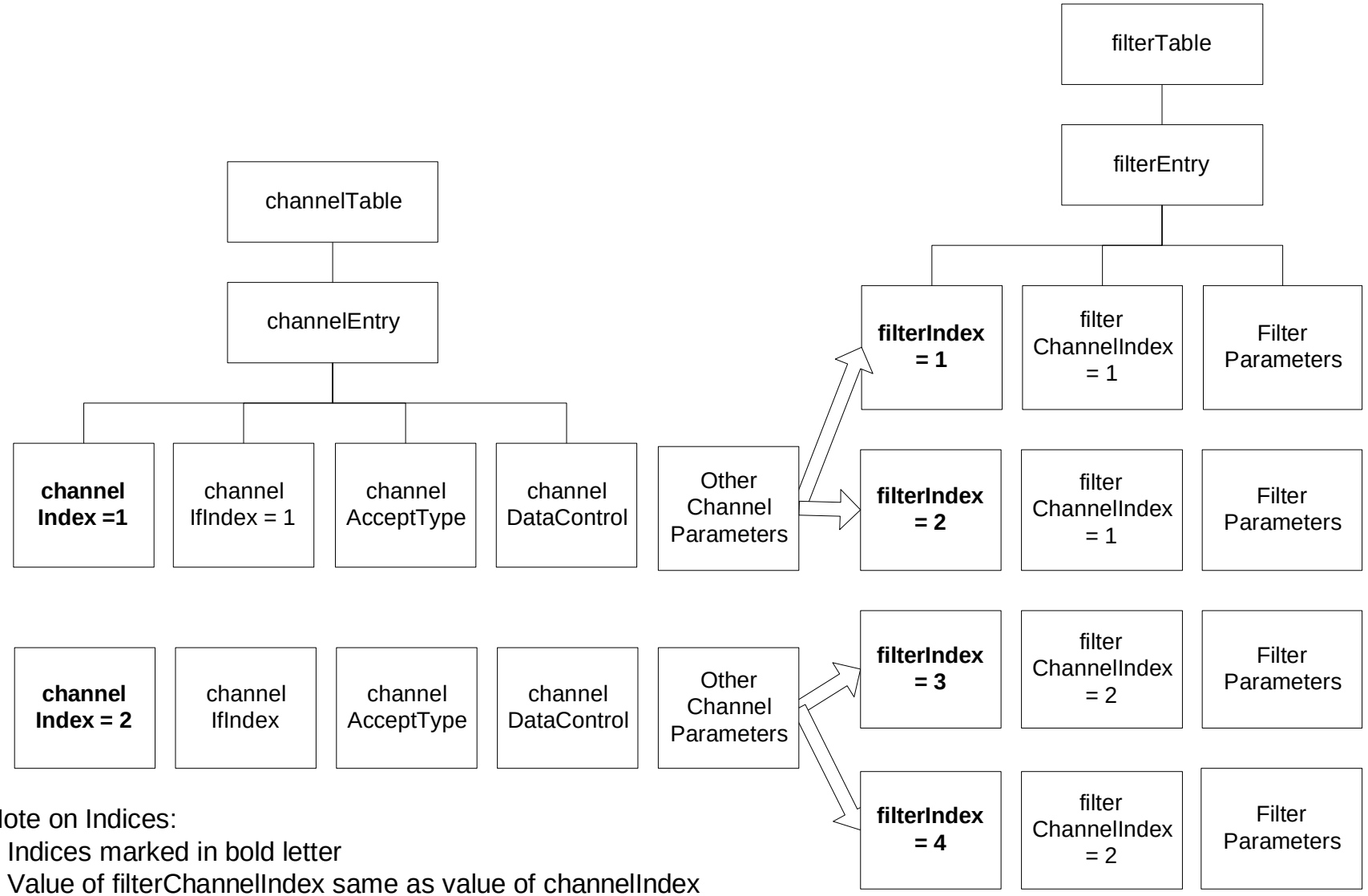
• Filter Group

- A channel is associated with

  filter1 OR filter2 OR … filter*n*

- Within a filter, any bits checked in the data and status are AND’ed with respect to other bits in the same filter.

