

RMON – Monitoramento Remoto

Prof. Mauro Tapajós



Remote Network Monitoring

- RMON é uma extensão a SNMP que agrega funcionalidades de monitoramento da rede e oferecem informações vitais para gerenciamento
- A MIB II somente oferecia informação puramente local de dispositivos individuais
- RMON oferece informações que dizem respeito a rede de forma distribuída, como contadores de pacotes e erros numa determinada LAN
- RMON é basicamente uma especificação de MIB
- Nenhuma mudança é necessária na SMI SNMP ou mesmo no protocolo SNMP, está tudo especificado dentro da MIB RMON

Objetivos

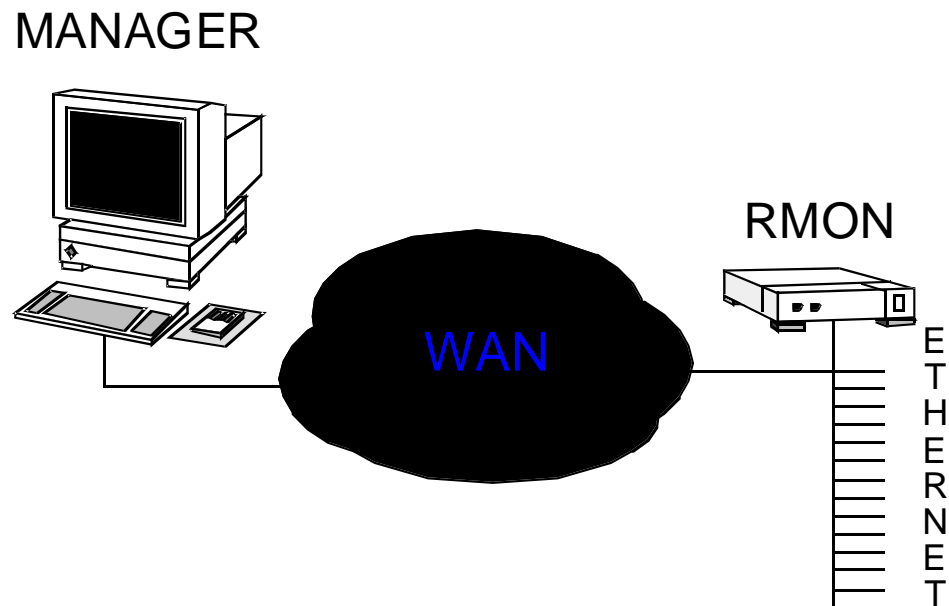
1. Operação independente da estação gerenciadora
 2. Monitoramento proativo (depende de recursos e da rede)
 3. Detecção de problemas – monitoramento preemptivo
 4. Dados de valor adicionado (especialização)
 5. Suporte a vários gerentes
- A MIB RMON oferece suporte a todos estes objetivos

Monitores

- Equipamentos / software usados para observar e controlar uma determinada LAN ou conjunto de dispositivos
- Também chamados de *probes*
- Possuem algum tipo de inteligência e armazenam dados coletados
- Monitoram a situação normal e alertam um gerente de uma anormalidade com uma *trap*
- Estão mais preocupados com indicadores como limites de erros e perfis de tráfego
- Independência: em caso de falha no gerente, continuam a coletar dados até a sua volta à operação

