# MONITORAMENTO REMOTO DE REDES: RMON

**Jadiael Santos de Lima**
Faculdade Sete de Setembro (FASETE)
dielslima@gmail.com

**Francina Cibelly Araújo**
Faculdade Sete de Setembro (FASETE)
cibellyaraujo@live.com

**RESUMO**
A crescente evolução na utilização das redes de computadores fez emergir o propósito de se buscar uma maneira consistente de gerenciá-las; uma vez que o gerenciamento é essencial para o funcionamento contínuo da rede. O padrão RMON de gerenciamento surgiu como uma das mais importantes alternativas para sanar esse problema, visto que suas técnicas de monitoramento remoto têm demonstrado bastante eficácia, evitando os prejuízos que as empresas outrora sofriam e oferecendo-lhes a possibilidade de se prevenir de futuros problemas relacionados ao gerenciamento das redes.
**Palavras-chave**: Monitoramento. RMON. Rede. Gerenciamento

**ABSTRACT**
The increasing trend in the use of computer networks made the purpose of searching for a consistent way to manage them, as we know that management is essential to the continued operation of the network. The model of RMON management has emerged as one of the most important alternatives for solving this problem since its remote monitoring techniques have showed quite efficiency, avoiding damages on these business companies and offering to them the ability to prevent future problems related to management networks.
**Keywords:** monitoring. RMON. Networks. management.

## INTRODUÇÃO

As redes de computadores foram inicialmente projetadas para possibilitar o compartilhamento de recursos, tais como: impressoras e outros instrumentos, além de serem exclusivas para ambientes acadêmicos, governamentais, militares e empresas de grande porte; tudo isso em meados da década de 60. No entanto, o crescimento da utilização de recursos computacionais, causado pelo barateamento do custo dos equipamentos, aliado à evolução das tecnologias de rede, motivou a propagação das redes de computadores nos diversos setores da sociedade, somando-se à utilização nas organizações.

Esse avanço despertou a necessidade de gerenciamento padronizado das redes, forçando as grandes instituições de pesquisa a se mobilizarem em busca de soluções. Em 1990, a *Internet Engineering Task Force* (IETF) – órgão responsável pelo desenvolvimento da padronização da internet – propôs, através da *Request for Comments* (RFC) – documento que descreve os padrões dos protocolos – 1157, o protocolo *Simple Network Management Protocol* (SNMP) – um protocolo de gerenciamento simples que emitia alertas quando a rede atingia um estado crítico.

Com o intuito de eliminar as limitações e os defeitos causados pela simplicidade excessiva do protocolo supracitado surgiu o padrão *Remote MONitoring* (RMON) de gerenciamento, que ao descentralizar e hierarquizar o monitoramento da rede se tornou uma solução completa e eficaz para a gerência de redes de médio e grande porte.

Este artigo foi elaborado com a finalidade de explanar de forma clara e concisa o funcionamento do padrão RMON, além disso, esclarecer os conceitos que cercam a utilização desse recurso e mencionar as mudanças e os benefícios decorrentes de sua evolução.

A organização deste artigo, que possui seis seções está dividida de forma a expor os conceitos necessários para entender esse padrão de gerenciamento. A seção 2, discorre sobre as definições do padrão RMON, além de seus objetivos, sua arquitetura e demais elementos que dele fazem parte; na seção 3, descreve-se a forma como o mesmo realiza o gerenciamento de redes; a seção 4 mostra as vantagens e desvantagens de utilizá-lo e na seção 5 destaca-se as versões existentes desse padrão. Na conclusão do artigo, que está na seção 6, apresentamos a nossa opinião sobre essa tecnologia e porque devemos utilizá-la em uma organização.

## 1 REMOTE MONITORING (RMON)

RMON não é uma pilha de protocolos; nem tampouco um protocolo por si só; trata-se de uma extensão de *Management Information Base* (MIB), para ser utilizada com protocolos de gerenciamento de redes em internets baseadas em TCP/IP. Esta é a definição dada para este padrão de gerenciamento de redes pela IETF, através da RFC 1757, em 1995.

Antes da existência do RMON, dispositivos de monitoramento dotados de teclado e visor eram utilizados. Para realizar um gerenciamento através destes, era necessário que o usuário estivesse em frente aos mesmos para coletar os resultados [Gaspary, 1998]. Além disso, os resultados de um mesmo monitoramento eram diferentes dependendo do fabricante do dispositivo, tornando as análises incompatíveis.