• Filter Group

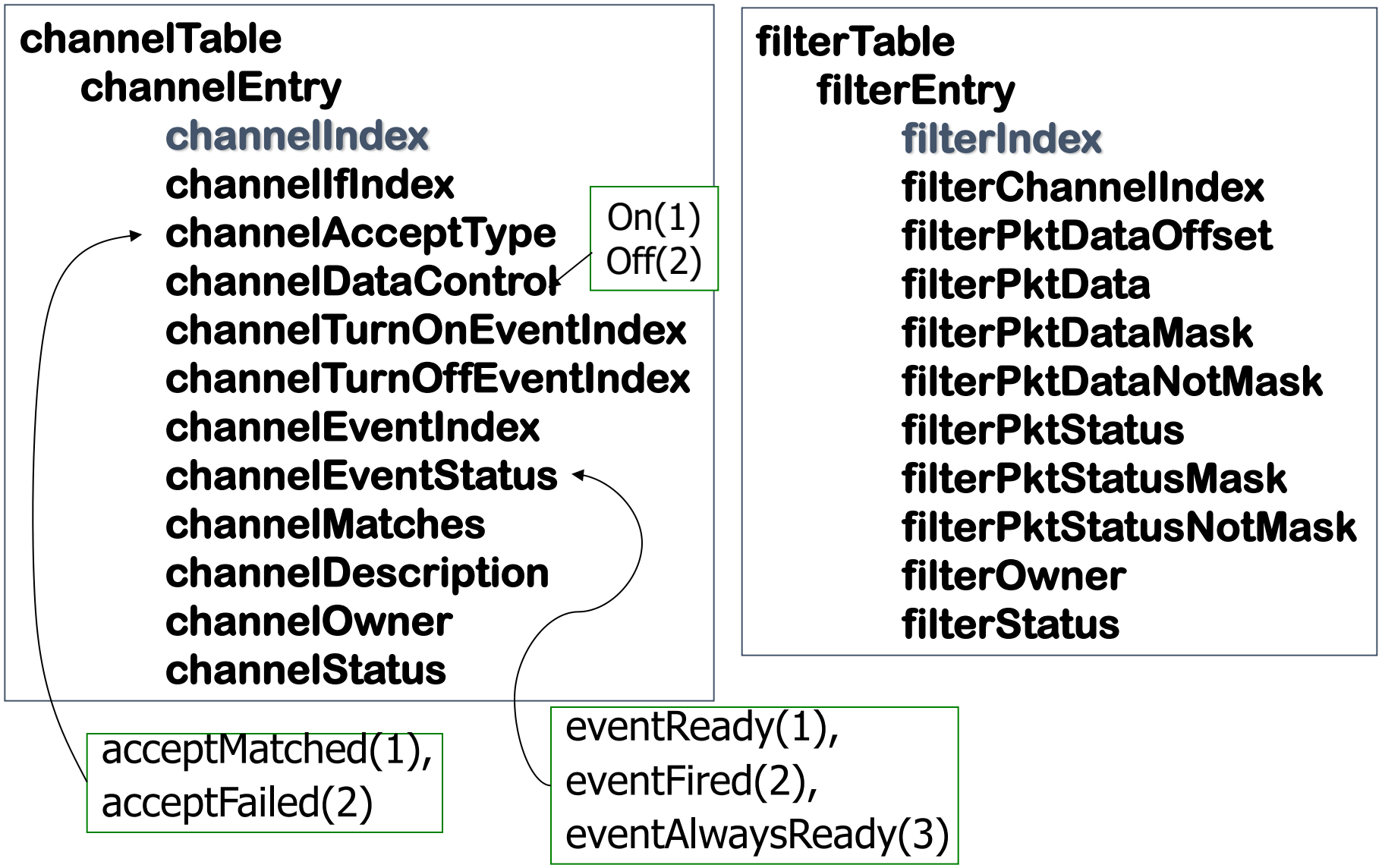


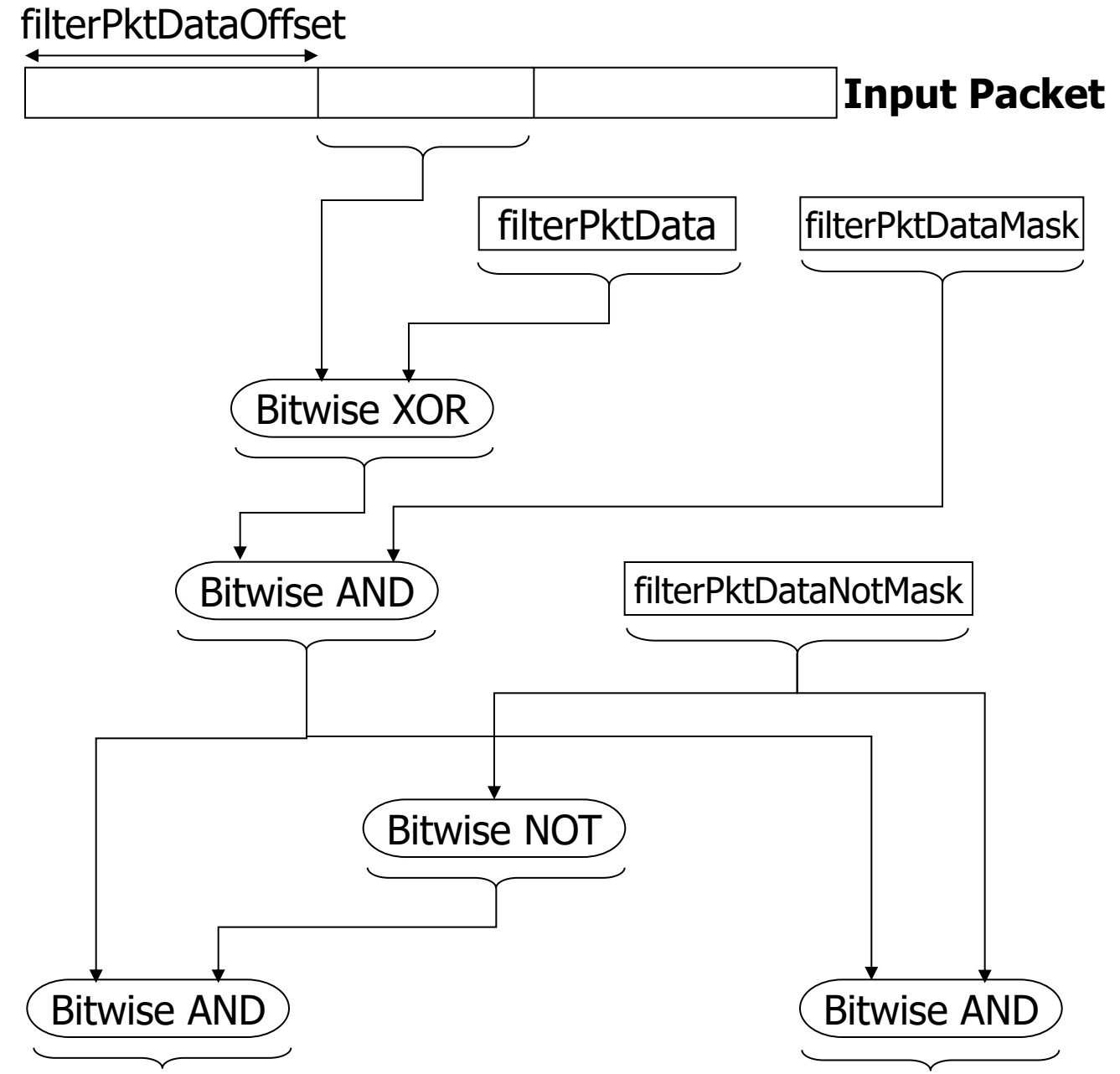
Note on Indices:

Indices marked in bold letter

Value of filterChannelIndex same as value of channelIndex

- **Filter**


channelTable
channelEntry
channelIndex
channelIfIndex
channelAcceptType
channelDataControl
channelTurnOnEventIndex
channelTurnOffEventIndex
channelEventIndex
channelEventStatus
channelMatches
channelDescription
channelOwner
channelStatus
On(1)
Off(2)
filterTable
filterEntry
filterIndex
filterChannelIndex
filterPktDataOffset
filterPktData
filterPktDataMask
filterPktDataNotMask
filterPktStatus
filterPktStatusMask
filterPktStatusNotMask
filterOwner
filterStatus
acceptMatched(1),
acceptFailed(2)
eventReady(1),
eventFired(2),
eventAlwaysReady(3)


filterPktDataOffset
Input Packet
filterPktData
filterPktDataMask
Bitwise XOR
Bitwise AND
filterPktDataNotMask
Bitwise NOT
Bitwise AND
Bitwise AND
Pass if all bits are 0
(pass if match)
Pass if any bits are 1
(pass if mismatch)

