

## **RMON2 Backgrounder**

The RMON standard has already increased the efficiency and lowered the cost of remote network monitoring and protocol analysis, and there's more yet to come! The RMON Working Group of the Internet Engineering Task Force (IETF) is already working on the next generation of RMON, dubbed RMON2. When RMON first arrived on the standards scene, it provided network managers with important data about the network segment health and performance. RMON2 moves beyond the segment up to the enterprise network and supplies the information needed for the health and performance monitoring of networked client/server applications and end-to-end communications.

## **RMON Introduction and Background**

Before getting into RMON2, first a little background on the original RMON, which will be referred to as RMON1 in this document for purposes of clarity. RMON1 is the **Remote Network MONitoring MIB** developed by the IETF to support monitoring and protocol analysis of Ethernet and Token Ring LANs. It included more open, comprehensive network fault diagnosis, planning and performance tuning features than any monitoring solution on the market at the time. It is an industry standard specification that provides much of the functionality offered by today's proprietary network analyzers and protocol analyzers.

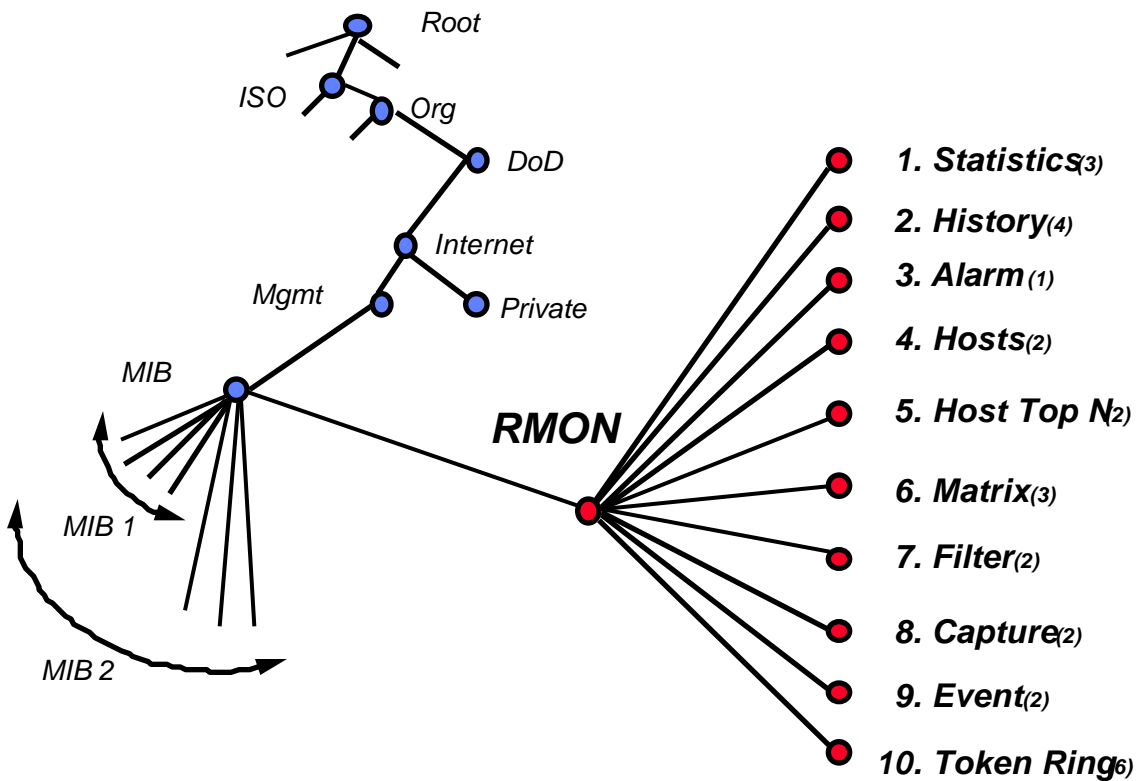
The RMON1 MIB standards effort started in 1990 with the creation of the RMON1 Working Group of the IETF. The RMON1 Proposed Standard, RFC 1271, was published in November, 1991. The first RFC focused specifically on Ethernet. The RMON1 Working Group augmented that initial work with the Token Ring extensions, RFC 1513, in 1993. Due to the high market demand and increasing customer interest, RMON1-compliant vendor implementations were rapidly developed and brought to market. The first RMON1 products were generally developed by independent LAN monitoring vendors, such as AXON (now part of the 3Com Network Management Division) with their RMON1-compliant LANServant Manager and Probes which began shipping to OEMs in 1992 and to end-user customers in 1993. Wide acceptance and adoption of the RMON1 standard by network infrastructure vendors followed. With proven, interoperable vendor implementations, the RMON1 MIB moved to Draft Standard status in December, 1994 and was assigned the new RFC number of 1757.

