Performance Management

- **Performance Management Overview**
- **Network Monitoring**
- **RMON**
- **RMON II**

Performance Management

- Choosing the performance metrics to monitor is difficult
  - Too many to choose from
  - Difficult to understand their significance
  - Vary from vendor to vendor -- standards are important
  - Difficult to interpret
  - Time consuming
- Can’t monitor everything - must determine what is critical
- Some performance metrics of interest:
  - Availability
  - Response Time
  - Accuracy
  - Throughput
  - Utilization
  - Traffic levels

Availability

- Availability: amount of time a resource or collection of resources if available to users expressed as a percentage
- A = MTBF/(MTBF + MTTR)
  - MTBF = Mean Time Between Failures
  - MTTR = Mean Time To Repair
  - Availability of the network or system as a whole is based on the availability of the individual components
    - The more redundancy that is built in the more available the system will be
    - But, there is a trade-off between redundancy and cost
    - Calculating the availability becomes more difficult as the complexity of the network or system increases

Response Time

- Response Time: the time it takes for a network or system component to respond to a request
  - There is a tradeoff between short response times and cost
    - Faster processors cost more
    - Prioritizing some tasks over others makes the “other” tasks slower
    - Goal is to achieve the shortest response times possible within the given budget constraints
  - Measuring response time
    - Inbound terminal delay
    - Inbound queuing time
    - Inbound service time
    - Processor delay
    - Outbound queuing time
    - Outbound service time
    - Outbound terminal delay

Accuracy and Throughput

- Accuracy: the transmission of data that is free of errors
  - Modern devices have built-in error correction so this is normally not a big concern
  - It is useful to monitor the number of errors being corrected so the cause can be identified and fixed
- Throughput: the number of transactions over a period of time
  - Useful for determining projected demand
  - Useful for detecting bottlenecks and other problem areas

Utilization

- Utilization: percentage of time that a resource is in use
  - ActiveTime/TotalTime * 100
  - Used to determine resources that are both over- and under-utilized
  - Look at differences between planned and actual loads on each link in the network
    - Some links may be carrying less than their share of the load and other more than their share
    - Loads may be able to be shifted to make the network operate more efficiently

Performance Management

- Performance management includes
  - Measurement
    - Agents residing in devices
    - Remote monitors (RMON) for shared networks
  - Analysis
    - Humans
    - Software tools
  - Control – ability to make changes based on performance measurement and analysis
- Keys to performance monitoring
  - Determining what is important to monitor
  - Accurately interpreting the results

Network Monitoring

Network Monitoring is a major aspect of Network Management

If we can't monitor it:

- we don't know what is going on
- we can't fix it when something goes wrong!

So how do we monitor the network effectively?

Distributed Monitoring

The only way to effectively monitor the entire network is with a distributed monitoring architecture.

A distributed architecture includes monitoring devices deployed across the network at strategic points.

These devices may report back to a centralized NMS via polling, events or both.

Monitoring Devices

- Remote Monitoring Devices are usually referred to as *probes*
- They may be:
  - Dedicated devices
  - Embedded agents - e.g. switch probe
  - Client-based agents

Monitoring Approaches

Monitoring takes two major forms:

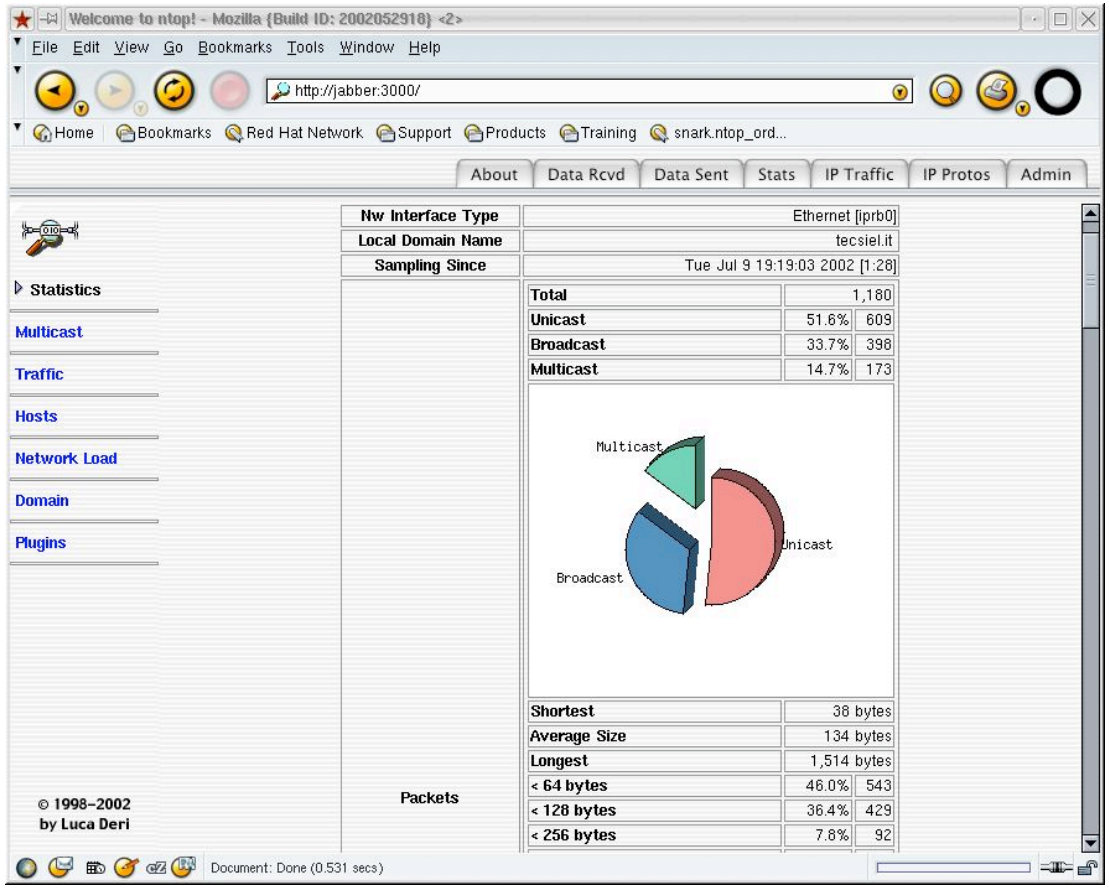
- Passive Monitors
  - No traffic is generated
  - Probe observes traffic in “promiscuous” mode
  - Behavior is analyzed, reported back to NMS
- Active Monitors
  - Targeted test traffic is generated
  - Performance of tests is measured (e.g. ping times)