Essa situação só começou a melhorar quando começaram a surgir *probes – agentes de gerenciamento* que não possuíam interface. Segundo Perkins [Perkins, 1998], esse foi o passo inicial rumo a definição do padrão RMON. Alguns destes dispositivos já utilizavam o protocolo SNMP para recuperar informações não padronizadas. A partir destas iniciativas, líderes do IETF formaram, em 1990, o grupo de trabalho RMON, destinado a criar e padronizar o mesmo.

A criação do grupo de trabalho RMON foi justificada porque, segundo Freitas e Monteiro, o protocolo SNMP, criado anteriormente pela própria IETF, não é adequado para ambientes de redes corporativas e constituídas de diversas redes locais conectadas através de outra de longa distância. Quando se utiliza o SNMP, esses enlaces de redes de longa distância passam a ter grande parte de sua banda de transmissão ocupada com informações de gerenciamento [Freitas e Monteiro, 2004]; haja vista que no referido protocolo é necessário um agente MIB para cada ponto de rede.

O próprio significado do padrão RMON já dá um indício de como foi solucionado o problema deixado pelo SNMP. O *Remote MONitoring* oferece suporte à implementação de um gerenciamento remoto e distribuído. Nele são atribuídas, a alguns elementos da rede, as funções de monitorar remotamente.

Vale ressaltar que é incorreto afirmar que uma empresa tem que escolher entre a gerência de RMON e de SMNP, porque, segundo Menezes e Silva, o RMON é uma MIB padrão do SNMP que controla agentes de monitoração remota. Assim sendo, RMON é considerado uma extensão do SNMP.

## 2 OBJETIVOS

Os objetivos gerenciais do RMON foram definidos nas RFC's 1757 e 2021. São eles:

- Operação *off-line*: Ocorre nas situações em que a estação de gerenciamento não está em contato contínuo com os monitores remotos. Pode ocorrer propositalmente, quando prevista no projeto de redes para reduzir custos de conexão, ou quando sucede uma falha na rede, interrompendo o contato.

Nestas ocasiões, o *probe* continua coletando estatísticas e fazendo diagnósticos, mesmo não estando conectado ao gerente. O monitor, porém, deve tentar comunicar à estação de gerenciamento sempre que ocorrer algum evento importante. Se a comunicação falhar, esses eventos são armazenados para serem informados aos gerentes assim que for possível.

- Monitoramento Proativo: Sempre que tiver recursos disponíveis, o monitor deve fazer diagnósticos constantes do desempenho da rede. O probe estará sempre disponível quando uma falha ocorrer. Deste modo ele deve notificar a estação de gerenciamento sobre a falha, bem como, guardar um registro histórico de informações estatísticas sobres os erros ocorridos, para ser posteriormente utilizado pelo gerente a fim de fazer um estudo mais detalhado e permitir a detecção e reparo das falhas.

- Detecção e notificação de problemas: O monitor tem a capacidade de identificar problemas (congestionamento, tempestades de broadcast, etc) no momento em que ocorrem. No advento de uma destas situações ele pode armazenar no histórico a ocorrência além de notificar à estação de gerenciamento. É possível que uma notificação seja enviada diretamente para o administrador da rede, por meio de SMS, por exemplo, desde que a estação esteja previamente configurada.

- Valor agregado aos dados: Considerando que estão em contato direto com as redes que monitoram, os probes podem realizar uma análise significativa nos dados, agregando valor a estes para poder fornecer informações específicas às estações de gerenciamento. Ex.: o monitor pode analisar o tráfego da sub-rede para determinar quais estações geram maior tráfego ou maior número de erros na sub-rede em questão [Stallings, 1996].

- Múltiplos gerentes: Um ambiente de rede pode possuir mais de uma estação de gerenciamento, seja para casos de recuperação rápida, ou para executar funções diferentes. Um monitor de rede deve ser capaz de se reportar a mais de um gerente simultaneamente.

## 3 ARQUITETURA

Como vimos, o RMON é um padrão da IETF, logo, não é proprietário. E, segundo Lessa, um único fabricante dificilmente irá implementar uma solução RMON completa. No cenário de gerenciamento RMON, os equipamentos de redes carregam MIB's RMON, a rede transporta os dados, um sistema de gerenciamento aceita os alarmes notificando aos usuários e uma ferramenta de análise RMON interage com os grupos RMON e seus dados [Lessa, 1999].

