RMON e RMON2 – *Remote Network Monitoring*

Luciano Paschoal Gaspary

O protocolo SNMP e a MIB-II ainda são amplamente utilizados para o gerenciamento de equipamentos de rede. Agentes de *software* presentes nesses equipamentos coletam informações sobre o tráfego de entrada e saída dos mesmos (ex.: número de pacotes recebidos e enviados). Com essas informações, o gerente de rede tem conhecimento sobre o volume de tráfego gerado por cada dispositivo monitorado. Para ter uma noção aproximada do tráfego total da rede, é preciso somar os valores obtidos de cada dispositivo. A distribuição cada vez maior, tanto geográfica como lógica, das redes de computadores tornou a utilização desta abordagem complexa e ineficiente.

Os equipamentos que suprem a dificuldade apontada acima são denominados monitores de rede ou *probes*. Tipicamente, um monitor opera em um segmento de rede local no modo *promíscuo*, observando cada pacote propagado nesse segmento. Os monitores podem produzir estatísticas com base nos pacotes observados (ex.: taxa de erros, número de colisões, número de pacotes entregues por segundo, entre outros). Além disso, podem armazenar pacotes para submetê-los, posteriormente, a algum tipo de análise. Filtros podem ser utilizados para limitar o número de pacotes contabilizados ou capturados, baseado em seu tipo ou alguma outra característica. As estatísticas e o tráfego armazenado podem ser recuperados pelas aplicações de gerenciamento através do protocolo SNMP [PER98].

Segundo Stallings [STA96], a maior contribuição ao conjunto de padrões SNMP foi a especificação de RMON1, MIB para monitoração remota, suplementar à MIB-II. Essa MIB foi criada para estabelecer funções e interfaces para a comunicação entre estações de gerenciamento e os *probes*.

Os objetos RMON são organizados em 20 grupos. Os primeiros 10 grupos constituem a MIB RMON1, voltada ao gerenciamento das operações realizadas nos níveis físico e de enlace em redes Ethernet. Ela compila estatísticas e informações históricas como número de colisões, erros de CRC, entre outras [MIL97]. Uma extensão dessa MIB adaptada para redes Token Ring está enquadrada em um grupo definido em um documento próprio. Os 10 grupos restantes constituem a MIB RMON2, proposta para viabilizar a coleta de estatísticas e informações para protocolos acima do nível de enlace. Ela permite a monitoração de padrões de uso da rede e a observação do tráfego de aplicações cliente-servidor (ex.: HTTP, FTP, DNS, entre outras) e comunicações fim a fim [PER98] (vide figura 1).