Passive Monitors

- General Traffic Monitors
  - Packet captures, sniffers
  - RMON probes
- Specific Applications
  - Embedded in client software
  - Observe client requests such as TCP connections or Web requests

Passive Examples

- Cisco NetFlow
- ntop
  http://www.ntop.org/ntop.html
- RMON
- Cyclades-nQuirer
  http://www.cyclades.com/products/29/nquirer/application_notes/19



Passive Application Monitors

Passive monitors on the client host

Watch user interactions with applications and record response time and availability.

- NETI@home - http://www.neti.gatech.edu/
- FirstSense - http://www.concord.com/

Active Monitors

- Active, synthetic tests
  - Send real traffic between *test devices* on client and server networks
  - Good test of the network, not of the actual service
- Active, real tests
  - Send “real” requests to the *production* servers
  - Test both the network and the service

Active Synthetic

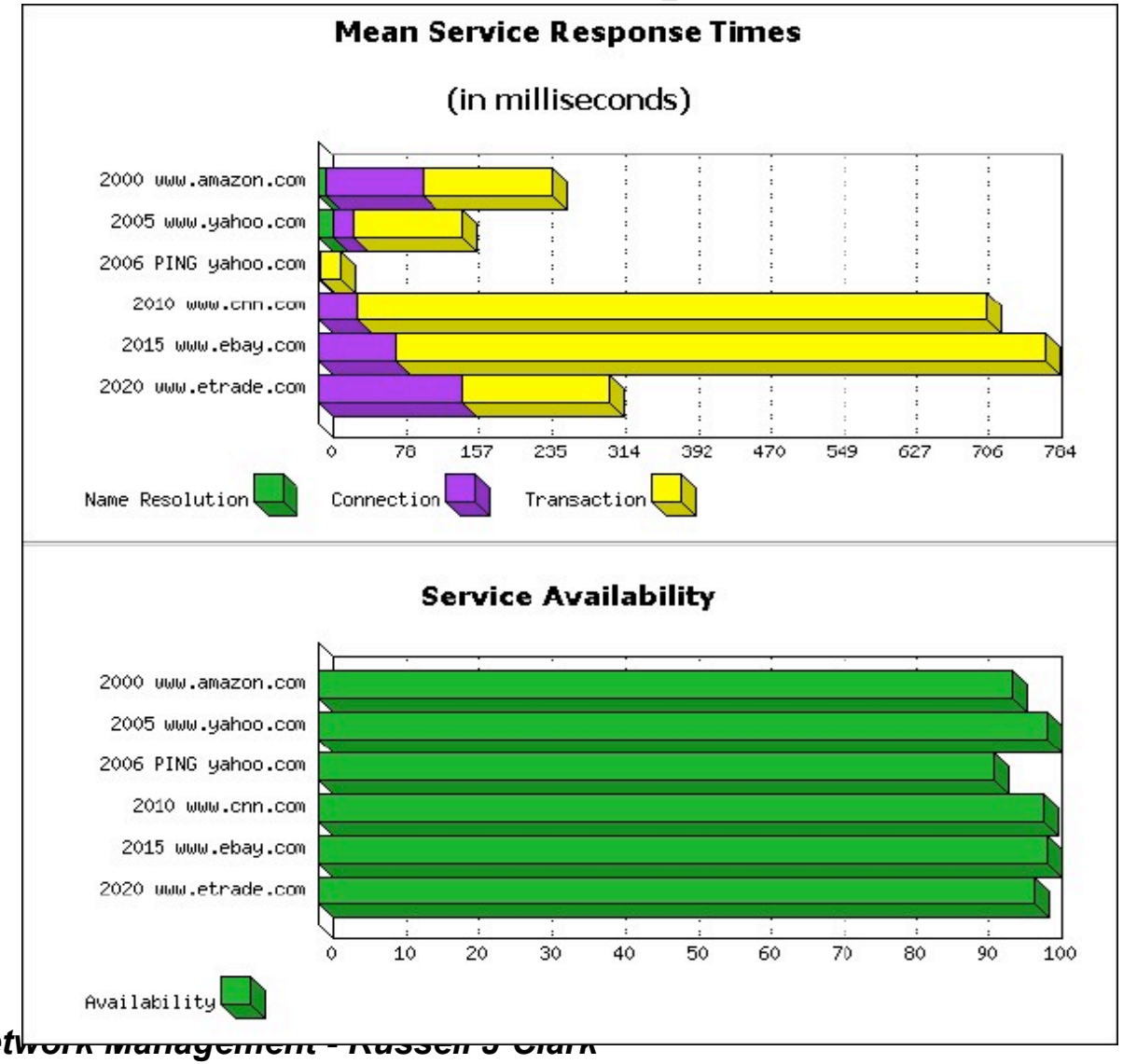
- Common Command Line Tools
  - Ping, traceroute
  - Iperf http://dast.nlanr.net/Projects/Iperf/