Na figura que se segue (Figura 1) podemos ver um exemplo de configuração usando RMON. As três sub-redes na porção esquerda/baixo são localizadas no mesmo prédio. As outras duas são em locais remotos. Uma estação gerente com RMON agente/gerente está na LAN central. Em duas das sub-redes, o agente RMON está em PC's, que podem ser dedicados ou não. Conectado ao backbone de FDDI (interface de dados

de fibra-ótica) está o segundo gerente. Finalmente, as funções de agente RMON para a LAN Token-Ring são executadas pelo roteador que conecta a LAN ao resto da Internet.

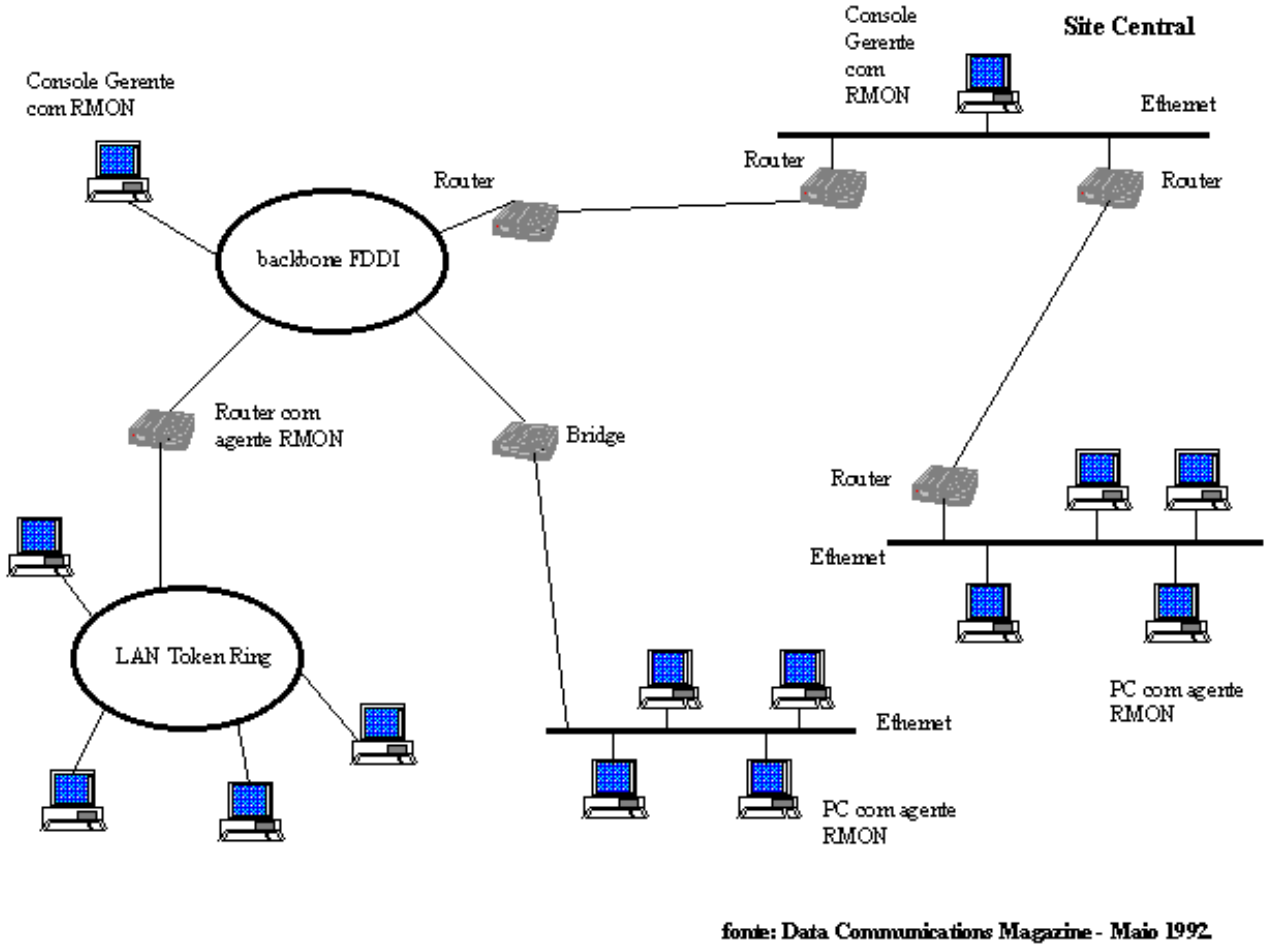


**Figura 1**. Arquitetura utilizando RMON
**Fonte:** Data Communications Maganize, 1992

### 3.1 Probes

Também chamados de monitores de rede, analisadores de redes, pontas de prova, ou simplesmente sondas, os *probes* são dispositivos usados para coleta de dados remotos no RMON e estudar o tráfego da rede como um todo [Mariz e Sadok, 2003]. Elas produzem informações sintéticas que incluem estatísticas de erro e desempenho, entre outras.

Geralmente, é necessário um probe por sub-rede [Mariz e Sadok, 2003], mas uma organização também pode empregar um dispositivo por segmento de rede [Lessa, 1999]. Podem ser configuradas como uma função disponível no sistema (no caso de ser um dispositivo com outras responsabilidades – *Workstation*, servidor, roteador) ou como um dispositivo dedicado (*stand-alone*). Nesta última hipótese, o monitor é capaz de executar funções mais complexas [Freitas e Monteiro, 2004].

Inicialmente, o *probe* tem a mesma função de um agente SNMP, porém, ela possui a capacidade de monitoramento remoto que os agentes não possuem. Na Figura 2 podemos ver um exemplo de arquitetura que usa SNMP e RMON, com os devidos *probes*.