Monitores

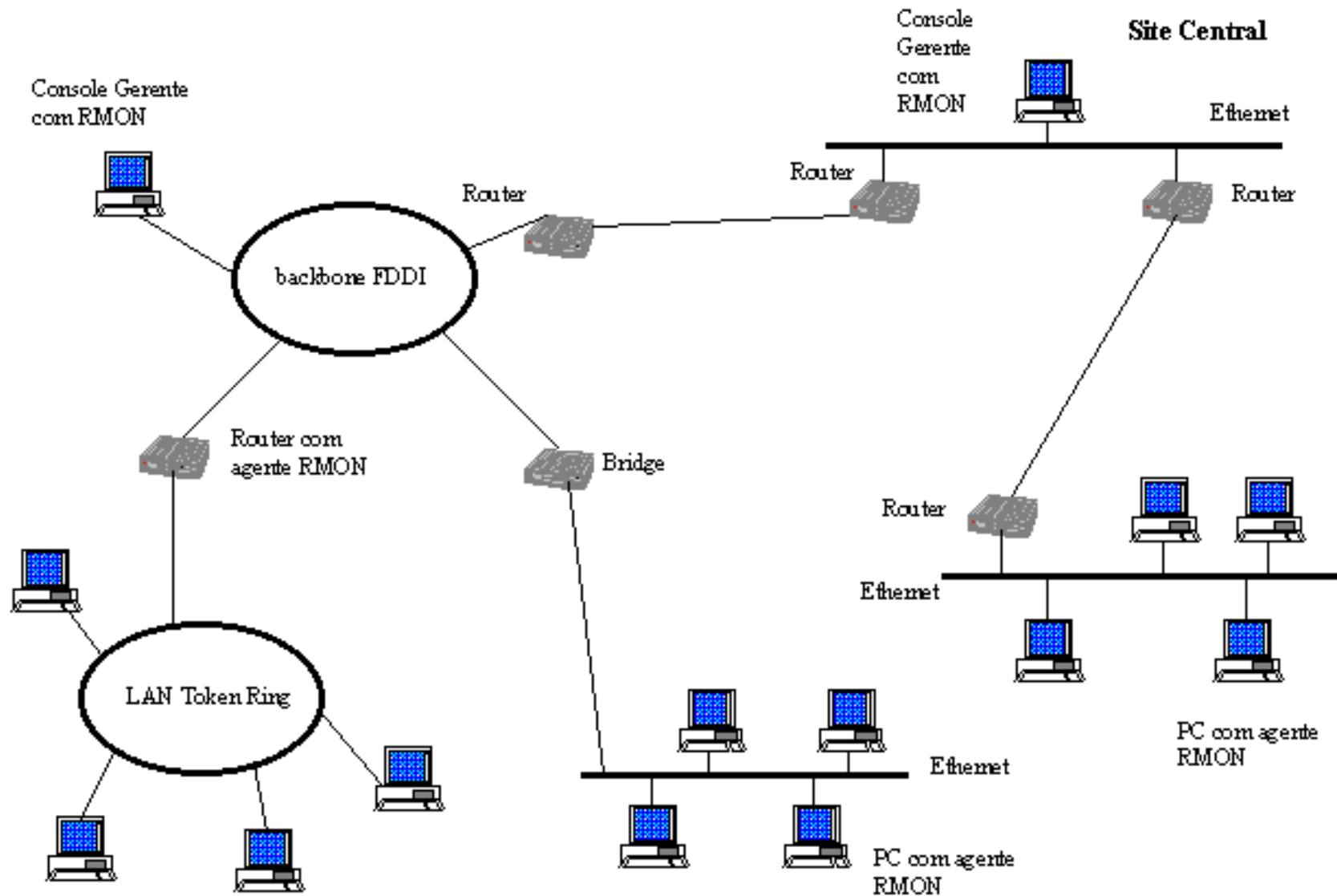
- Podem ter múltiplas interfaces de rede, permitindo um monitoramento de várias redes distintas ou do tráfego entre elas
- Monitores sabem o que ocorre na rede e possuem inteligência para reagir a certas situações, isto o torna extremamente útil
- Podem armazenar estas informações de forma a permitir uma posterior análise



A MIB RMON

- É uma MIB definida na RFC 2819 e que apresenta mecanismos para um gerente configurar e controlar um monitor, ter condições de coletar seus dados importantes e receber seus alarmes
- A MIB permite o “compartilhamento” do monitor entre várias estações gerentes
- A RFC 2819 define variáveis e estatísticas gerais
- Algumas variáveis e estatísticas são específicas de alguma tecnologia, estas descritas em documentos específicos