- Chariot from NetIQ
  - http://www.netiq.com/products/chr/default.asp

Active Real Example

Service Response from Concord

http://www.concord.com



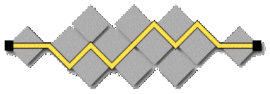
BREAK

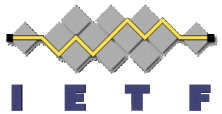
RMON Overview

- Remote MONitoring (RMON): allows remote monitoring and analyzing of network segment traffic
  - A significant enhancement to MIB-II
    - Provides information related to traffic on the network segment as a whole versus information on individual devices as provided by MIB-2
    - Specified as a separate SNMP MIB
  - An RMON agent is known as a probe
    - One per LAN segment
    - Can be a standalone probe or be imbedded in another device (e.g., hub, server, etc.)
    - Sends information back to the management station
  - Works in promiscuous mode: sees every packet sent on the segment
- RMON 1 focuses on OSI layers 1 and 2

RMON Standards

RFC		Title
1513	P	Token Ring Extensions to the Remote Network Monitoring MIB
2819	S	Remote Network Monitoring Management Information Base
2021		Remote Network Monitoring MIB Version 2 using SMIv2
2074	P	Remote Network Monitoring MIB Protocol Identifiers
2613	P	Remote Network Monitoring MIB Extensions for Switch Networks Version 1
2895		Remote Network Monitoring MIB Protocol Identifier Reference
2896		Remote Network Monitoring MIB Protocol Identifier Macros
3144		Remote Monitoring MIB Extensions for Interface Parameters Monitoring





RFC 1757

RMON Goals

- **Offline Operation**: the RMON probe is designed to collect network statistics regardless of whether it is connected to the management station or not
- **Proactive Monitoring**: this allows the probe to continuously run diagnostics (provided it has enough resources), to log the information for future reference, and notify the management station concerning any problems
- **Problem Detection and Reporting**: the probe can be configured to continuously check for certain problems - it can both log the problem and notify the manager
- **Value Added Data**: provides valuable information that could only be obtained by a device dedicated to network management on a particular segment
- **Multiple Managers**: can support more than one manager

RMON Terminology

- RMON Agent
- RMON Probe
- RMON MIB

RMON Probe = RMON Agent

Analogous to SNMP Agent

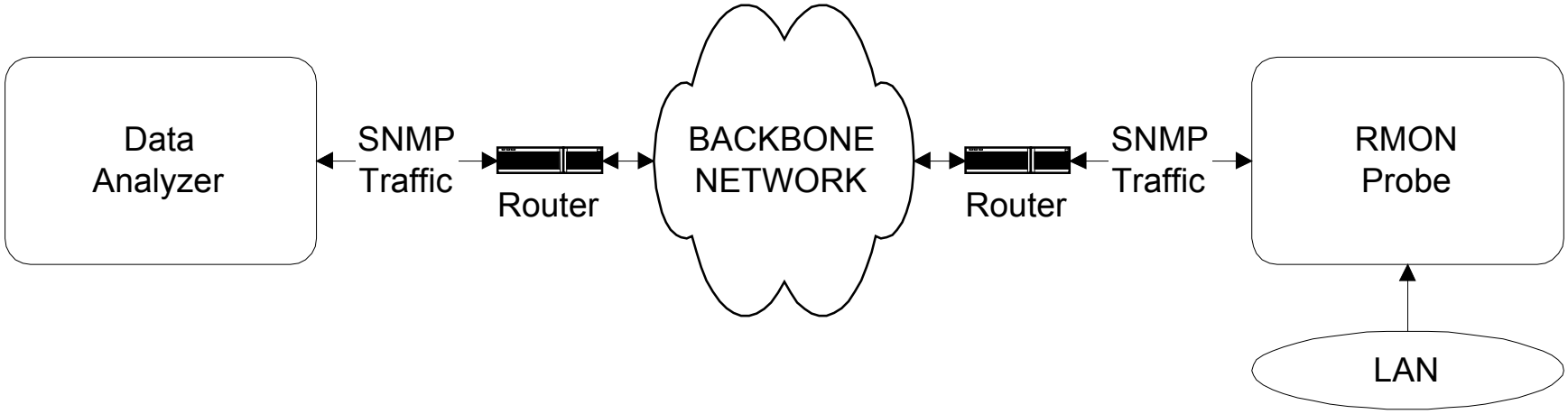
RMON Services

- RMON is an important extension to “basic” MIB-II
  - Provides a mechanism to monitor *traffic* on a subnetwork as opposed to *devices* on a subnetwork
- Based on the idea of a remote monitor
  - Gathers statistical / historical information, relays to the NMS
- Monitor *could* be a dedicated device
  - Or a router, switch, or general purpose host
- Functions provided are similar to LAN analysis devices

What does a Remote Monitor do?