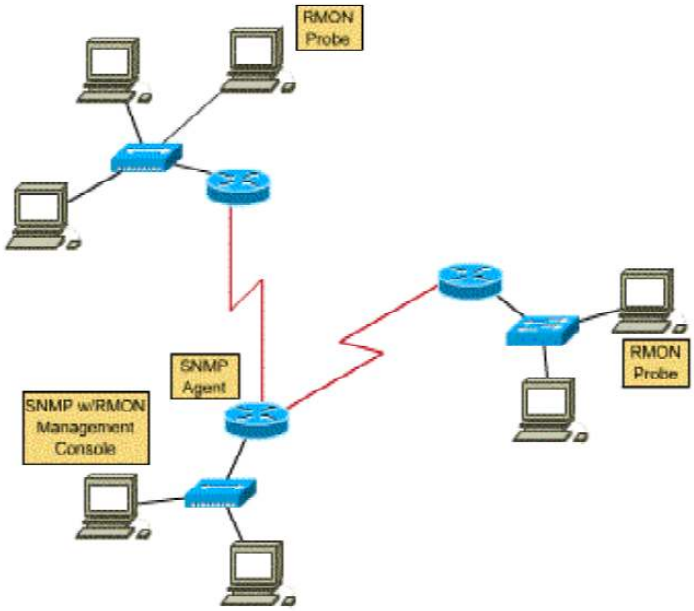


**Figura 2**. Probes RMON
**Fonte:** Cysco Systems Inc, 2000

Na ilustração da figura 2 acima cada monitor coleta dados específicos de cada sub-rede e os encaminha para o Console de Gerenciamento Central que, como no SMNP, é o ponto de coleta de dados. Pelas características dos *probes*, nota-se que elas atendem perfeitamente a todos objetivos – metas – definidos para o padrão RMON.

### *3.1.1 Management Information Base* (MIB)

Segundo Menezes e Silva, Base de Informação Gerencial (MIB – *Management Information Base*) é o nome que se dá ao conjunto de informações de gerenciamento; nele estão incluídos os objetos gerenciados e seus atributos, operações e notificações e, em alguns casos, as informações para configuração do sistema.

Cada objeto gerenciado representa um recurso sujeito ao gerenciamento e, é definido pelos seus atributos, pelas operações a que pode ser submetido, notificações que pode emitir e seus relacionamentos com os outros objetos gerenciados. Sendo assim, o conjunto de objetos gerenciados junto aos seus atributos, operações e notificações constituem a MIB [Menezes e Silva, 1998].

A MIB-RMON é organizada em grupos funcionais, onde dentro de cada grupo existem tabelas de controle e tabelas de dados. Nas tabelas de controle (que permitem leitura e escrita), que têm a função de descrever os dados, cada linha contém informações de controle sobre a monitoração, sendo cada coluna um parâmetro. As tabelas de dados (que são somente-leitura) contêm os dados coletados.