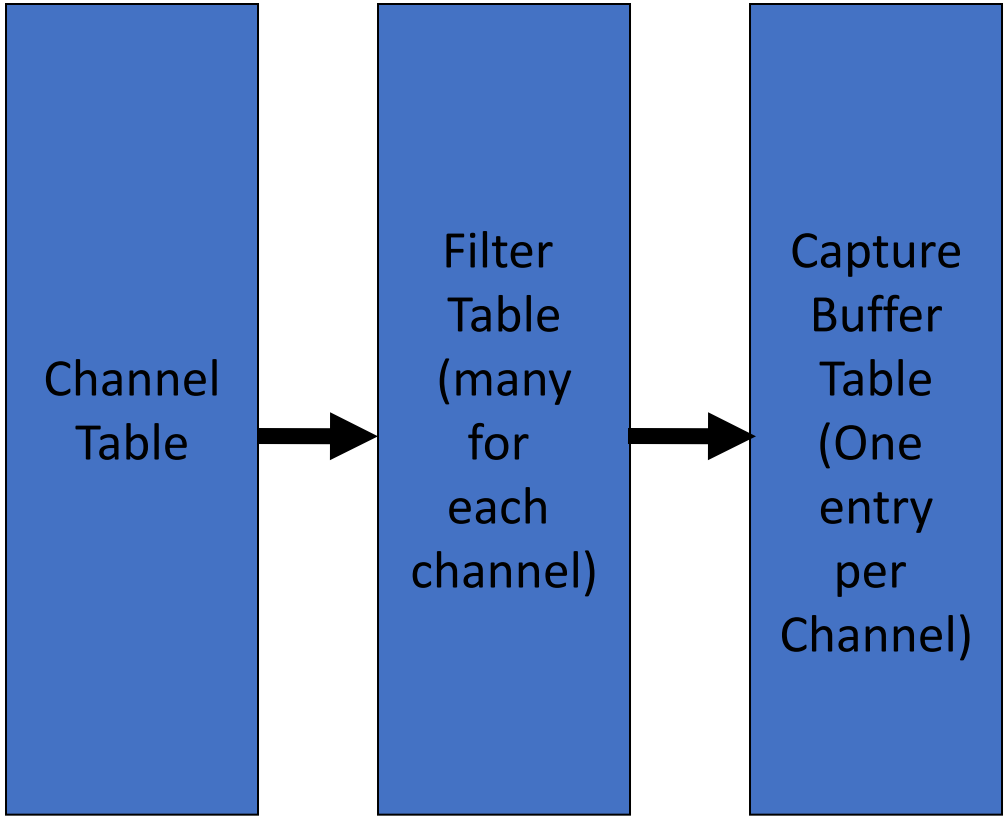
- **Filter Example**

```
filterPktDataOffset     =     0
filterPktData           =     0x000000000A50000000000BB
filterPktDataMask       =     0xFFFFFFFFFFFFFFFFFFFFFFF
filterPktDataNotMask    =     0x000000000000FFFFFFFFFFF
```

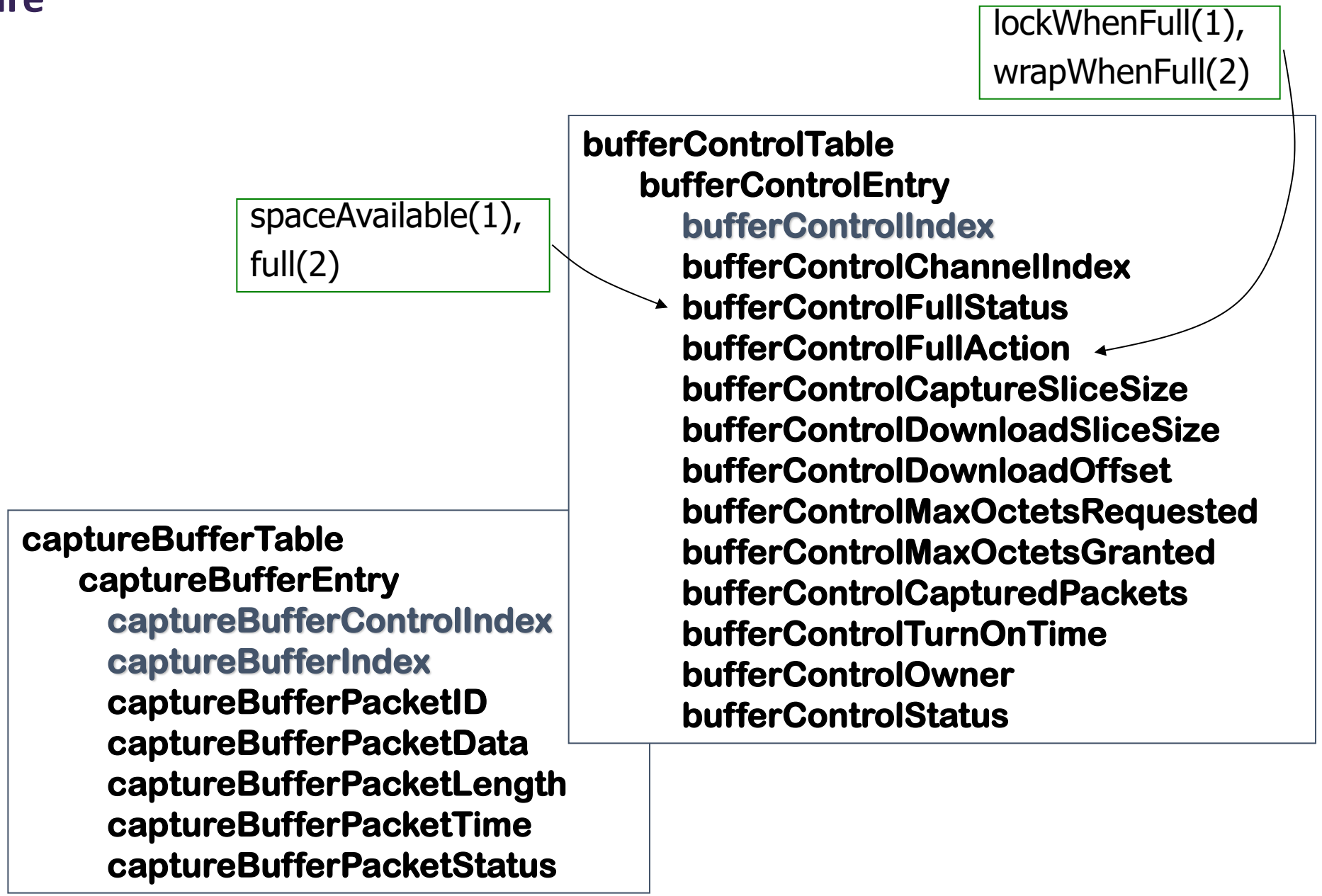
Accept all Ethernet packets that have a destination address of 0xA5 and that do not have a source address of 0xBB.