Monitoramento com RMON



Configuração do RMON

- Várias estações de gerenciamento podem requerer estatísticas e dados da rede
- A configuração da RMON basicamente diz respeito ao tipo e a forma dos dados a serem coletados
- Para cada estatística existe parâmetros definidos pelo gerente (Ex. intervalo de medição)
- Normalmente, existirão duas tabelas: uma de controle e uma de resultados do monitoramento
- Cada gerente configura seus pedidos na tabela de controle
- Cada entrada nesta tabela possui um identificador que será usado depois para reconhecer o dado coletado na tabela de resultados

Configuração do RMON

- Duas variáveis da tabela de controle definem o acesso aos dados:
 - **OwnerString**: é uma string que identifica o dono da entrada na tabela. É sugerido que este nome contenha informações específicas da estação gerente como seu endereço IP, o nome da estação, sua localização, ...
 - **EntryStatus**: é um valor inteiro que indica o estado atual da entrada na tabela. Operações de *set* irão criar a entrada. Inicializações serão feitas e logo depois a entrada terá status de *valid*. Após o trabalho ter acabado o *status* se torna *invalid*. Valores possíveis:
 - *Valid* (1)
 - *createRequest* (2)
 - *underCreation* (3)
 - *Invalid* (4)

Vários gerentes

- Problemas podem surgir com a utilização de um mesmo monitor por vários gerentes
 - Muitos pedidos concorrentes de vários gerentes podem sobrecarregar a capacidade de um monitor
 - Uma única estação gerente pode alocar muitos recursos do monitor e mantê-los por muito tempo (injustiça no atendimento)
 - Uma estação gerente pode alocar recursos e sofrer um problema impedindo a liberação destes recursos para outros gerentes

Manipulação de Tabelas

- A tabela em SNMP é uma estrutura lógica
- Existem operações sobre linhas inteiras (deletar, acrescentar, controle de consistência)
- Coluna *EntryStatus* (RFC 2819): criada para definir o estado de uma determinada linha da tabela. Seus valores podem ser:
 - *createRequest*
 - *underCreation*
 - *Valid*
 - *invalid*
- Criação de linhas: pode-se usar valores *default*

Operações sobre as tabelas

- **Adição de uma linha:** gerente envia operação de *set* com todos os dados necessários. O monitor verifica a consistência dos dados segundo a MIB RMON
- **Deleção de uma linha:** operação de *set* para *EntryStatus* como *invalid*
- **Modificação de linhas:** normalmente se deleta as linhas correspondentes e se cria novas de acordo com a alteração

Grupos da MIB RMON

Grupos de estatísticas de tráfego e erro

- ***statistics (1)***: contadores simples de tráfego (octetos, colisões, erros, etc) numa interface de rede
- ***history (2)***: conjuntos de estatísticas pedidas e coletadas em intervalos definidos
- ***host (4)***: para cada host descoberto na rede, o monitor pode coletar estatísticas de tráfego e erros.
- ***hostTopN (5)***: os *hosts* que apresentarem números mais relevantes (“tops”) num determinado intervalo, são ordenados e apresentados numa tabela para fins de geração de relatórios. Requer a implementação do grupo *host*

Grupos da MIB RMON

Matriz de tráfego entre sistemas

- **Matrix (6):** estabelece tabelas onde se sabe os valores de tráfego de e para cada sistema na rede. Aqui se reconhece as origens e destinos dos pacotes que trafegam na rede. Cada entrada é criada para cada nova informação de comunicação entre dois endereços, obtida de pacotes recebidos. Útil para detecção de intrusos.