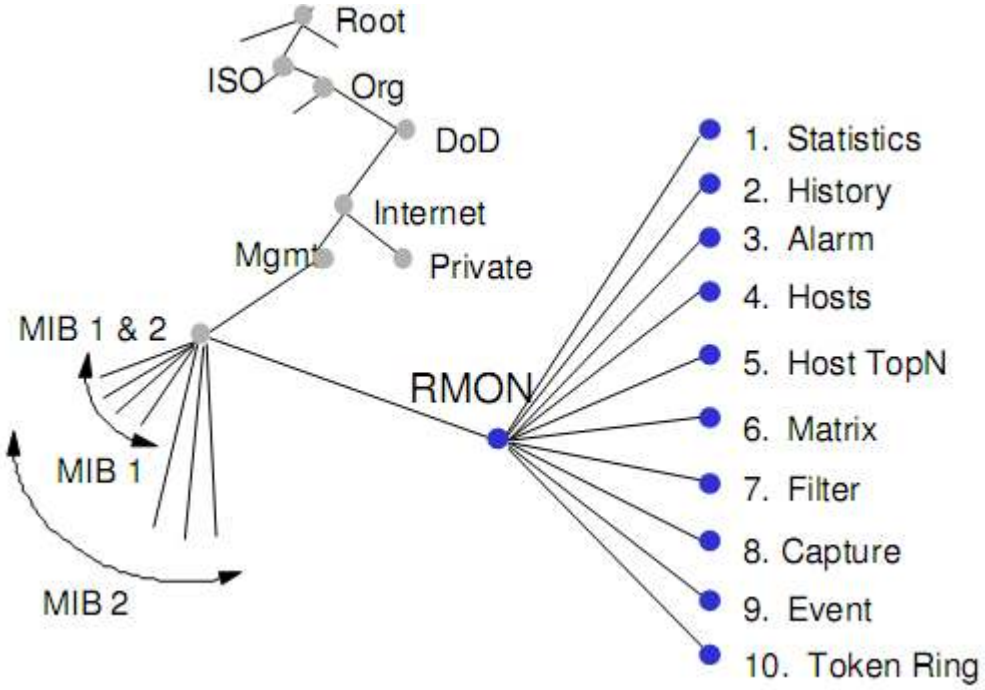


**Figura 3.** Grupos da MIB – RMON FONTE
**Fonte:** Mariz e Sadok, 2003

Na Figura 3 podemos ver os 10 grupos que estão definidos na MIB RMON. Vejamos o que significa cada um deles [Artola, 1998], [Perkins, 1998], [Stallings, 1996]:

**1.** Estatístico: esse grupo mantém estatísticas coletadas em cada interface monitorada pelo agente. Tais estatísticas incluem contadores de bytes, de pacotes, de erros, tamanho de quadro, etc.

**2.** Histórico: registra amostras estatísticas periodicamente armazenando-as no *probe* para um gerenciamento pró-ativo. Esse grupo contribui tanto para a redução de tráfego gerencial na rede como para diminuição do processamento realizado pela estação de gerenciamento [TEC, 1997]. A redução de tráfego se explica porque nem toda informação coletada deve ser enviada ao gerente, visto que é armazenada no próprio monitor, e a redução do processamento de gerenciamento porque tal tarefa foi dividida entre os probes.

**3.** Alarmes: define limites (*thresholds*) de desempenho para os objetos gerenciados. Esses limites são previamente configurados e se, no momento de uma coleta de dados, algum limite inferior ou superior for atingido, um evento (alarme) é gerado, criando uma notificação para a estação de gerenciamento.

**4.** *Hosts*: contém informações sobre cada *host* conhecido no segmento de rede. Os *hosts* são descobertos na rede a partir da captura de pacotes recebidos promiscuamente. É utilizado no gerenciamento de contabilidade, de desempenho e de configuração.

**5.** Classificação de 'n' Hosts: permite ordenar os hosts a partir de um critério de classificação para, posteriormente, gerar relatórios com informações úteis. Ex.: quais hosts geram o maior número de tráfego de broadcast.