- **Capture Group**

rmon 8



- **Capture**


lockWhenFull(1),
wrapWhenFull(2)
spaceAvailable(1),
full(2)
bufferControlTable
bufferControlEntry
bufferControlIndex
bufferControlChannelIndex
bufferControlFullStatus
bufferControlFullAction
bufferControlCaptureSliceSize
bufferControlDownloadSliceSize
bufferControlDownloadOffset
bufferControlMaxOctetsRequested
bufferControlMaxOctetsGranted
bufferControlCapturedPackets
bufferControlTurnOnTime
bufferControlOwner
bufferControlStatus
captureBufferTable
captureBufferEntry
captureBufferControlIndex
captureBufferIndex
captureBufferPacketID
captureBufferPacketData
captureBufferPacketLength
captureBufferPacketTime
captureBufferPacketStatus

- **RMON TR Extension Groups**

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

- **RMON2**

- Applicable to Layers 3 and above
- Functions similar to RMON1
- Enhancement to RMON1
- Defined conformance and compliance

- **RMON 2 MIB**

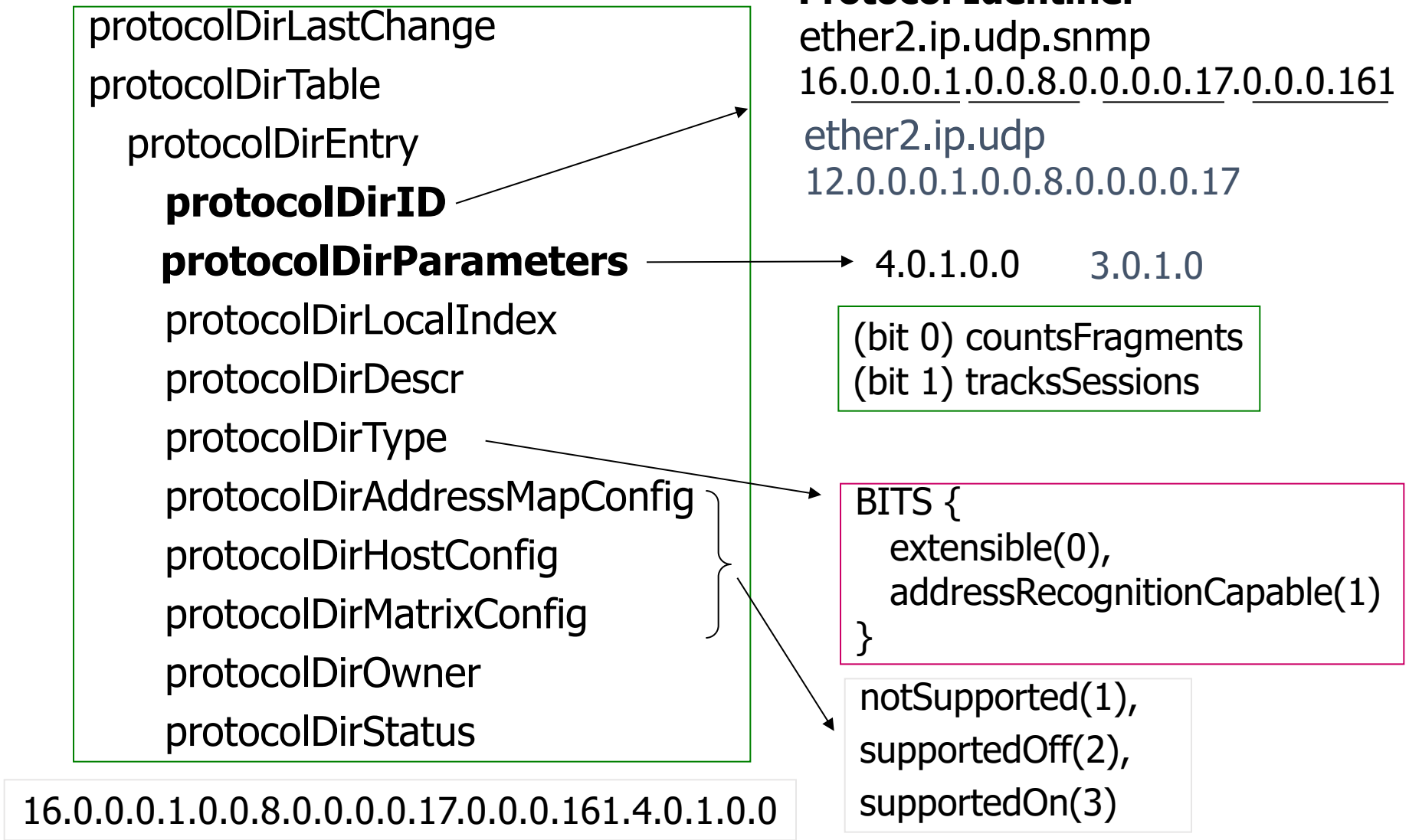
Group	OID	Function	Tables
Protocol Directory	rmon 11	Inventory of protocols	protocolDirTable
Protocol Distribution	rmon 12	Relative statistics on octets and packets	protocolDistControlTable protocolDistStatsTable
Address Map	rmon 13	Mac address to network address on the interfaces	addressMapControlTable 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

- **RMON 2 MIB**

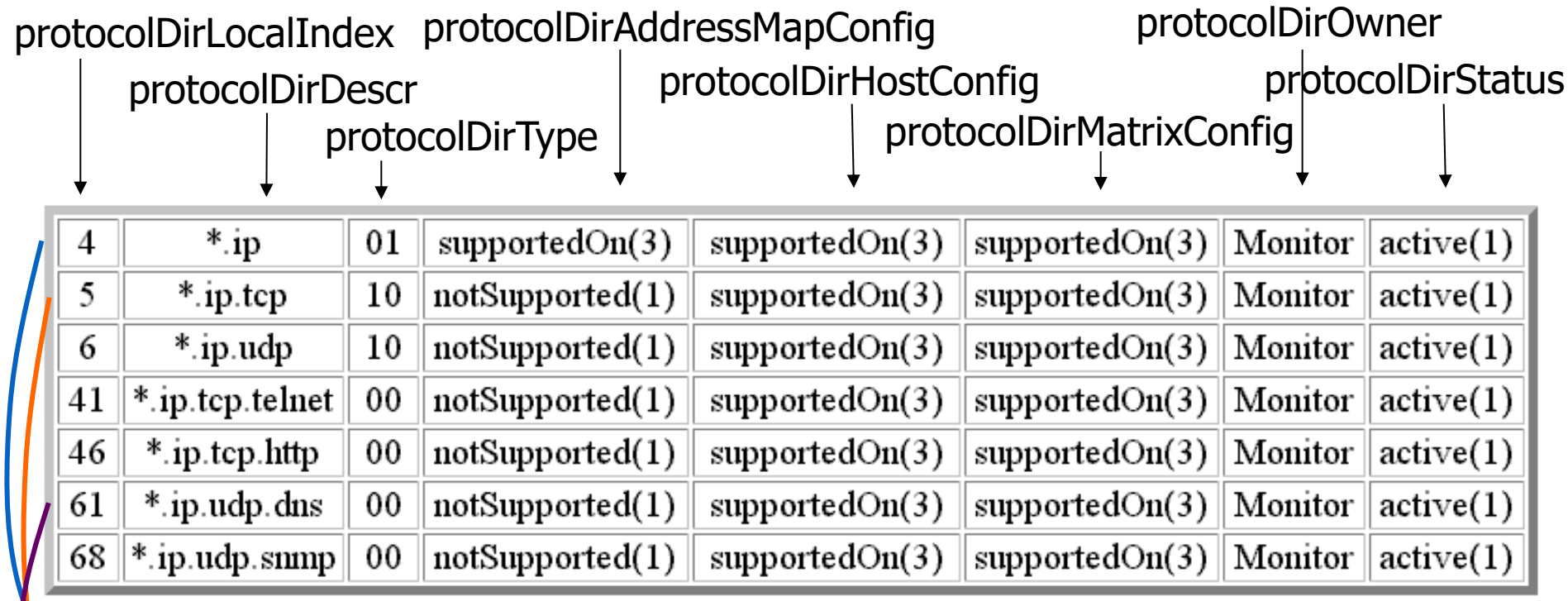
Application Layer Host	rmon 16	Traffic data by protocol from and to each host	a1HostTable
Application Layer Matrix	rmon 17	Traffic data by protocol between pairs of hosts	a1MatrixSDTable a1MatrixDSTable a1MatrixTopNControlTable a1MatrixTopNTable
User History Collection	rmon 18	User-specified historical 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