- Watch a LAN as a whole
- Gather information without polling and adding traffic
- Track the traffic flows that contribute the most to the network activity
- Detect failures hard to find by polling.
- Find duplicate IP address assignments
- Can be configured to watch for signs of troubles (because it is "intelligent": processor and memory resources)
- Can be configured to send trap message when an error counter passes over a set threshold

RMON Components



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

RMON Components

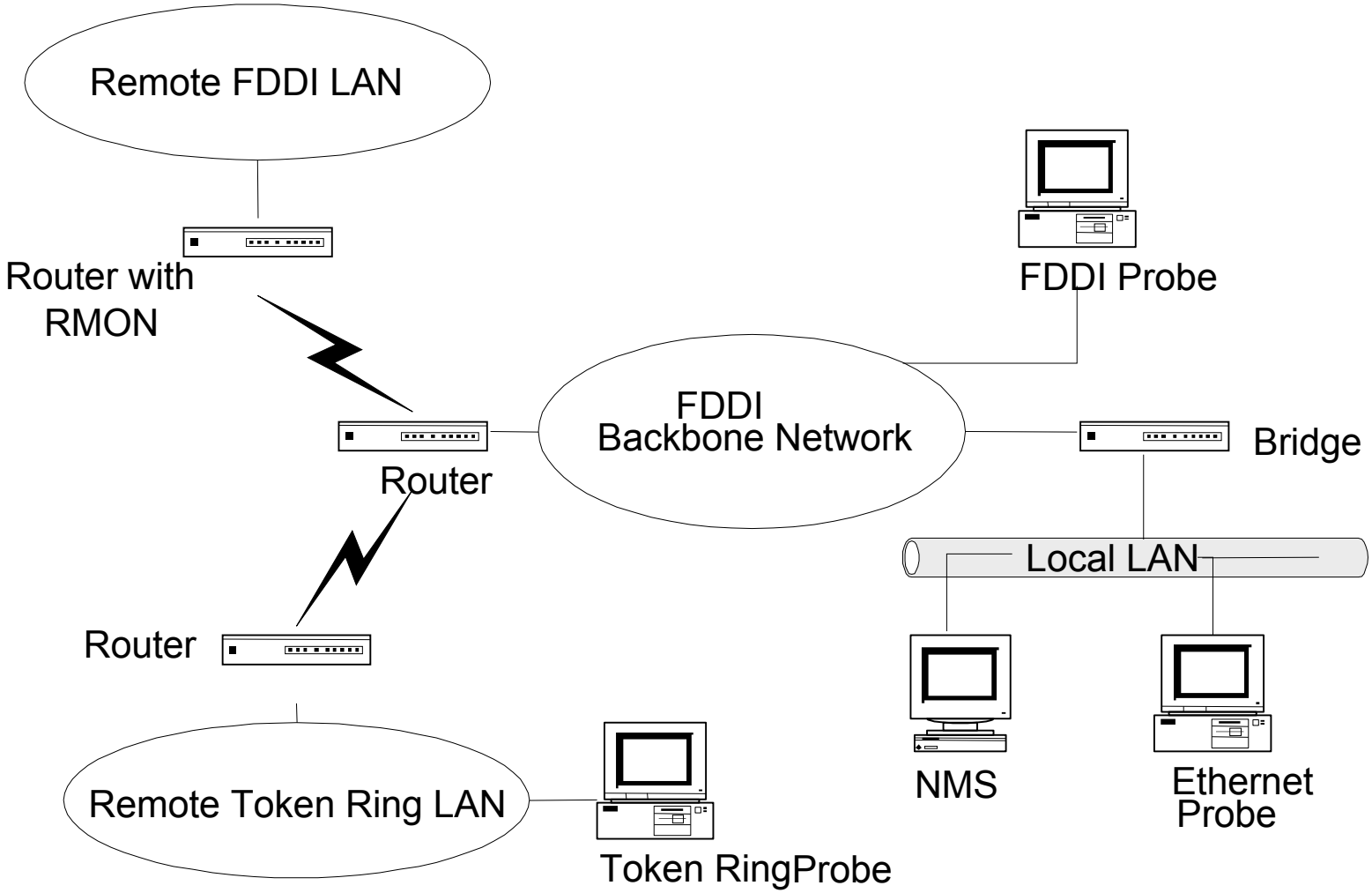


Figure 8.1 Network Configuration with RMONs
Network Management - Russell J Clark

With RMON you can . . .