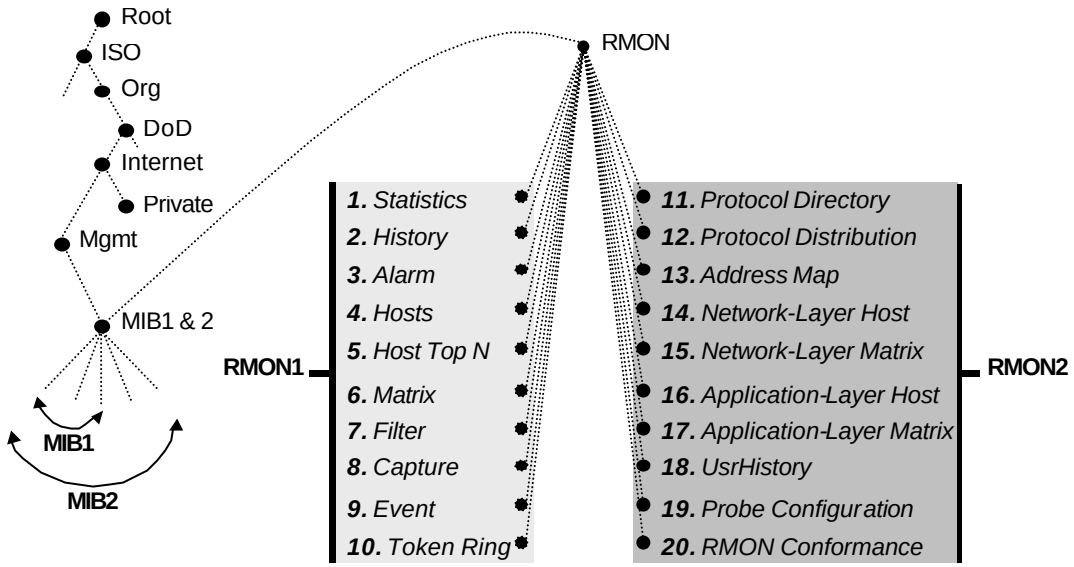


Figura 1 - Grupos das MIBs RMON e RMON2

1. Histórico e evolução das MIBs RMON

Antes da existência das MIBs RMON, vendedores forneciam dispositivos de monitoração dotados de teclado e visor. Os usuários desses dispositivos precisavam estar fisicamente presentes em frente aos mesmos para observar as estatísticas por eles coletadas. Havia várias interfaces e formatos para apresentar os resultados coletados aos usuários. Além disso, as informações recuperadas por dispositivos de diferentes fabricantes não eram coincidentes.

Segundo Perkins [PER98], o passo inicial rumo a definição do padrão RMON ocorreu quando alguns fabricantes começaram a desenvolver *probes* que não possuiam interface. Esses dispositivos eram uma "caixa-preta" com uma interface de rede e outra serial. À interface serial era conectado um terminal ASCII para configuração inicial do *probe*. Alguns destes dispositivos usavam um protocolo proprietário, outros SNMP, para recuperar informações de MIBs não padronizadas. Líderes do IETF reuniram essas iniciativas e formaram, em 1990, o grupo de trabalho RMON.

O primeiro documento gerado pelo grupo foi a RFC 1271, publicada em novembro de 1991. Este documento contém a definição da MIB RMON1 para redes Ethernet. Em 1993 o grupo de trabalho propôs extensões para redes Token Ring através da RFC1513 (vide tabela 1). O início dos trabalhos para a definição de RMON2 ocorreu em 1994. Paralelamente, o resultado das primeiras implementações e operações com RMON1 foi utilizado para aprimorar a versão original desta MIB. Esta iniciativa deu origem à RFC 1757, publicada em fevereiro de 1995, que substituiu a RFC 1271. Os trabalhos na definição da MIB RMON2 resultaram na publicação das RFCs 2021 e 2074, em janeiro de 1997.

Tabela 1 - RFCs de RMON

RFC	Título	Data
1271 obsolet	Remote Network Monitoring Management Information Base	Novembro de 1998
1513	Token Ring Extensions to the Remote Network Monitoring MIB	Setembro de 1993
1757	Remote Network Monitoring Management Information Base	Fevereiro de 1995
2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2	Janeiro de 1997
2074	Remote Network Monitoring MIB Protocol Identifiers	Janeiro de 1997
2613	Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0	Junho de 1999
internet draft	Remote Network Monitoring Management Information Base for High Capacity Networks	-
internet draft	Remote Network Monitoring MIB Protocol Identifier Macros	-
internet draft	Remote Network Monitoring MIB Protocol Identifier Reference	-

Ainda em 1997 novos trabalhos foram iniciados: MIB RMON para redes de alta velocidade e aprimoramento dos identificadores de protocolos.

2. Objetivos almejados para RMON

As metas definidas pelo grupo de trabalho para a definição das MIBs RMON são descritas nas RFCs 1757 e 2021 [PER98]. São elas:

- *Operação off-line:* nem sempre a estação de gerenciamento estará em constante contato com os *probes* RMON; isto pode ser feito com a finalidade de diminuir os custos de comunicação (especialmente quando o enlace de comunicação é uma linha discada) ou por falha entre as estações de gerenciamento e os agentes. Por essa razão, a MIB RMON deve permitir que os agentes sejam configurados para realizar diagnósticos e coletar estatísticas continuamente, mesmo que a comunicação entre a estação de gerenciamento e os agentes não seja possível ou não seja eficiente. O agente deve tentar notificar a estação de gerenciamento sobre a ocorrência de algum evento importante. Se a comunicação de notificação falhar, a informação sobre essa ocorrência pode ser continuamente acumulada pelos monitores e repassada às estações de gerenciamento da forma mais conveniente e eficiente possível.
- *Monitoração pró-ativa*: os recursos disponíveis nos monitores são potencialmente úteis para continuamente executar diagnósticos e manter *logs* de desempenho da rede. Como o monitor está sempre disponível desde o início de qualquer problema, ele deve poder notificar a estação de gerenciamento sobre a ocorrência de uma determinada falha e fazer um registro histórico de informações estatísticas sobre as falhas ocorridas. Esse histórico pode ser revisado pela estação de gerenciamento para, no futuro, realizar diagnósticos sobre as causas dos problemas.
- *Detecção e registro de problemas*: o monitor deve poder ser configurado para o reconhecimento de determinadas condições, realizando constantes averiguações. Quando uma dessas condições ocorre, o evento pode ser armazenado num *log* e as estações de gerenciamento podem ser notificadas de diferentes maneiras.