- **Protocol Directory**

rmon 11



- **protocolDirTable Example**



4	*.ip	01	supportedOn(3)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
5	*.ip.tcp	10	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
6	*.ip.udp	10	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
41	*.ip.tcp.telnet	00	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
46	*.ip.tcp.http	00	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
61	*.ip.udp.dns	00	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)
68	*.ip.udp.snmp	00	notSupported(1)	supportedOn(3)	supportedOn(3)	Monitor	active(1)

protocolDirLocalIndex.protocolDirID.protocolDirParameters

.1.3.6.1.2.1.16.11.2.1.3.8.1.0.0.1.0.0.8.0.2.0.0

.1.3.6.1.2.1.16.11.2.1.3.12.1.0.0.1.0.0.8.0.0.0.0.6.3.0.0.0

.1.3.6.1.2.1.16.11.2.1.3.16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.53.4.0.0.0.0

- **Protocol Distribution**

rmon 12

protocolDistControlTable
  protocolDistControlEntry
    protocolDistControlIndex
    protocolDistControlDataSource
    protocolDistControlDroppedFrames
    protocolDistControlCreateTime
    protocolDistControlOwner
    protocolDistControlStatus

Object Identifier	Value
1.3.6.1.2.1.16.12.1.1.2.1	1.3.6.1.2.1.2.2.1.1.1
1.3.6.1.2.1.16.12.1.1.3.1	0
1.3.6.1.2.1.16.12.1.1.4.1	0:00:03
1.3.6.1.2.1.16.12.1.1.5.1	monitor
1.3.6.1.2.1.16.12.1.1.6.1	1

protocolDistStatsTable
  protocolDistStatsEntry
    protocolDistStatsPkts
    protocolDistStatsOctets

Object Identifier	Value
1.3.6.1.2.1.16.12.2.1.1.1.4	132684185
1.3.6.1.2.1.16.12.2.1.2.1.4	3101564931

```
INDEX { protocolDistControlIndex,
        protocolDirLocalIndex }
```

protocolDistStatsTable

OID(protocolDistStatsPkts)	protocolDistStatsPkts	protocolDistStatsOctets
.1.3.6.1.2.1.16.12.2.1.1.1.4	152226584	2843228331
.1.3.6.1.2.1.16.12.2.1.1.1.5	30243806	1959274214
.1.3.6.1.2.1.16.12.2.1.1.1.6	120905544	790647401
.1.3.6.1.2.1.16.12.2.1.1.1.7	7996093	511820512
.1.3.6.1.2.1.16.12.2.1.1.1.8	2	140
.1.3.6.1.2.1.16.12.2.1.1.1.9	1	64
.1.3.6.1.2.1.16.12.2.1.1.1.10	1	70

	OID(protocolDistStatsPkts)	protocolDistStatsPkts	protocolDistStatsOctets
ip	.1.3.6.1.2.1.16.12.2.1.1.1.4	152226584	2843228331
*.ip.tcp	.1.3.6.1.2.1.16.12.2.1.1.1.5	30243806	1959274214
*.ip.tcp.telnet	.1.3.6.1.2.1.16.12.2.1.1.1.41	3847220	1373764210
*.ip.udp	.1.3.6.1.2.1.16.12.2.1.1.1.6	120905544	790647401
*.ip.udp.netbios	.1.3.6.1.2.1.16.12.2.1.1.1.66	2408006	581005950
*.ip.udp.rip	.1.3.6.1.2.1.16.12.2.1.1.1.73	989794	516661768
*.arp	.1.3.6.1.2.1.16.12.2.1.1.1.7	7996093	511820512
*.ip.tcp.ftp-data	.1.3.6.1.2.1.16.12.2.1.1.1.39	487171	492196391
*.ip.udp.snmp	.1.3.6.1.2.1.16.12.2.1.1.1.68	1694817	338336823

protocolDirLocalIndex

protocolDirDescr
(protocolDirTable)

Sorted by Octets

- **Address Map Group**

rmon 13

addressMapControlTable
  addressMapControlEntry
    addressMapControlIndex
    addressMapControlDataSource
    addressMapControlDroppedFrames
    addressMapControlOwner
    addressMapControlStatus

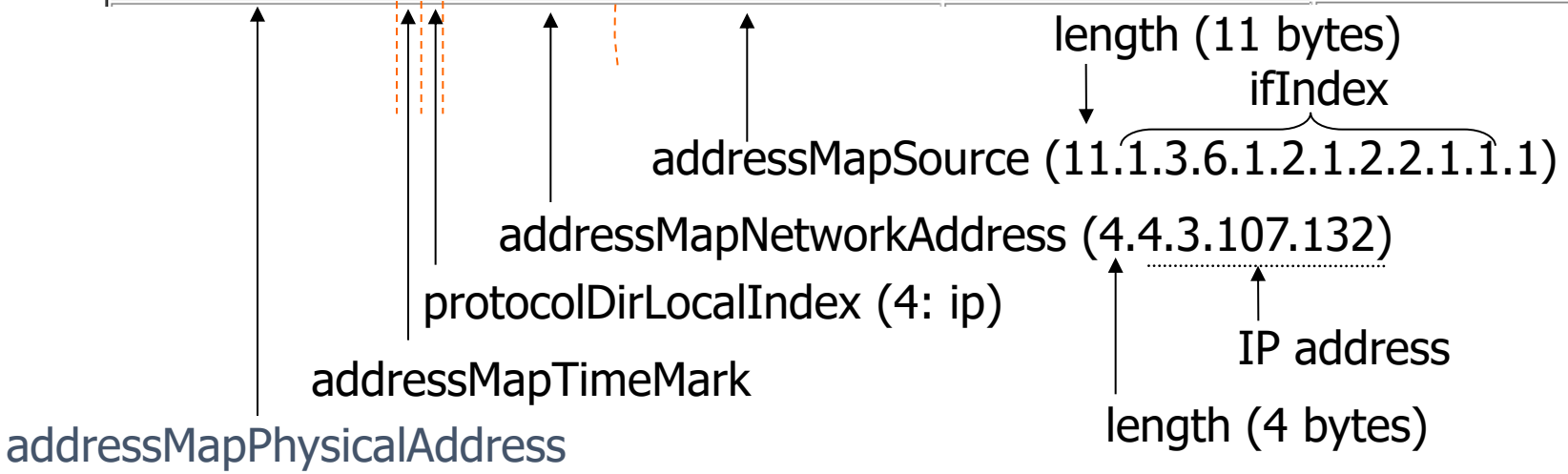
Object Identifier	Value
1.3.6.1.2.1.16.13.4.1.2.1	1.3.6.1.2.1.2.2.1.1.1
1.3.6.1.2.1.16.13.4.1.3.1	43764662
1.3.6.1.2.1.16.13.4.1.4.1	monitor
1.3.6.1.2.1.16.13.4.1.5.1	1