- Configure the type and form of data to be collected
- Explicitly control actions by the probe
- Control a probe from multiple managers
- Safely modify data tables in the probe

Two Key RMON Features

- Configuration - all but basic statistical counters must be explicitly configured by the manager
  - Control Tables (RW)
    - Source of data to be collected
    - Type of Data
    - Collection interval
  - Data Tables (R-O)
    - Collected Data
- Action Invocation
  - SNMP Set operation
    - Some RMON MIB objects represent states
    - Setting these MIB objects may change the state a managed element

Table Management

For the Control Tables, settable via SNMP, we have to establish some rules

- Textual Conventions
- Row Status Column
- Row Addition
- Row Modification & Deletion

Table Management

Textual Conventions

- `OwnerString ::= DisplayString`
- `EntryStatus ::= INTEGER {  valid (1),`
  `createRequest(2),`
  `underCreation(3),`
  `invalid(4)  }`

Table Management

Control Tables

- rm1ControlIndex
- rm1ControlParameter
- rm1ControlOwner
- rm1ControlStatus

Table Management

Row Addition

- Uses SNMPv2 Row Addition technique
  - SNMP SetRequest PDU with variable bindings = OIDs and instance values for index (indices) of the table (min) or ideally, all columnar objects in the table.
- *RMON Polka* prevents two managers from simultaneously requesting similar row values

Dealing with Multiple Managers

- Potential problems when multiple managers are responsible for managing the same devices
  - One manager may undo the changes made by another manager
  - Two or more managers may try to access the same probe at the same time
  - One manager could tie up the probe's resources for long periods so that other managers are not able to make other necessary changes
- How RMON deals with multiple managers
  - Each control table identifies the owner of each particular function in the control table
    - Ownership information should include, according to the RMON specification, one or more of the following: IP address, management station name, network manager's name, location, and phone number
    - Other managers can still change parameters "owned" by another manager but shouldn't without coordinating with them