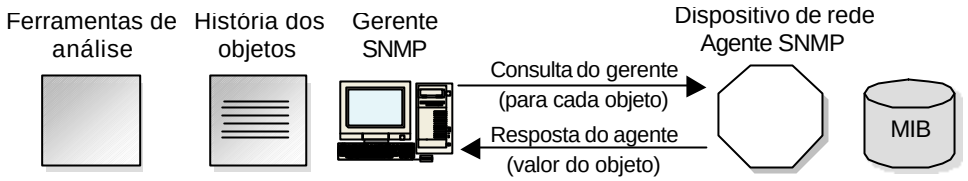
- *Dados com valor agregado:* o monitor de rede deve poder realizar análises específicas com os dados coletados na sub-rede onde atua, liberando a estação de gerenciamento dessa responsabilidade. Por exemplo, o *probe* pode analisar o tráfego da sub-rede para determinar que estações geram maior tráfego ou maior número de erros na sub-rede em questão [STA96].
- *Múltiplos gerentes*: uma organização pode ter múltiplas estações de gerenciamento em diferentes unidades da organização e com diferentes funções, possibilitando assim uma fácil recuperação de falhas. Como os ambientes com múltiplas estações de gerenciamento são comuns, os monitores remotos devem ter a capacidade de se relacionar com mais de uma estação de gerenciamento, usando assim seus recursos potencialmente.

3. Grupos da MIB RMON1

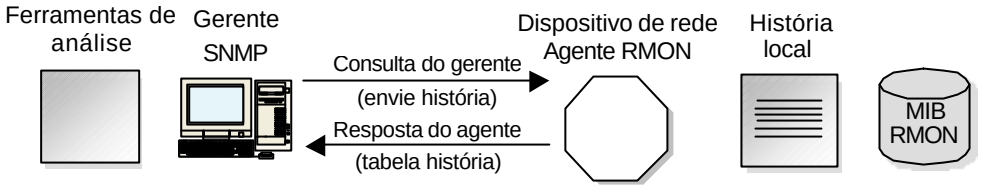
Os agentes RMON1 podem residir não apenas em dispositivos dedicados à tarefa de monitoração (*probes)*, mas também em equipamentos como *switches*, roteadores, entre outros. Distribuídos em pontos remotos, eles coletam informações definidas na MIB RMON1, analisando os quadros que trafegam nos segmentos da rede. A figura 1 lista os grupos da MIB RMON1 e ilustra onde ela se enquadra dentro dos padrões da ISO e do IETF [RMO97]. São eles [ART98, PER98, STA96]:

- *statistics*: esse grupo provê estatísticas medidas pelo monitor em cada uma de suas interfaces. As estatísticas incluem número de pacotes *unicast*, *broadcast e multicast*, número de colisões observadas no segmento, número de pacotes não contabilizados pelo agente, entre outras;
- *history*: registra amostras estatísticas periodicamente e armazena para uma posterior recuperação. Em cada amostra, são coletados dados pré-determinados. No caso de redes Ethernet, alguns dos dados coletados são: número de octetos e de pacotes observados, números de pacotes *broadcast* e *multicast*, número de erros de CRC, número de colisões, entre outros. Esta funcionalidade contribui tanto para a redução de tráfego SNMP na rede como para a diminuição do processamento realizado pela estação de gerenciamento [TEC97] (vide figura 2);
- *alarm*: esse grupo periodicamente obtém amostras estatísticas de variáveis da MIB e as compara com limiares superior e inferior previamente configurados. Se o valor recuperado ultrapassa o limite superior ou fica abaixo do limite inferior, um evento é gerado. Para limitar a geração de alarmes, o grupo define o mecanismo denominado *histerese*;
- *host*: mantém estatísticas sobre cada *host* descoberto na rede. O termo *host* designa qualquer equipamento dotado de uma interface de rede;
- *hostTopN*: o grupo *hostTopN* mantém relatórios que especificam os principais *hosts* de uma lista, ordenados por uma de suas estatísticas (ex.: primeiros 20 *hosts* com maior número de pacotes enviados);
- *matrix*:armazena estatísticas de tráfego e número de erros entre pares de *hosts*;
- *filter*: esse grupo provê um mecanismo para a estação de gerenciamento poder instruir o *probe* a observar pacotes selecionados. O critério para seleção dos pacotes é definido no formato de um ou mais filtros conjugados;