With the RMON1 MIB, network managers can collect information from remote network segments for the purposes of troubleshooting and performance monitoring. The RMON1 MIB provides:

- Current and historical traffic statistics for a network segment, for a specific host on a segment, and between hosts (matrix)
- A versatile alarm and event mechanism for setting thresholds and notifying the network manager of changes in network behavior
- A powerful, flexible filter and packet capture facility which can be used to deliver a complete, distributed protocol analyzer

The following figure shows a listing of the RMON1 groups and where RMON fits within the International Standards Organization (ISO) and IETF standards.

### RMON1 MIB Tree Diagram



(n) indicates number of tables in the group, including control tables

### How Does RMON Work?

RMON implementations are generally delivered as a two-part client/server solution. The “client” is the application that runs on the network management station and presents the RMON information to the user. The “servers” are the monitoring devices distributed throughout the remote networks that collect the RMON information and analyze network packets. The monitoring device is commonly called a “probe,” and it runs a software program, generally called an RMON “agent.” RMON agents can be found in dedicated devices and/or embedded in network infrastructure devices such as hubs and switches. The application and the agent communicate across the network using the Simple Network Management Protocol (SNMP).

RMON is designed so that the data collection and processing is done by the remote probe devices. This reduces the SNMP traffic on the network and the processing load on the management station. Instead of continuous polling, information is only transmitted to the management station when required. Many RMON “client” applications located in various parts of the network can simultaneously communicate with and get information from one RMON “server.” The information from a single RMON server can be used for many tasks, from troubleshooting and protocol analysis to performance monitoring and capacity planning.

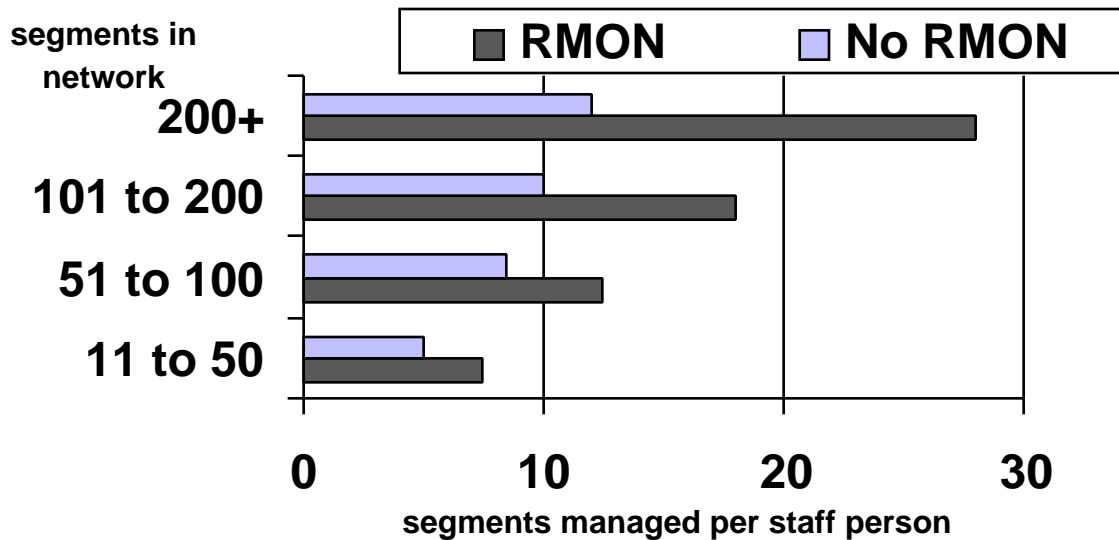
RMON1 provides valuable statistics on the whole network segment. Contrast this with other SNMP management products, which focus on monitoring and control of a specific network device. While device-specific management tools are important, they do not provide a picture of the health of the whole network segment with all its devices, servers, applications, and users.

## **Benefits Achieved with RMON1**

The benefits of RMON1 are clear. Without leaving the office, a network manager can see the traffic on a LAN segment, whether that segment is physically located around the corner or around the world. Armed with that traffic knowledge, the network manager can identify trends, bottlenecks, and hotspots. When a problem arises, RMON1 also includes a powerful protocol analyzer so the network manager has distributed troubleshooting tools immediately at hand. Since the RMON1 device is permanently attached to the network segment, it’s already collecting data about the remote LAN and ready to transmit it to a central network management station whenever required. All this network monitoring and troubleshooting can be done without spending the time and travel required to send expensive network experts with “lug-able” protocol analyzers to the remote site.