Table Management

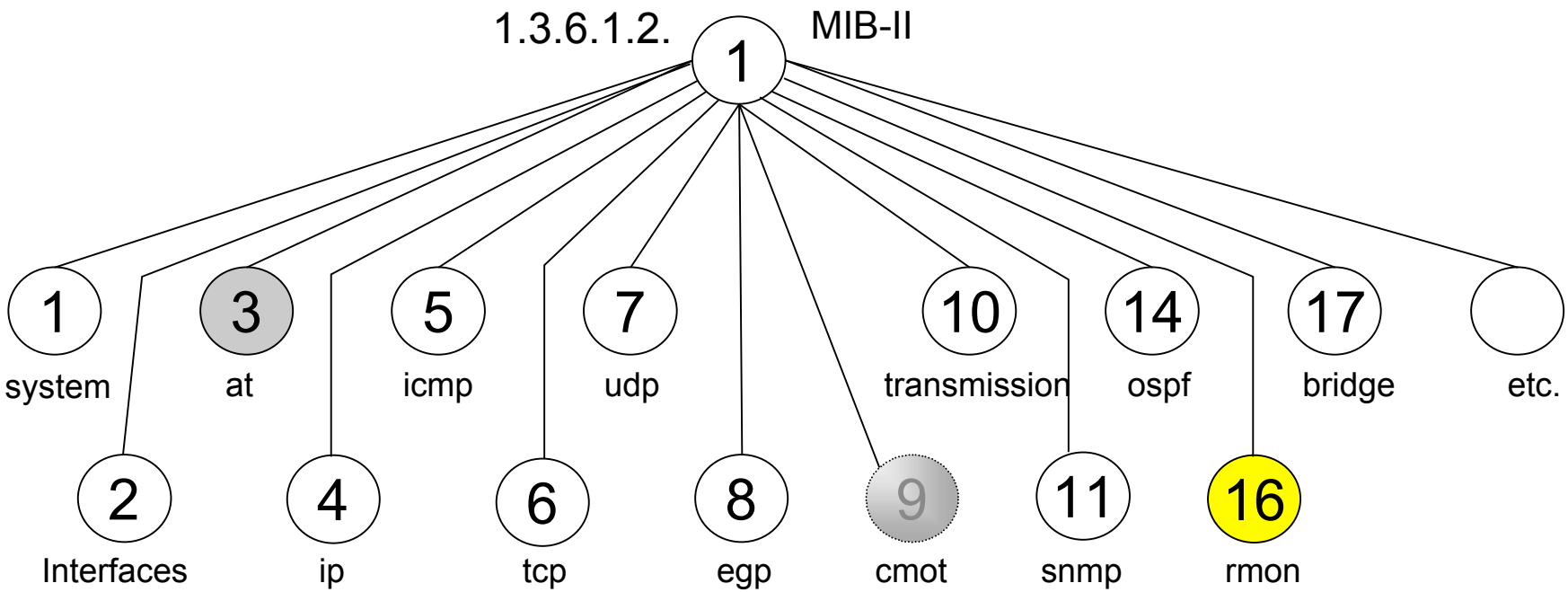
Row Modification and Deletion

SetRequest PDU

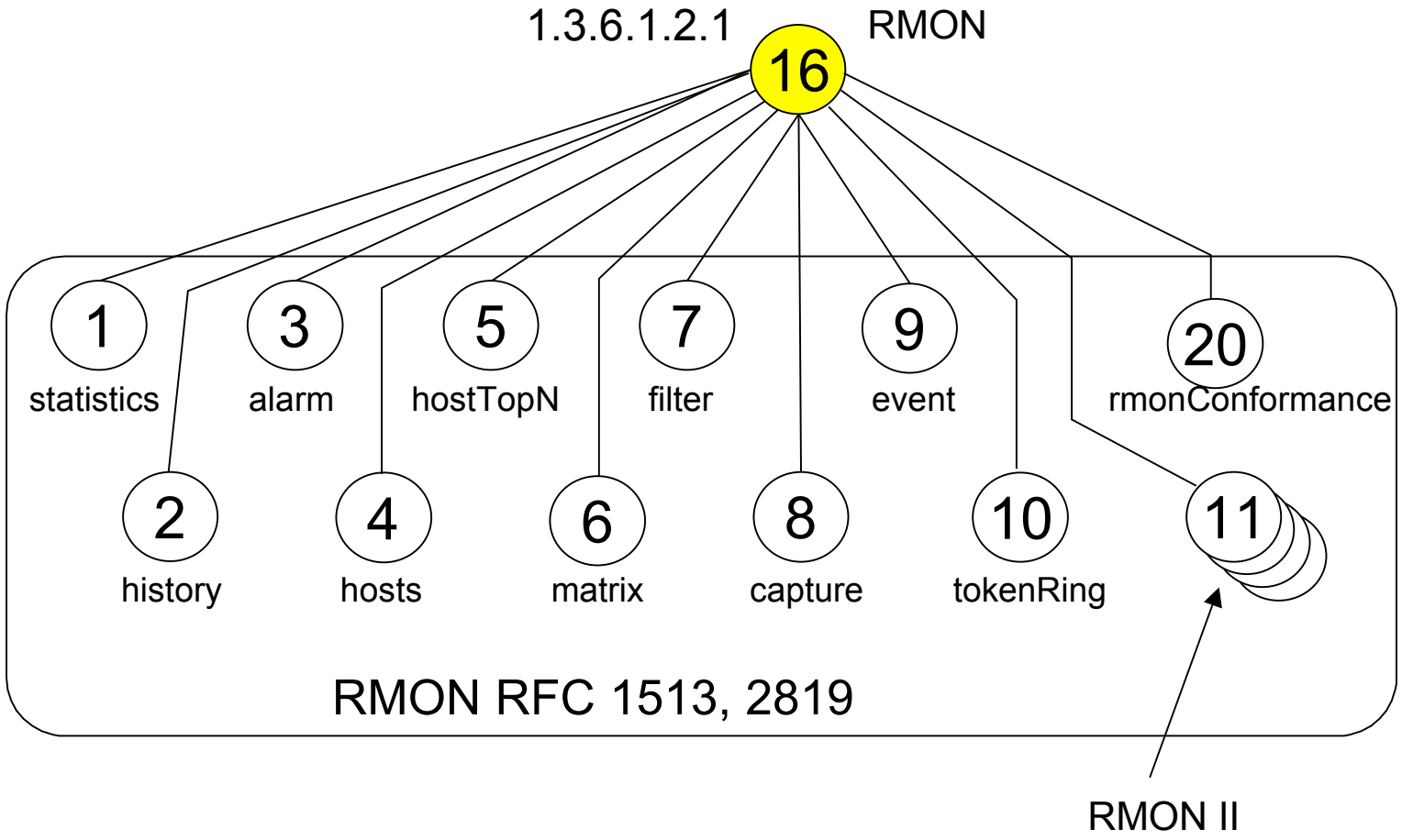
- Set status object for that row to invalid
- Manager is restricted to changing the state of an entry in the following ways:

From	To	valid	createRequest	underCreation	invalid
valid		N/A	NO	YES	YES
createRequest		N/A	N/A	N/A	N/A
underCreation		YES	NO	N/A	YES
invalid		NO	NO	NO	N/A
nonExistent		NO	YES	NO	N/A

The RMON MIB


1.3.6.1.2.
MIB-II
1
1
system
2
Interfaces
3
at
4
ip
5
icmp
6
tcp
7
udp
8
egp
9
cmot
10
transmission
11
snmp
14
ospf
16
rmon
17
bridge
etc.

The RMON MIB


1.3.6.1.2.1
RMON
16
1
statistics
2
history
3
alarm
4
hosts
5
hostTopN
6
matrix
7
filter
8
capture
9
event
10
tokenRing
11
20
rmonConformance
RMON RFC 1513, 2819
RMON II

RMON MIB

1.3.6.1.2.16.

1. **Statistics**: contains statistics (in the form of counters) for each interface on the device being monitored by the probe
   - Collects information on errors and collisions
   - Similar to MIB-2 interfaces plus more detail and packet size distributions
2. **History**: contains historical samples of statistics and allows setup of the sampling process
3. **Alarm**: allows comparisons between statistical samples and defined thresholds - a message is sent for each threshold exceeded
4. **Hosts**: keeps an inventory of hosts connected to the subnetwork by compiling a list of source and destination MAC addresses the probe sees in packets transmitted over the LAN segment

RMON MIB

1.3.6.1.2.16.

5. **hostTopN**: contains a list of hosts with the highest values for a particular statistic
6. **matrix**: a matrix which contains information on transmissions between pairs of hosts on the subnetwork
7. **filter**: allows the probe to match packets based on a filter equation
8. **packetCapture**: allows the probe capture packets that match a filter
   - Captures length of packet, time of capture, and error status
   - This group is optional but if you choose to implement it you must also implement the filter group
9. **event**: allows control of the generation and forwarding of events from the probe

RMON MIB

1.3.6.1.2.16.