Grupos da MIB RMON

Grupos de filtragem e captura de tráfego

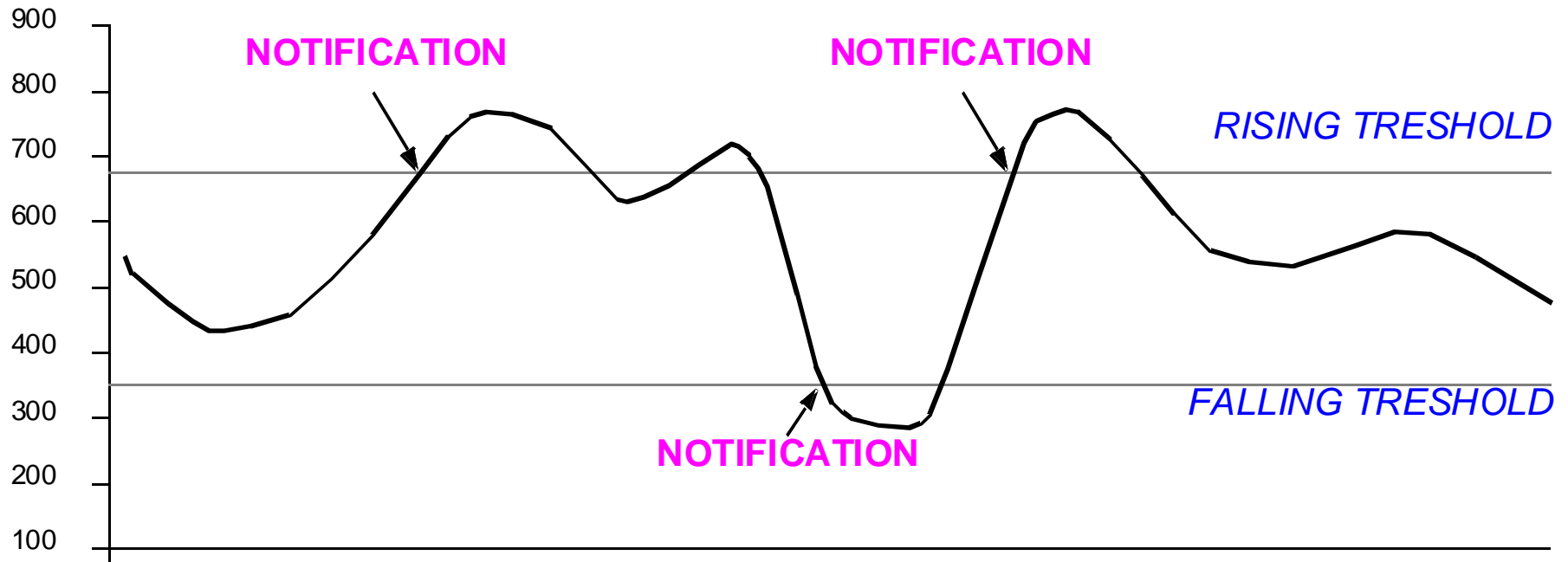
- ***Filter (7)***: parâmetros que definem critérios de filtragem dos pacotes criando “canais” (fluxos de pacotes que satisfazem determinada expressão lógica usada na filtragem)
- ***Packet capture (8)***: configuração do armazenamento dos resultados da filtragem feita. Requer a implementação do grupo *filter*.

Grupos da MIB RMON

Grupos de alarmes e eventos

- **Alarm (3):** o grupo contém variáveis que devem ser vigiadas e relacionamentos com eventos que serão disparados no caso destas variáveis ultrapassarem certos limites. Estes limites definem o que pode ser um indicativo de problema e também o que pode ser uma volta à normalidade. Sua implementação exige o grupo *event*
- **Event (9):** define cada evento de forma a notificar um gerente via *trap* ou atualizar um arquivo de log, ou outras ações como acionar uma captura de tráfego

Eventos e Alarmes



RMON 2

- RMON 1 basicamente lidava com quadros em nível de enlace (camada MAC), apesar de chamá-los de pacotes
- Uma extensão à RMON 1 era requerida para lidar com o tráfego de protocolos acima da camada MAC
- RFC 2021 – é um padrão proposto
- Assim, monitores RMON 2 podem analisar PDU's de níveis superiores (camadas de rede até aplicação) oferecendo a possibilidade de monitoramento do tráfego proveniente de roteadores e até de aplicações distintas
- Com isso, os fenômenos de tráfego podem ser melhor compreendidos (fatos como aplicações mais “pesadas”, servidores mais acessados, protocolos mais exigidos, etc)