addressMapTable
  addressMapEntry
    addressMapTimeMark
    addressMapNetworkAddress
    addressMapSource
    addressMapPhysicalAddress
    addressMapLastChange

{ addressMapTimeMark, protocolDirLocalIndex, addressMapNetworkAddress, addressMapSource }

- **addressMapTable**

OID(addressMapPhysicalAddress)	addressMapPhysicalAddress	addressMapLastChange
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.0.0.0.0.11.1.3.6.1.2.1.2.2.1.1.1	00 0c 6e 8b 24 fc	88 days, 18 hours, 31 minutes, 46 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.1.128.12.3.11.1.3.6.1.2.1.2.2.1.1.1	a0 0f c0 60 08 3d	79 days, 12 hours, 45 minutes, 18 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.1.182.0.208.11.1.3.6.1.2.1.2.2.1.1.1	6a 87 65 d9 08 65	79 days, 11 hours, 31 minutes, 23 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.1.229.252.193.11.1.3.6.1.2.1.2.2.1.1.1	01 03 60 0f ef e6	79 days, 12 hours, 46 minutes, 55 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.3.87.16.6.11.1.3.6.1.2.1.2.2.1.1.1	cb 26 14 5b be a4	79 days, 11 hours, 20 minutes, 5 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.3.178.146.134.11.1.3.6.1.2.1.2.2.1.1.1	fe 7b 80 b2 ea 04	79 days, 12 hours, 13 minutes, 52 seconds.
.1.3.6.1.2.1.16.13.5.1.4.0.4.4.4.3.107.132.11.1.3.6.1.2.1.2.2.1.1.1	00 08 e3 dd b3 2b	75 days, 8 hours, 17 minutes, 16 seconds.



- **Network Layer Host Group**

hlHostControlTable

Object Identifier	Value
1.3.6.1.2.1.16.14.1.1.2.1	1.3.6.1.2.1.2.2.1.1.1
1.3.6.1.2.1.16.14.1.1.3.1	43862736
1.3.6.1.2.1.16.14.1.1.4.1	1260049
1.3.6.1.2.1.16.14.1.1.5.1	1254088
1.3.6.1.2.1.16.14.1.1.6.1	-1
1.3.6.1.2.1.16.14.1.1.7.1	44537366
1.3.6.1.2.1.16.14.1.1.8.1	2605477
1.3.6.1.2.1.16.14.1.1.9.1	2589365
1.3.6.1.2.1.16.14.1.1.10.1	-1
1.3.6.1.2.1.16.14.1.1.11.1	monitor
1.3.6.1.2.1.16.14.1.1.12.1	1

hlHostControlTable
- hlHostControlEntry
  - hlHostControlIndex
  - hlHostControlDataSource
  - hlHostControlNlDroppedFrames
  - hlHostControlNlInserts
  - hlHostControlNlDeletes
  - hlHostControlNlMaxDesiredEntries
  - hlHostControlAlDroppedFrames
  - hlHostControlAlInserts
  - hlHostControlAlDeletes
  - hlHostControlAlMaxDesiredEntries
  - hlHostControlOwner
  - hlHostControlStatus

hl, nl, al means higher layer, network layer, and application layer

- **Network Layer Host Table**

rmon 14 2

nlHostTable
- nlHostEntry
  - nlHostTimeMark
  - nlHostAddress
  - nlHostInPkts
  - nlHostOutPkts
  - nlHostInOctets
  - nlHostOutOctets
  - nlHostOutMacNonUnicastPkts
  - nlHostCreateTime

INDEX { hlHostControlIndex, nlHostTimeMark, protocolDirLocalIndex, nlHostAddress }

```
nlHostOutPkts.1.783495.18.4.128.2.6.6.
```

- **Network Layer Matrix Group**

rmon 15

rmon 15 1

Object Identifier	Value
1.3.6.1.2.1.16.15.1.1.2.1	1.3.6.1.2.1.2.2.1.1.1
1.3.6.1.2.1.16.15.1.1.3.1	44585985
1.3.6.1.2.1.16.15.1.1.4.1	1297186
1.3.6.1.2.1.16.15.1.1.5.1	1280047
1.3.6.1.2.1.16.15.1.1.6.1	-1
1.3.6.1.2.1.16.15.1.1.7.1	44636481
1.3.6.1.2.1.16.15.1.1.8.1	2733462
1.3.6.1.2.1.16.15.1.1.9.1	2689097
1.3.6.1.2.1.16.15.1.1.10.1	-1
1.3.6.1.2.1.16.15.1.1.11.1	monitor
1.3.6.1.2.1.16.15.1.1.12.1	1

hlMatrixControlTable
hlMatrixControlEntry
hlMatrixControlIndex
hlMatrixControlDataSource
hlMatrixControlNlDroppedFrames
hlMatrixControlNlInserts
hlMatrixControlNlDeletes
hlMatrixControlNlMaxDesiredEntries
hlMatrixControlAlDroppedFrames
hlMatrixControlAlInserts
hlMatrixControlAlDeletes
hlMatrixControlAlMaxDesiredEntries
hlMatrixControlOwner
hlMatrixControlStatus

- **Network-Layer Source/Destination Statistics**

rmon 15 2

nlMatrixSDTable
- nlMatrixSDEntry
  - nlMatrixSDTimeMark
  - nlMatrixSDSourceAddress
  - nlMatrixSDDestAddress
  - nlMatrixSDPkts
  - nlMatrixSDOctets
  - nlMatrixSDCreateTime

INDEX { hlMatrixControlIndex, nlMatrixSDTimeMark, protocolDirLocalIndex, nlMatrixSDSourceAddress, nlMatrixSDDestAddress }

rmon 15 3

nlMatrixDSTable
- nlMatrixDSEntry
  - nlMatrixDSTimeMark
  - nlMatrixDSSourceAddress
  - nlMatrixDSDestAddress
  - nlMatrixDSPkts
  - nlMatrixDSOctets
  - nlMatrixDSCreateTime