10. tokenRing:

- Defined in RFC 1513
- Used for managing 802.5 token ring networks
- Most original RMON groups apply all types of subnetworks including token ring
- The token ring adds new tables to the statistics and history groups since the counters in these groups are specific to each subnetwork type

Two Key RMON Groups

- Alarms
  - Set a sampling interval and an alarm threshold
  - For any MIB object of type
    - COUNTER
    - GAUGE
    - TIMETICKS
    - INTEGER
- Events
  - Table of events to report (such as alarms)
  - Can be triggered by a condition elsewhere in the MIB
  - Can trigger an action defined elsewhere in the MIB

Alarm Group

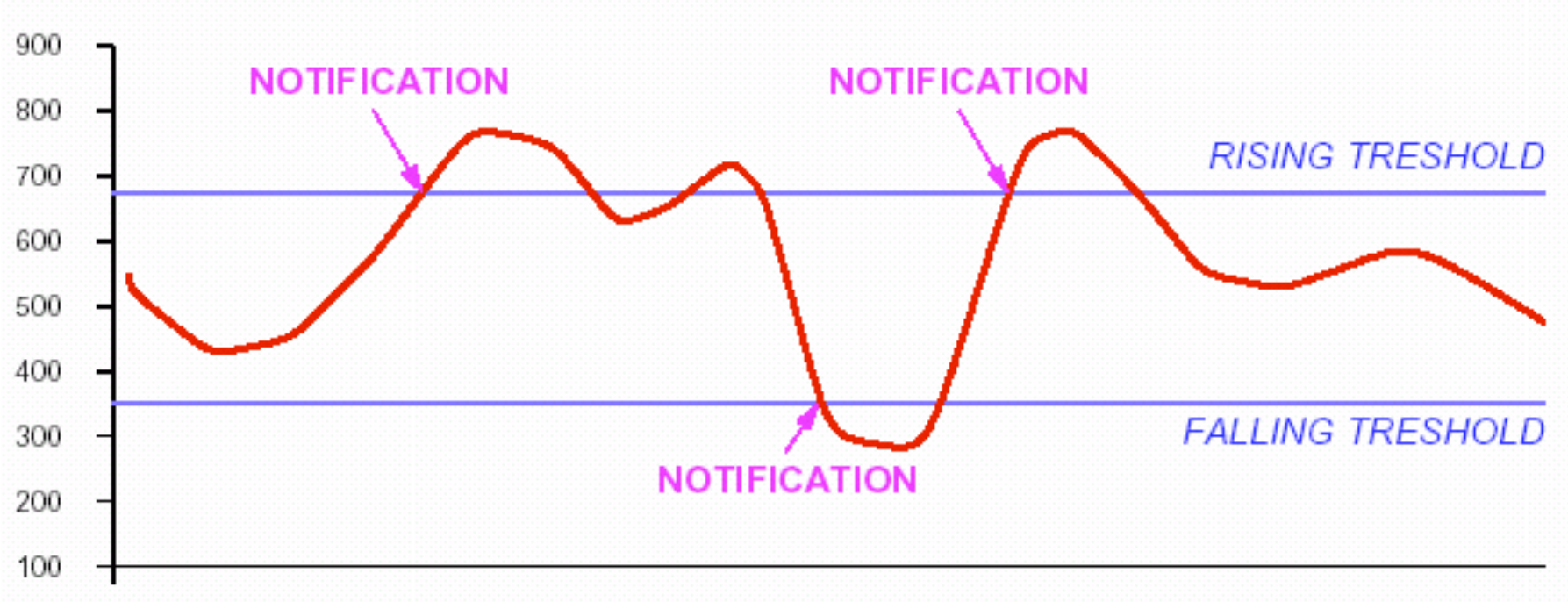
1.3.6.1.2.16.3

.1 alarmTable

- .1 alarmEntry
  - .1 alarmIndex
  - .2 alarmInterval
  - .3 alarmVariable
  - .4 alarmSampleType
  - .5 alarmValue
  - .6 alarmStartupAlarm
  - .7 alarmRisingThreshold
  - .8 alarmFallingThreshold
  - .9 alarmRisingEventIndex
  - .10 alarmFallingEventIndex
  - .11 alarmOwner
  - .12 alarmStatus

Alarm Group

1.3.6.1.2.16.3



Event Group

1.3.6.1.2.16.9

.1 eventTable
- .1 eventEntry
  - .1 eventIndex
  - .2 eventDescription
  - .3 eventType
  - .4 eventCommunity
  - .5 eventLastTimeSent
  - .6 eventOwner
  - .7 eventStatus

.2 logTable
- .1 logEntry
  - .1 logEventIndex
  - .2 logIndex
  - .3 logTime
  - .4 logDescription

RMON 2 Overview

- Addresses packets operating in OSI layers 3 - 7
- Can look beyond a particular LAN segment
  - Network Layer protocols such as IP (traffic to and from a LAN via routers)
    - Looks at the IP header to determine source and destination
      - Can see where excessive external (to the LAN) traffic is coming from
      - Can see if a particular host or group of hosts is causing excessive traffic leaving the LAN through a router
      - Can see if there is a lot of pass-through traffic (i.e., in through one router and out through another)
    - Very helpful for improving performance since the network manager is able to see more of the "big picture"
  - Application Layer protocols such as email and web traffic
    - Can show traffic percentages for each protocol used by a particular application
    - "Application" (in RMON 2) includes any protocol above the network layer (layer 3)

RMON 2 MIB Extensions

1.3.6.1.2.16.