Deploying network management staff resources more efficiently means that one expert at a central site can be working on several problems by getting information from several probes at remote sites. Alternatively, several experts with different specialties can be focused on a single segment by getting information from a single probe.

Network managers desperately need tools that can leverage their resources and increase their scope of control. RMON1 does just that. A recent study by McConnell Consulting found that by using RMON1 distributed LAN management and remote monitoring techniques, a network management team can support as many as two-and-a-half times the users and segments without adding staff. Using RMON1 and the network to bring the problem to the expert is far more cost-efficient than dispatching someone to the remote site with a portable protocol analyzer.



Source: McConnell Consulting, Inc.  
9/94 Survey of LAN Managers

## What's Next? RMON2 !

The RMON2 Working Group began their efforts in July, 1994. As with the RMON1 standard, the approach is to carve out a set of deliverables that bring clear benefits to the network manager, that are implementable by multiple vendors, and that will lead to successful interoperability between independently developed solutions.

With those broad goals in mind, the top priority defined by the RMON2 Working Group is to go up the protocol stack and provide statistics on network- and application-layer traffic. By monitoring at the higher protocol layers, RMON2 provides the information that network managers need to see beyond the segment and get an internetwork or enterprise view of network traffic.

RMON1 vendors are already delivering some of these higher-layer protocol capabilities in the form of protocol distribution graphs, MAC-to-IP address translations, and application traffic analysis. This is currently done through proprietary extensions to their RMON1 products, but it means there are a number of examples and techniques that can be used as the RMON2 Working Group defines the new standard.

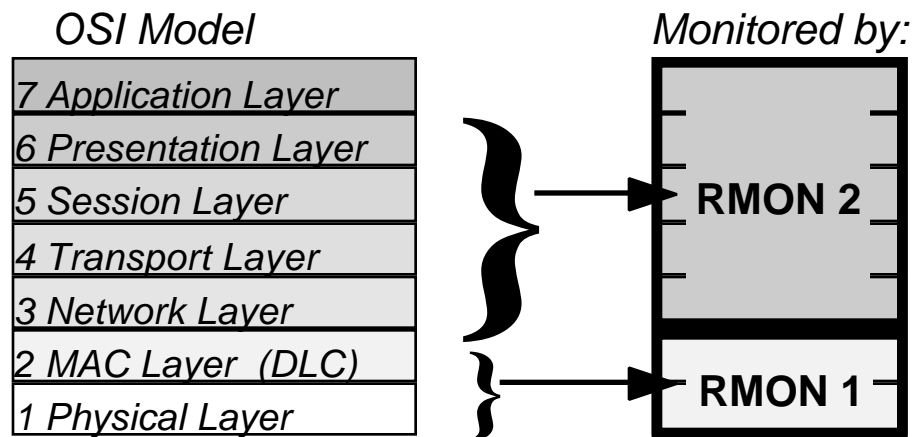
It's important to note that RMON2 is not a superset of or replacement for RMON1. Both MIBs will be required, with RMON1 providing the data for segment monitoring and protocol analysis and RMON2 providing the data for network and application monitoring.

## RMON2 Capabilities

The most visible and most beneficial capability in RMON2 is monitoring above the MAC layer which supports protocol distribution and provides a view of the whole network rather than a single segment. Although the exact contents of RMON2 may change during the standard development process, the capabilities expected to be delivered by RMON2 include:

- **Address Translation.** Binding between MAC-layer addresses and network-layer addresses which are much easier to read and remember. Address translation not only helps the network manager, it supports the SNMP management platform and will lead to improved topology maps. This feature also adds duplicate IP address detection, solving an often elusive problem that wrecks havoc with network routers and Virtual
  - **Higher Layer Statistics.** Traffic statistics, host, matrix, and matrix topN tables at the network layer and the application layer. By monitoring these statistics, the network manager can see what clients are talking to what servers, so systems can be placed at the correct location on the correct segment for optimized traffic flow.

AXON Networks has submitted their LANServant Manager Enterprise Communications Analysis Module (ECAM) MIB to the RMON2 Working Group to provide the technology required for these higher-layer statistics.



LANs.

- **User Defined History.** With this new feature, the network manager can configure history studies of any counter in the system, such as a specific history on a particular

file server or a router-to-router connection. In the RMON1 standard, historical data is collected only on a predefined set of statistics.