INDEX { hlMatrixControlIndex, nlMatrixDSTimeMark, protocolDirLocalIndex, nlMatrixDSDestAddress, nlMatrixDSSourceAddress }

```
nlMatrixSDPkts.1.783495.18.4.128.2.6.6.4
                    128.2.6.7
```

- **nlMatrixSDTable**

OID(nlMatrixSDPkts)	nlMatrixSDPkts	nlMatrixSDOctets	nlMatrixSDCreate
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.0.0.0.0.4.255.255.255.255	3273	1174059	61 days, 13 hours, 4 minutes, 36 seconds
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.4.4.56.51.4.163.22.22.63	1	64	84 days, 2 hours, 33 minutes, 14 seconds
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.4.4.61.29.4.163.22.22.196	1	66	82 days, 8 hours, 27 minutes, 36 seconds
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.10.10.29.220.4.163.22.22.43	1361	156706	82 days, 23 hours, 1 minutes, 48 seconds
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.10.10.30.35.4.163.22.22.40	105	8743	69 days, 15 hours, 0 minutes, 28 seconds
.1.3.6.1.2.1.16.15.2.1.4.1.0.4.4.10.10.30.35.4.163.22.22.43	105	8743	69 days, 15 hours, 0 minutes, 28 seconds

nlMatrixSDPkts

nlMatrixSDDestAddress

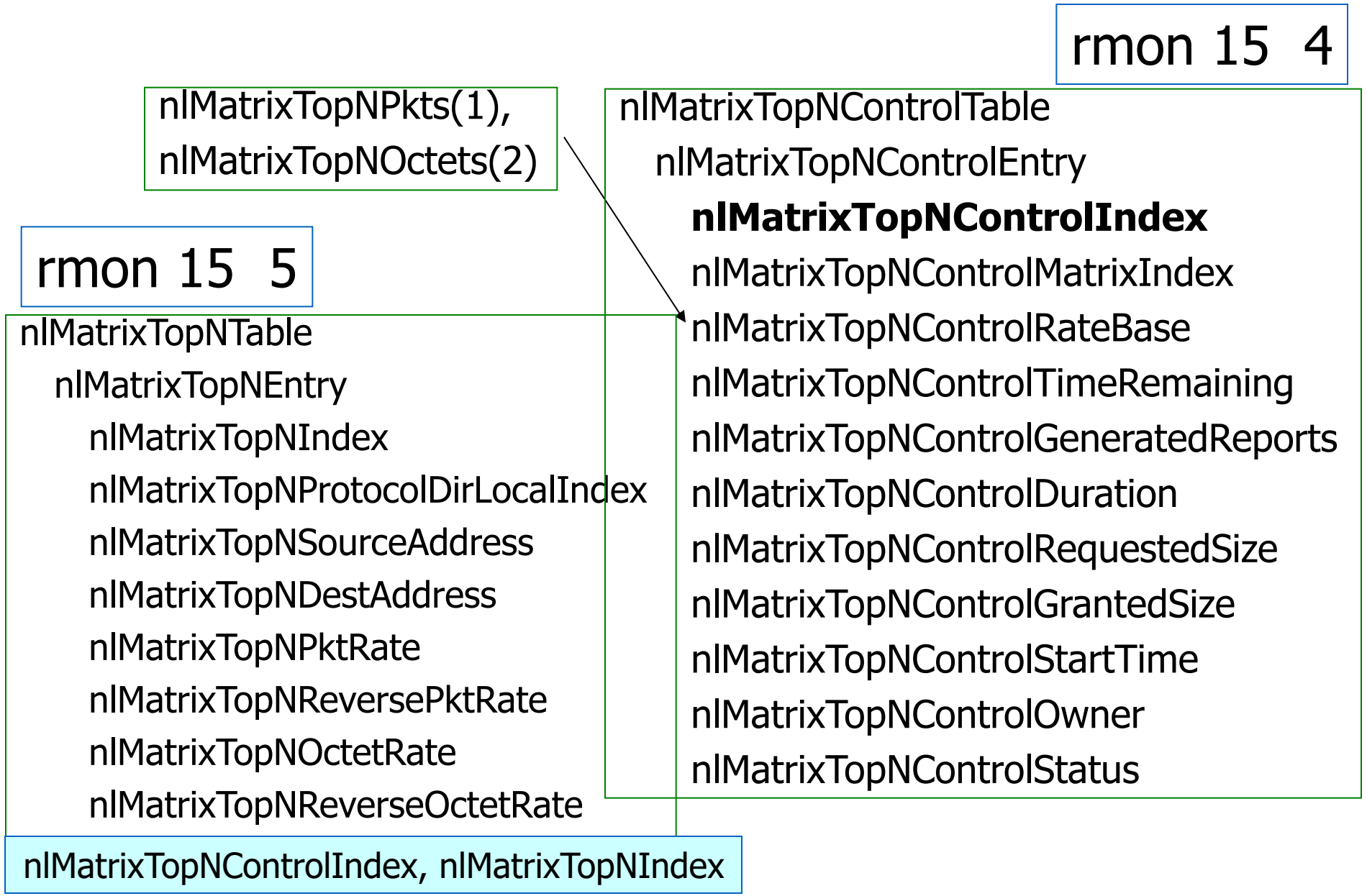
nlMatrixSDSourceAddress

protocolDirLocalIndex (ip)

nlMatrixSDTimeMark

hlMatrixControlIndex

- **Network-Layer Top N Matrix**



- **Application-Layer Host Group**

rmon 16

rmon 16 1

alHostTable
- alHostEntry
  - alHostTimeMark
  - alHostInPkts
  - alHostOutPkts
  - alHostInOctets
  - alHostOutOctets
  - alHostCreateTime

*.ip

INDEX { hlHostControlIndex, alHostTimeMark, protocolDirLocalIndex,
nlHostAddress, protocolDirLocalIndex }

*.ip.tcp.http

- **alHostTable**

OID(alHostInPkts)	alHostInPkts	alHostOutPk	alHostInOct	alHostOutOct	alHostCreateTime
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.4	854	1652	66115	137243	62 days, 0 hours, 7 minutes, 28 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.5	592	705	46124	56107	62 days, 0 hours, 7 minutes, 58 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.6	0	195	0	18720	62 days, 0 hours, 7 minutes, 59 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.16	262	752	19991	62416	62 days, 0 hours, 7 minutes, 28 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.46	202	315	20396	30367	62 days, 0 hours, 8 minutes, 3 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.52	195	195	12864	12870	62 days, 0 hours, 7 minutes, 58 seconds.
.1.3.6.1.2.1.16.16.1.1.2.1.0.4.4.10.10.26.186.65	0	195	0	18720	62 days, 0 hours, 7 minutes, 59 seconds.