- An extension of the original RMON MIB
- Groups added by RMON 2:

1.3.6.1.2.1.16.

- 11. protocol directory (protocolDir)
- 12. protocol distribution (protocolDist)
- 13. address map (addressMap)
- 14. network-layer host (nlHost)
- 15. network-layer matrix (alHost)
- 16. application-layer host (alMatrix)
- 17. application-layer matrix (alMatrix)
- 18. user history collection (usrHistory)
- 19. probe configuration (probeConfig)

RMON 2 MIB

1.3.6.1.2.16.

11. **Protocol directory (protocolDir)**: the directory that contains all the protocols the probe can support
    - Contains information on each supported protocol so the management station is aware of which protocols the probe is capable of handling
    - Helps managers deal with the numerous protocols that exist at the various network layers
12. **Protocol distribution (protocolDist)**: provides a summary of the # of octets and packets have been sent by each supported protocol

RMON 2 MIB

1.3.6.1.2.16.

13. **Address map (addressMap)**: maps each network (e.g., IP) address to a MAC-level address associated with a specific port on the device
    - Used for node discovery and for determining network traffic paths
    - Can also detect duplicate IP addresses
14. **Network-layer host (nlHost)**: allows packets to be decoded based on network layer address
    - Contains statistics on traffic into and out of each host based on network-layer address
    - Statistics include error-free packets and octets transmitted to and from the address in question

RMON 2 MIB

1.3.6.1.2.16.

15. **Network-layer matrix (nlMatrix)**: traffic statistics for pairs of hosts by network layer address
    - Statistics related to transmissions from one source network layer address to a destination and vice versa (similar to RMON matrix group)
    - Information related to the most active pairs of hosts for a particular statistic (similar to RMON hostTopN group)
    - RMON 2 bases this information on network layer (IP) address rather than MAC address (RMON 1)
16. **Application-layer host (alHost)**: statistics related to the amount of traffic into and out of hosts by application-layer address

RMON 2 MIB

1.3.6.1.2.16.

17. **application-layer matrix (alMatrix)**: traffic statistics for pairs of hosts by application layer address
    - Statistics related to transmissions from one host to another
    - Application layer information related to the most active pairs of hosts for a particular statistic
18. **user history collection (usrHistory)**: Periodically polls and logs statistics based on user defined parameters
    - Data that can be collected is not limited to predefined statistics as is the case with RMON 1
    - Can look at historical data for any counter in the system
19. **probe configuration (probeConfig)**: defines a standard set of configuration parameters for RMON probes -- improves interoperability between managers and probes

RMON Considerations

- An RMON probe can run on any of the following
  - Dedicated computer workstation
  - Non-dedicated server or management station
  - Non-dedicated network device such as a router, hub, or switch
- Which hardware option is selected depends on
  - Size of the subnetwork
  - Complexity of the subnetwork
  - The reliability/survivability requirements of the probe
- Interoperability issues
  - Multi-vendor RMON environments are difficult to configure and maintain
  - Single vendor environments normally do not have significant interoperability problems but in today's environment it is rare to find this

RMON Considerations

- RMON is very powerful but has limitations
  - Need to be careful not to collect too much data using RMON which can overload the probe, the network segment, the internet connection, and/or the management station
  - One way to lessen this problem is to install software on the monitor that allows the data collected by the probe to be analyzed before it is sent to the management station
    - Requires more processing power for the device the probe and the additional software resides on
    - Requires less bandwidth than sending all the raw data to the management station for analysis there
  - Filters can be an effective way to minimize the number of packet captured by the probe but there are tradeoffs here as well
    - Can limit the data collected which lessens some resource concerns, but
    - If the filters are complicated or there are a lot of filters defined it can cause the platform supporting the probe to become overloaded

RMON Considerations

- RMON can monitor non-snmp enabled devices
- RMON can produce a network inventory without enabling SNMP on every device
- RMON probe requirement for processing power and memory

RMON Future

- Switch Monitoring (SMON) is defined in RFC 2613 and addresses remote monitoring of switch interfaces
  - Many vendors are implementing RMON on switch ports but there are some limitations and tradeoffs
    - It is difficult to identify ports on the switch and to map them to physical addresses especially with modular switches
    - Switch backbone connections are normally full-duplex (two separate transmit and receive connections) and RMON was designed for shared media networks
  - Uses 64 bit counters instead of 32 bit counters which is helpful for VLANs with many high-speed interfaces
- High Capacity RMON (HCRMON): defines 64 bit counters and gauges for RMON 1 and 2 to handle high speed network technologies such as Gigabit Ethernet

RMON Summary

- RMON 1
  - Focuses on layers 1 and 2
  - Allows network managers to remotely gather statistics from subnetworks
  - Allows managers to define how statistics are collected, analyzed, and retrieved
  - RMON is also useful for performing inventories of network equipment especially ones that are not SNMP manageable
- RMON 2
  - Provides more detailed information than RMON 1
    - Focuses on layers 3 through 7 (above the MAC layer)
    - Must track many more protocols than RMON 1 so it more complicated and resource intensive
    - Normally runs on a dedicated high-end workstation due to resources required
  - Performance also varies greatly for RMON 2 probes so try to purchase a probe that scores high in industry/government evaluations