Novos Grupos RMON 2

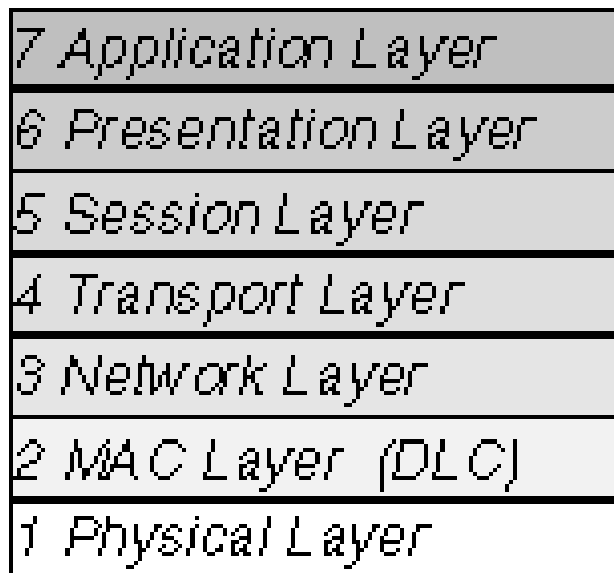
- ***protocol directory (11)***: informações sobre os protocolos que o monitor pode analisar
- ***protocol distribution (12)***: dados do tráfego apresentado por cada protocolo
- ***address map (13)***: dados do mapeamento de endereços MAC em endereços de rede
- ***network-layer host (14)***: estatísticas de tráfego a nível de endereços de rede, entrante e saiente num determinado host
- ***network-layer matrix (15)***: estatísticas de tráfego de e para, a nível de endereços de rede

Novos Grupos RMON 2

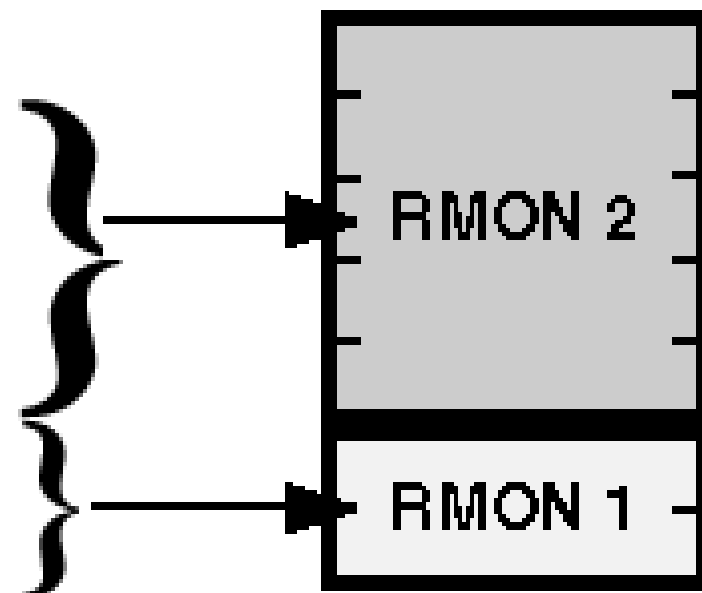
- ***application-layer host (16)***: estatísticas de tráfego a nível de aplicação, entrante e saínte num determinado host
- ***application-layer matrix (17)***: estatísticas de tráfego de e para, a nível de aplicação
- ***user history (18)***: dados específicos por usuários
- ***probe configuration (19)***: parâmetros operacionais de configuração do monitor RMON (configurações de interações com interfaces seriais, aspectos de download de informações, destinos de traps, etc)
- Extensão de grupos de RMON1 - alguns objetos específicos

RMON 2

OSI Model



Monitored by:



SMON

- Estende RMON para uso em redes comutadas (*switched*)
- Neste tipo de rede o tráfego não tem característica *broadcast* (meio compartilhado)
- Incorpora segmentação lógica (VLAN's) e mecanismos de priorização (operação mais complexa)
- Os mecanismos propostos em RMON não oferecem facilidades para estas características específicas
- São disponibilizadas facilidades para monitoramento de tráfego entre portas distintas, espelhamento de tráfego, VLAN's, e adequação à monitoramento IEEE 802.1q (priorização) e 802.1p (suporte VLAN's)
- É um padrão proposto na RFC 2613