①②③ ④ ⑤

①: hlHostControlIndex ②: alHostTimeMark ③: protocolDirLocalIndex,
④: nlHostAddress ⑤:protocolDirLocalIndex

- **Application Layer Matrix Group**

rmon 17

rmon 17 1

alMatrixSDTable
alMatrixSDEntry
alMatrixSDTimeMark
alMatrixSDPkts
alMatrixSDOctets
alMatrixSDCreateTime

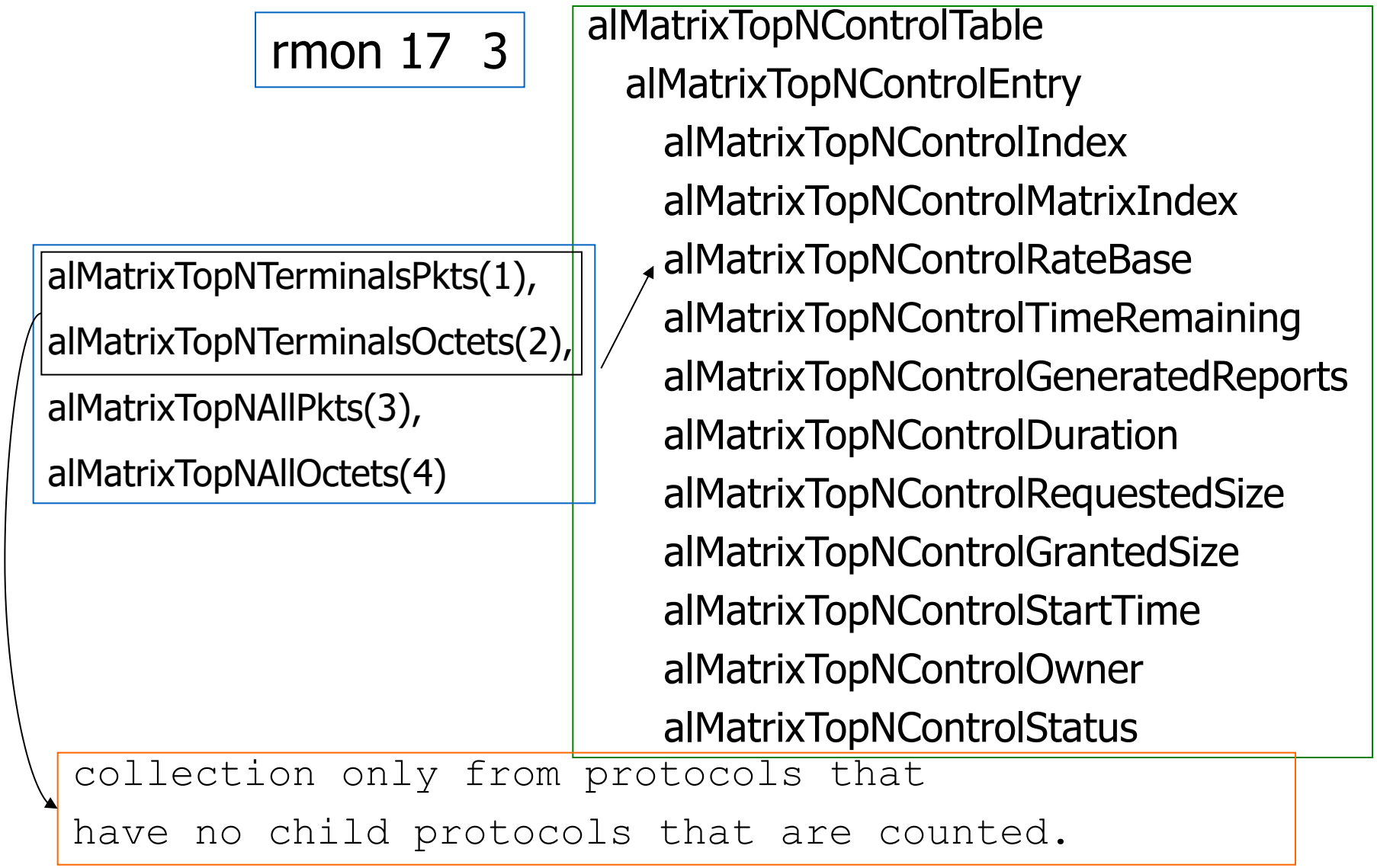
rmon 17 2

alMatrixDSTable
alMatrixDSEntry
alMatrixDSTimeMark
alMatrixDSPkts
alMatrixDSOctets
alMatrixDSCreateTime

INDEX { hlMatrixControlIndex, alMatrixSDTimeMark, protocolDirLocalIndex,
nlMatrixSDSourceAddress, nlMatrixSDDestAddress, protocolDirLocalIndex }

INDEX { hlMatrixControlIndex, alMatrixDSTimeMark, protocolDirLocalIndex,
nlMatrixDSDestAddress, nlMatrixDSSourceAddress, protocolDirLocalIndex }

- **Application-Layer Top N Matrix**



- **alMatrixTopNTable**

rmon 17 4

alMatrixTopNTable
- alMatrixTopNEntry
  - alMatrixTopNIndex
  - alMatrixTopNProtocolDirLocalIndex
  - alMatrixTopNSourceAddress
  - alMatrixTopNDestAddress
  - alMatrixTopNAppProtocolDirLocalIndex
  - alMatrixTopNPktRate
  - alMatrixTopNReversePktRate
  - alMatrixTopNOctetRate
  - alMatrixTopNReverseOctetRate

INDEX { alMatrixTopNControlIndex, alMatrixTopNIndex }

- **User History Collection Group**

rmon 18

rmon 18 1

usrHistoryControlTable
- usrHistoryControlEntry
  - usrHistoryControlIndex
  - usrHistoryControlObjects
  - usrHistoryControlBucketsRequested
  - usrHistoryControlBucketsGranted
  - usrHistoryControlInterval
  - usrHistoryControlOwner
  - usrHistoryControlStatus

rmon 18 2

usrHistoryObjectTable
- usrHistoryObjectEntry
  - usrHistoryObjectIndex
  - usrHistoryObjectVariable
  - usrHistoryObjectSampleType

absoluteValue(1),
deltaValue(2)

INDEX { usrHistoryControlIndex, usrHistoryObjectIndex }

- **User History Table**

rmon 18 3

usrHistoryTable
  usrHistoryEntry
    usrHistorySampleIndex
    usrHistoryIntervalStart
    usrHistoryIntervalEnd
    usrHistoryAbsValue
    usrHistoryValStatus

valueNotAvailable(1),
valuePositive(2),
valueNegative(3)

INDEX { usrHistoryControlIndex, usrHistorySampleIndex,
        usrHistoryObjectIndex }

• A Case Study

- 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)

• A 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%

• A Case Study Results

Traffic Pattern

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%.