**6.** Matriz: mantém informações de tráfego entre conversas envolvendo pares de hosts na sub-rede.

**7.** Filtro: permite selecionar pacotes de acordo um critério de específico, para que eles possam ser observados ou capturados. Existem dois tipos: filtro de dados e filtro de status. O de dados é projetado para um determinado padrão de dados; o de status, conforme o tipo de pacotes observado. Esse grupo é utilizado no gerenciamento de falhas de segurança.

**8.** Captura de pacotes: define como devem ser capturados os dados dos pacotes que trafegam pela rede, ou que atendem a um dos requisitos dos filtros, para que sejam analisados detalhadamente.

**9.** Evento: controla a geração e a notificação de eventos. Ajuda a eliminar a necessidade do gerente da rede de averiguar, ele próprio, periodicamente, os dispositivos para descobrir falhas, visto que ele será informado se algo ocorrer.

**10.***Token Ring*: contém contadores específicos para redes *Token Ring* – tipo de rede cuja topologia é em formato de anel (*ring*) e na qual circula uma ficha (*token*) que é o dispositivo pelo qual são enviadas as mensagens.

Convém enfatizar que não é obrigatório o uso de todos os grupos MIB em uma determinada configuração de rede. Entretanto há casos em que um grupo depende de outro (ex.: grupo 6 depende do 5). Há também grupos que são para tipos de redes muito específicas (ex.: grupo 10).

## 4 GERENCIAMENTO DE REDE COM O PADRÃO RMON

O gerenciamento de rede utilizando RMON ocorre em duas etapas: configuração e invocação de ação [Freitas e Monteiro, 2004].

- Configuração: tipicamente, para que um monitor remoto colete dados, ele precisa ser configurado. Essa configuração é feita inserindo, alterando ou removendo linhas da tabela de controle da MIB, como também, as funções que devem ser executadas pelo *probe* são definidas e implementados no mesmo.

- Invocação de Ação: sabemos que o SNMP tem apenas a capacidade de ler e alterar (setar) valores de objetos com visão MIB. O RMON, por sua vez, permite realizar uma ação em virtude de valores assumidos por objetos dentro da MIB. Ex.: digamos que os objetos representem estados. Uma ação é executada se a estação gerenciada mudar de estado (que é o valor do objeto). Os valores podem ser alterados através do comando “SNMP set”.

A seguir veremos dois exemplos sobre a utilização do padrão RMON. O primeiro é um gerenciamento de perdas de pacotes em uma rede ethernet.

Consideremos uma rede *ethernet* em que o percentual de perda de pacotes aceitável é 1% (acima disso é considerado crítico). Por meio de uma estação de gerenciamento (gerente), o administrador da rede configura, na tabela de controle da MIB, o limite de perdas de pacotes para 0,5%; recapitulamos que o grupo da MIB responsável pelos limites é o Grupo de Alarme.

Caso, em algum momento, a rede perca mais que 0,5%, um alarme será ativado pelo *probe* gerando um evento (outro grupo da MIB). O evento suscitará uma notificação à estação de gerenciamento, além de, estando ele configurado para isso, enviar uma mensagem diretamente ao administrador da rede (via SMS, por exemplo). O monitor que detectou aquela anormalidade iniciará também um processo de filtragem e captura de dados (pacotes) para análise porvindoura.

O segundo exemplo é um pouco mais abrangente: considere uma empresa X de saneamento de água de nível estadual. Digamos que X possui sede tecnológica na capital do estado, onde ficam as centrais dos programas e do gerenciamento de rede. X também possui uma sub-rede em cada município em que possui estação de tratamento de água. X também possui sub-núcleos de tecnologia divididos por macro-regiões, onde cada macro-região abrange 20 municípios.

Aplicando o padrão RMON, colocaremos um *probe* para cada sub-rede, ou seja, em cada cidade onde há estação de tratamento; usaremos gerência descentralizada, em cada macro-região haverá uma estação de gerenciamento, além da Estação Central de Gerenciamento, que ficará localizada na capital do estado.

Suponhamos que o *probe* responsável por analisar a sub-rede 001 tenha sido configurada para emitir alarme quando o nível de envio de mensagens broadcast de um determinado host ultrapassar 3%. Ressaltamos que essa configuração é feita na tabela de controle do grupo Alarme do MIB.