- **Improved Filtering.** Additional filters are required to support the higher-layer protocol capabilities of RMON2. This improved filtering allows the user to configure more flexible and efficient filters, especially relating to the higher-layer protocols.
- **Probe Configuration.** With RMON2, one vendor's RMON application will be able to remotely configure another vendor's RMON probe. Currently, each vendor provides a proprietary means of setting up and controlling their probes. The probe configuration specification is based on the Aspen MIB which was jointly developed by AXON and Hewlett-Packard. The Aspen MIB provides probe device configuration, trap administration, and control of the probe's out-of-band serial port.

## How Does RMON2 Work?

As with RMON1, RMON2 implementations will generally be delivered in two-part client/server solutions with the "client" applications communicating to the "server" agents using the Simple Network Management Protocol (SNMP). Like RMON1, RMON2 agents will be found in dedicated devices and/or embedded in network infrastructure devices. With the increased volume of traffic statistics being collected by RMON2, the processor power and memory of the agent will be very important considerations.

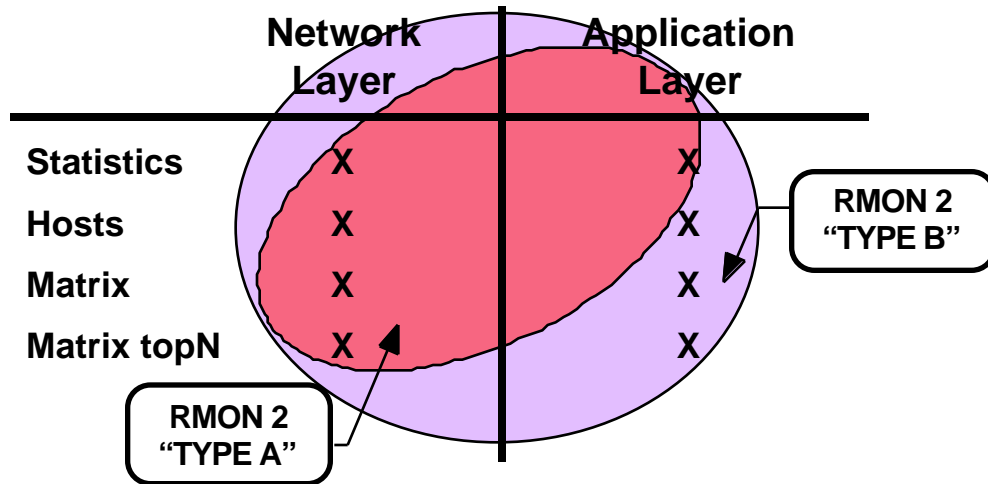
The most difficult challenges in meeting the RMON2 goal of providing traffic statistics at the network and application layers were:

- Defining the open, extensible structure for collecting the traffic, host and matrix data for each protocol and application
- Mapping the data collected by a probe to the correct protocol name that can then be displayed to the network manager

There are dozens of protocols running on any given network. Some are well known, some may be custom protocols developed for a particular customer or application. Any RMON2 solution had to provide a framework to support them all.

The Protocol Directory concept, submitted to the RMON2 Working Group with AXON's ECAM MIB, provided the solution. It separates the protocol definition from the table structure where the protocol traffic information is stored. As described by Robin Iddon, Chief Architect and AXON's delegate to the RMON2 Working Group, "The Protocol Directory is a simple and interoperable way for an RMON2 application to establish which protocols a particular RMON2 agent implements. This is especially important when the application and the agent are from different vendors."

The RMON2 Working Group currently plans to authorize two types of compliant implementations. Both types will support traffic statistics at the network and application layers. Products with less processor power and less memory can provide an RMON2-compliant implementation with host and matrix groups restricted to the network layer. Products with more processor power and more memory can provide an RMON2-compliant implementation with host and matrix groups supported at the more complex level of the application layer. This allows a range of RMON-compliant solutions to be developed, each targeted to a different purpose, and priced according to the capabilities provided.



For example, a less expensive, less memory-intensive “Type A”<sup>\*</sup> RMON2-compliant solution can be brought to market that provides a robust view of the internetwork backbone traffic and the network layer protocols that make up that traffic. A “Type A” RMON2 agent could be embedded in a network infrastructure device such as a hub or a router. An RMON2 client application could use “Type A” information to support network troubleshooting and the tuning of router backbones.

A more complex “Type B” RMON2-compliant application can be brought to market that provides a full matrix view of which systems are communicating with which servers and what applications are being used, highlighting the busiest Lotus Notes conversation pairs, or which PCs are sending the most cc: mail traffic. A “Type B” RMON2 agent is likely to require a dedicated probe device to supply the required processor performance and memory. An RMON2 client application could use this more complex “Type B” information to form the basis of a trend analysis/capacity planning solution or a complete accounting/chargeback system.