- *capture*: é usado para configurar um esquema de armazenamento temporário para captura de pacotes, de acordo com um dos critérios de seleção definido no grupo *filter*;
- *event*: esse grupo controla a geração e notificação de eventos.



(a) Esquema de consultas tradicional



(b) Esquema de consultas em soluções RMON/RMON2

Figura 2 - Interações entre gerentes e agentes

4. Monitoração de tráfego de protocolos de níveis superiores

A MIB RMON2 é uma extensão da MIB RMON1 tradicional, criada para suportar a monitoração de protocolos de alto nível [GAS98]. Os grupos definidos por ela são ilustrados na figura 1. São os seguintes:

- *protocol directory:* é um repositório que indica todos os protocolos (encapsulamentos) que o *probe* é capaz de interpretar;
- *protocol distribution*: agrega estatísticas sobre o volume de tráfego gerado por cada protocolo, por segmento de rede local;
- *address map*: associa cada endereço de rede ao respectivo endereço MAC, armazenando-os em uma tabela. A tradução de endereços permite a geração de mapas topológicos aprimorados e a detecção de endereços IP duplicados em uma rede;
- *network-layer host*: coleciona estatísticas sobre o volume de tráfego de entrada e saída das estações com base no endereço do nível de rede. Como conseqüência, o gerente pode observar além dos roteadores que interligam as sub-redes e identificar as reais estações que estão se comunicando. Este grupo coleta estatísticas similares às do grupo *host* da MIB RMON1. A diferença é que o grupo *nlHost* faz esta coleta com base no endereço de rede e não no endereço MAC;
- *network-layer matrix*: provê estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de rede;
- *application-layer host*: agrega estatísticas sobre o volume de tráfego de entrada e saída das estações com base em endereços do nível de aplicação. Consultas a este grupo permitem que o gerente trace um perfil sobre o volume de tráfego

gerado ou recebido por aplicações específicas como o *Lotus Notes*, o *Microsoft Mail*, entre outras;

- *application-layer matrix:* coleciona estatísticas sobre o volume de tráfego entre pares de estações com base no endereço do nível de aplicação;
- *user history collection:* amostra periodicamente objetos especificados pelo usuário (gerente) e armazena as informações coletadas de acordo com parâmetros definidos também pelo usuário. No padrão RMON1, esta funcionalidade é oferecida para um conjunto pré-definido de objetos;
- *probe configuration:* define parâmetros de configuração padrões para *probes* RMON. Deste modo, a estação de gerenciamento com *software* de um fabricante é capaz de configurar remotamente um *probe* de outro fabricante;
- *rmon conformance:* descreve requisitos de conformidade para a MIB RMON2.

a. *Visibilidade no nível de rede*

Com RMON1 , um *probe* pode monitorar todo o tráfego da LAN a qual está ligado. Ele pode capturar todos os quadros relativos à sub-camada MAC do nível de enlace e ler os endereços MAC fonte e destino dos mesmos. O *probe* é capaz de prover informações detalhadas sobre o tráfego de quadros enviados e recebidos por cada estação em cada LAN associada. Contudo, se um roteador está ligado a uma destas LANs, não há como determinar a fonte do tráfego que chega por ele, tampouco o destino de quadros que saem do segmento via este roteador [STA96]. Esta situação é ilustrada na figura 3 (extraída de [TEC97]).