Em um determinado instante, esse *host* emite 5% de mensagens *broadcast*. Nesse momento, um evento do MIB é ativado e o monitor, ao tempo em que inicia o processo de armazenamento de dados sobre aquela situação para gerenciamento proativo, tenta notificar à estação de gerenciamento à qual está "subordinado" – que gerencia aquela macro-região. Contudo, exatamente neste momento, há uma falha de comunicação entre o *probe* e a estação de gerenciamento, impossibilitando o envio daquela notificação.

Agora, convenhamos que esse mesmo probe tenha sido configurado para reportar a mais de um gerente, simultaneamente (que é o objetivo 5 do RMON). O monitor então envia aquela notificação para a Estação Central de Gerenciamento, que alertará o administrador da rede a tomar as devidas providências a respeito daquele "evento".

Nestes exemplos percebem-se, além do cumprimento dos objetivos do RMON, as duas fases do gerenciamento no padrão RMON, citadas anteriormente: a configuração (inicial) e a invocação de ação.

## 5 VANTAGENS E DESVANTAGENS

A maior vantagem do RMON é o próprio monitoramento remoto. Ele desencadeia uma série de outras vantagens secundárias:

- Diminuição do tráfego de gerenciamento na rede (como as informações de erros são analisadas pelos próprios *probes* a mensagem é refinada antes de ser enviada para a estação de gerenciamento);
- Redução no processamento de erros na estação central (quando um gerenciamento é distribuído ele deixa de fazer todo o processamento em um único equipamento para fazer um pouco em vários);
- Informações bem mais detalhadas sobre o erro (ao contrário do SNMP que emitia apenas um alerta, os *probes* RMON enviam informações precisas);
- Filtros de captura (critérios que diminuem a quantidade de pacotes que devem ser analisados na amostragem);
- Coleta tráfego da rede (recurso que não existe no SNMP) *in loco*.

- Possibilidade de gerenciar redes pequenas, médias (essas duas por causa da "qualidade" da informação captada pelos *probes*) e grandes empresas (por causa das vantagens mencionadas acima).

Quanto às desvantagens do RMON, a principal delas é que esse padrão só opera até a camada Media *Access Contro*l (MAC), o que faz com que o RMON não tenha a capacidade de distinguir o tráfego originado através de um roteador (Menezes e Silva, 1998). Porém, essa deficiência não existe no RMON2, que foi lançado posteriormente.

Outra desvantagem diz respeito ao preço dos monitores autônomos, que podem não ser acessíveis para empresas de pequeno porte, além de requerer certo tempo para posicioná-las para uso.

## 6 VERSÕES

Visando suprir as limitações do RMON, que opera apenas até a camada MAC do modelo OSI e é destinado apenas ao gerenciamento de redes *Ethernet* e *Token* Ring, foram publicadas, em janeiro de 1997, as RFC's 2021 e 2074, que definiram o padrão RMON 2.

O RMON 2 é uma extensão do RMON criada para suportar a monitoração de protocolos de alto nível [Gaspary, 1998], possibilitando coletar informações estatísticas e monitorar a comunicação fim-a-fim, e o tráfego gerado por diferentes tipos de aplicações. Essa expansão torna possível ter uma visão completa dos fluxos de tráfego da rede.

A MIB RMON2 também possui dez grupos em sua arquitetura, conforme veremos na Figura 4. São eles [Gaspary, 1998]:

- Diretório de protocolo;
- Distribuição de protocolos;
- Mapeamento de endereços;
- Camada de rede do host;
- Matriz da camada de rede;
- Camada de aplicação do host;
- Matriz da camada de aplicação;
- Histórico do usuário;
- Configuração do probe;
- Conformidade RMON.