---

<sup>\*</sup> The RMON2 Working Group has not assigned names to the two classifications of RMON2-compliant products. “Type A” and “Type B” are used here for purposes of illustration only.

This choice of “Type A” and “Type B” is similar to the implementation flexibility in the RMON1 standard. While there are 10 groups defined in the RMON1 standard, a vendor is only required to fully implement one group in order to be RMON1-compliant.

The Protocol Directory will be the definitive listing of protocols supported by each vendor’s RMON2 MIB and whether “Type A” or “Type B” monitoring is provided for each protocol. In the category of “buyer beware,” it will be incumbent on the purchaser to ask the vendor which protocols are supported and what level of monitoring is provided for each protocol. The RMON2 Working Group is not dictating which protocols must be supported. A vendor can choose to support multiple protocol or specialize in in-depth monitoring for a single protocol and still be RMON2-compliant.

## **Benefits Expected with RMON2**

The most visible improvement provided by RMON2 is the extension of the traffic monitoring to the higher protocol layers. RMON1 provided traffic statistics at the MAC layer of the protocol. RMON2 adds insight to those traffic statistics by specifying the protocol and applications that make up that traffic. This protocol- and application-specific knowledge is crucial to deploying and troubleshooting today’s client/server environments. As a result, this raises RMON from the “segment-view” provided by RMON1 to the “enterprise-view” provided by RMON2.

RMON2 will clearly show the network manager who is talking to whom and what application(s) they are using. With this detailed knowledge of traffic patterns in the network and how the traffic from client/server applications is growing and changing , the network manager can ensure that users and resources are placed in the correct network location to optimize performance and reduce costs.

The network manager can debug network problems faster and more accurately using the statistics from the network layer matrix table which shows the protocol specific traffic between communicating pairs of systems. Instead of detecting that a given server is “dead” because it is not transmitting any packets (something that can be accomplished with RMON1), the network manager can diagnose the more difficult problem encountered when the server is “alive” but a specific protocol stack is malfunctioning.

Another example that highlights the usefulness of higher-layer monitoring is when the network manager is looking at information from an RMON probe on a particular network segment. A node on another segment is sending lots of traffic and having a negative impact on network performance. With RMON2, the network manager will see the actual host address of the “babbling” node whether it’s one hop away or halfway across the Internet. Contrast this to an existing RMON1 solution which would show the MAC address of the local router as the source of all traffic that originates off the segment.

## **RMON2 Status**

The initial Internet Draft of the RMON2 standard was released in June, 1995. It is expected to receive an RFC number and be published as a Proposed Standard during the summer of 1996. Once the Proposed Standard is published, RMON2-compliant vendor implementations can rapidly follow. If all proceeds well, RMON2-compliant solutions will be on the market late in 1996. Based on customer demand and vendor adoption, RMON2 could progress to a Draft Standard status with the required proven, interoperable vendor implementations in 1997.

AXON, now owned by 3Com Corporation and part of the new 3Com Network Management Division, is an active member and contributor to the RMON2 Working Group. AXON submitted their Enterprise Communications Analysis Module (ECAM) MIB for consideration as the architectural foundation for the RMON2 “up-the-stack” monitoring. It has acknowledged technical merit and field-proven implementation experience. The ECAM framework, in particular the protocol directory concept, has been used in significant parts of the new RMON2 MIB. AXON also jointly submitted with HP the Aspen MIB, many components of which have been adopted for standardizing the configuration of RMON probes.

RMON2 will deliver a dramatically increased volume of vital network traffic data. It will take a powerful application with a superior user interface to really make use of RMON2. Significant innovation is required in designing a method to gather RMON2 data from multiple probe and agent sources, combine and correlate the data, and present the data in the form of easy-to-understand information. With success in designing the award-winning RMON1 user interface—LANServant Manager; and field-proven experience delivering higher-layer protocol and application statistics—Enterprise Communications Analysis Module; you can count on 3Com/AXON to deliver RMON2 data to the network manager in a way that highlights the vital information and leads to improved performance of the network ... and the network management team!

AXON gratefully acknowledges the cooperation and assistance of Andy Bierman, chair of the RMON2 Working Group, Senior Software Engineer at Cisco Systems, and Steve Waldbusser, editor of the RMON2 specification and author of the RMON1 standard, Principal Architect at International Network Services, in the development and editing of this document.