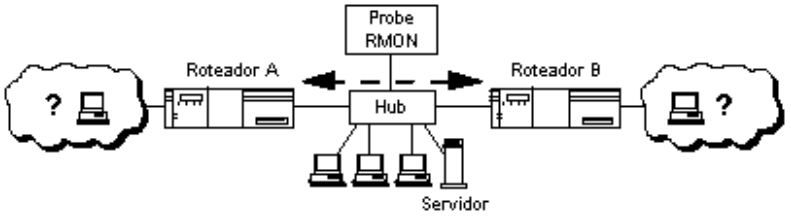


Figura 3 - Limitação da MIB RMON1

Com RMON2, por outro lado, o *probe* é capaz de operar com protocolos localizados acima do nível de enlace. Ele pode, por exemplo, ler o cabeçalho do protocolo do nível de rede encapsulado no quadro, que é tipicamente o protocolo IP. Isto permite a ele analisar o tráfego que passa através do roteador para determinar a fonte e destino reais dos pacotes. Com esta capacidade, o gerente de rede pode responder a uma série de questões como:

1. Se há sobrecarga na LAN devido ao tráfego que chega via o roteador, que sub-redes ou estações são responsáveis por atrair este volume de tráfego?
2. Se um roteador está sobrecarregado devido a um grande volume de tráfego de saída, que estações locais são responsáveis por este volume de tráfego e para que sub-redes ou estações destinos o tráfego é direcionado?
3. Se existe um grande volume de dados que chega via um roteador e deixa o segmento através de outro, que redes ou estações são responsáveis por este volume de tráfego?

Com respostas a questões como estas, o gerente de rede pode ser capaz de fazer um melhor planejamento para confinar este tráfego e, consequentemente, melhorar o

desempenho da rede. Por exemplo, ele pode verificar que clientes estão se comunicando com que servidores e posicionar estes sistemas em segmentos apropriados da rede, visando otimizar o fluxo de tráfego.

b. *Visibilidade no nível de aplicação*

Um *probe* RMON2 não está limitado à monitoração e decodificação de tráfego no nível de rede. Ele pode observar também protocolos do nível de aplicação. É importante salientar que utilizando a terminologia apresentada na RFC que define o RMON2, qualquer protocolo acima do nível de rede é considerado um protocolo de aplicação.

Um *probe* RMON2, por exemplo, é capaz de verificar acima do nível IP através da leitura e decodificação de protocolos de níveis superiores como TCP encapsulados no datagrama IP e, mais ainda, verificando os cabeçalhos dos protocolos do nível de aplicação. Isto permite ao gerente de rede monitorar tráfego com um alto grau de detalhamento [STA96].

Com RMON2, uma aplicação de gerenciamento de rede pode implementar a geração de gráficos apresentando porcentagens de tráfego por protocolo ou por aplicações. Novamente, este nível de detalhamento viabiliza a otimização da carga da rede e a manutenção do seu desempenho.

Referências bibliográficas

[ART96] ARTOLA, ESMILDA SÁENZ. **Olho vivo - Sistema Especialista para Gerência Pró-Ativa Remota**. Dissertação de Mestrado. Porto Alegre: PGCC da UFRGS, 1996.

[GAS98] GASPARY, LUCIANO P. **Estudo do padrão RMON2**. Trabalho Individual n. 646. Porto Alegre: PGCC da UFRGS, 1998.

[MIL97] MILLER, MARK. **Managing Internetworks with SNMP**. Second Edition. USA: M&T Books, 1997.

[PER98] PERKINS, DAVID T. **RMON - Remote Monitoring of SNMP-Managed LANs**. First Edition. USA: Prentice Hall, 1998.

[RMO97] RMON METHODOLOGY. **RMON Methodology**. Disponível por WWW em http://www.3com.com/nsc/500251.html (6 Nov. 1997).

[STA96] STALLINGS, WILLIAM. **SNMP, SNMPv2 and RMON**: Practical Network Management. Second Edition. USA: Addison Wesley, 1996.

[TEC97] TECHNOLOGY BANDWIDTH MANAGEMENT FOR CORPORATE INTRANETS. **Monitoring Intranet Traffic Flows with RMON/RMON2**. Disponível por WWW em http://www.3com.com.nsc/500631b.htm (22 de julho de 1998).