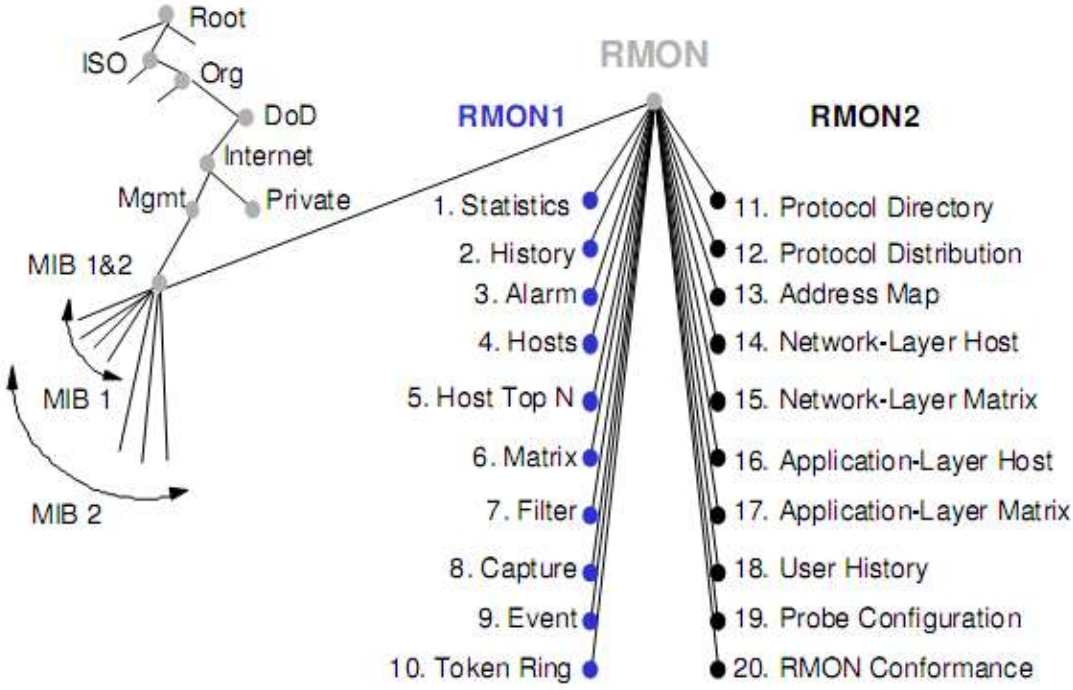


**Figura 4.** Arquitetura RMON2
**Fonte:** Gaspary, 1998

## CONSIDERAÇÕES FINAIS

Ao optar pelo padrão RMON para realizar o gerenciamento da rede, uma organização está aderindo a uma das mais completas e eficazes soluções existentes no setor. Seu monitoramento descentralizado garantirá a rápida detecção de erros sem implicar em perda de desempenho da rede.

Apesar de ter que realizar um investimento significativo inicialmente, a empresa usufruirá da garantia de confiabilidade e disponibilidade da rede sem interrupções ou perdas. Do mesmo modo como tudo que envolve tecnologia está sempre em evolução, vimos que o padrão RMON de gerenciamento também evoluiu, dando suporte a um gerenciamento potencialmente mais abrangente, e extinguindo quaisquer deficiências encontradas no modelo anterior.

Conclui-se que, os motivos que levam uma empresa a optar pelo padrão RMON, além de já serem muitos, estão em constante evolução buscando melhorar continuamente e garantir o bom desempenho de um número cada vez maior de redes de computadores.

## REFERÊNCIAS

ARTOLA, Esmilda Sáenz. **Olho vivo:** Sistema Especialista para Gerência Pró-Ativa Remota. 1996. Dissertação (Mestrado). PGCC da UFRGS, Porto Alegre.
FREITAS, Claiton Araújo. MONTEIRO, João Wesley Alves. **Análise de Protocolos na Área de Gerência de Redes.** Projeto Final de Curso. Goiânia - 2004
GASPARY, Luciano P. **Estudo do padrão RMON2.** n. 646. Porto Alegre: PGCC da UFRGS, 1998.

LESSA, Demian. **O Protocolo de Gerenciamento RMON.** Disponível em: < http://www.rnp.br/newsgen/9901/rmon.html.> Acessado em: 18 de maio de 2010.
MARIZ, Dênio. SADOK, Djamel. **Gerenciamento de Redes – RMON- Remonte Network Monitoring.** Recife – UFPE/cin, 2003.
MENEZES, Elionildo da Silva. SILVA, Pedro L. Leite. **Gerenciamento de Resdes:** Estudo de Protocolos. Workshop de Administração e Integração de Sistemas. Recife, UFPE - DPI, 1998.
PERKINS, David T. **RMON - Remote Monitoring of SNMP-Managed LANs**. First Edition. USA: Prentice Hall, 1998.
STALLINGS, William. **SNMP, SNMPv2 and RMON**: Practical Network Management. Second Edition. USA: Addison Wesley, 1996.
TECHNOLOGY Bandwidth Management For Corporate Intranets**. Monitoring Intranet Traffic Flows with RMON/RMON2.** Disponível em: < http://www.3com.com.nsc/500631b.htm> Acessado em: 22 de julho de 1998.