

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

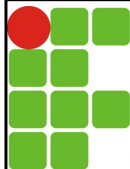


Gerência de Redes

Turma : 20172.5.01405.1N

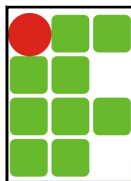
RMON

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>



Agenda

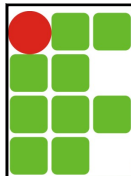
- Introdução
- Monitores
- Objetivos
- MIB RMON
 - Grupos
- RMON2
 - Histórico
 - MIB RMON2



Introdução

- Limitações da MIB-2
 - O gerenciamento é realizado em cada dispositivo individualmente
 - Gerentes podem obter informações locais de cada agente individualmente, mas não da rede como um todo
 - Os dispositivos gerenciados precisam ter instalados um agente e uma MIB
 - O gerenciamento gera um tráfego que pode ser elevado
 - A estação de gerência, dependendo da quantidade de dispositivos gerenciados, pode ficar sobrecarregada
 - A visão "localizada" de cada agente dificulta a geração de estatísticas
 - Essas estatísticas podem ter problemas de precisão

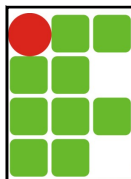
3



Introdução

- RMON = Remote Network Monitoring
- Ele define a "remote monitoring MIB" a qual suplementa a MIB-2 e provê aos gerentes informações vitais sobre o funcionamento da rede sem realizar nenhuma alteração no protocolo SNMP
 - O RMON é considerado a adição mais importante ao conjunto de padrões do SNMP.
- De um forma primária, o RMON é uma especificação de uma nova MIB porém, seu efeito é o de padronizar funcionalidades e interfaces de monitoramento de uma rede como um todo
 - MIB RMON -> RFC 2819

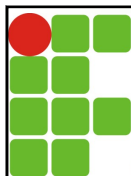
4



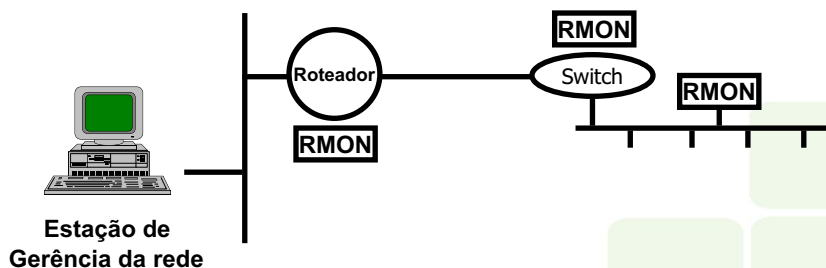
Monitores

- O RMON apresenta mecanismos para um gerente configurar e controlar um **monitor** remoto, coletar seus dados e receber seus alarmes
 - Historicamente, dispositivos e/ou softwares que analisam todo o tráfego de uma rede são chamados **monitores** ou **analísadores de tráfego**. Atualmente, também são denominados de PROBES (sondas).
- **Monitores são utilizados para observar e controlar um segmento de rede definido ou um conjunto de dispositivos**
 - São independentes: em caso de falhas no gerente continuam a coletar dados
 - Podem ser dispositivos dedicados à captura de dados e a sua análise
 - Dão suporte a MIB-2 (para poderem ser monitorados) e a MIB RMON (para poderem monitorar o segmento de rede)

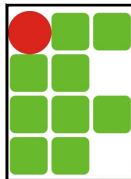
5



Monitores



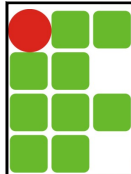
6



Monitores

- Controle dos Monitores
 - Um monitor deve ser dotado de memória e processamento extras (se comparados com um agente tradicional), já que realiza tarefas mais complexas e um maior número de funções
 - O controle de monitor através dos gerentes normalmente se dá pelo envio de mensagens SNMP SetRequest para objetos específicos da MIB RMON

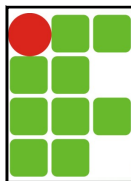
7



Objetivos

- São objetivos do RMON:
 - Operação Offline
 - Monitoramento Proativo
 - Detecção e Monitoramento de Problemas
 - Múltiplos Gerentes
 - Análise de Dados

8

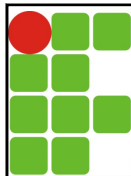


Objetivos

■ Operação Offline

- O monitor deve coletar informações de configuração, performance e falhas continuamente, mesmo se não solicitado por um gerente
- O monitor continuamente acumula estatísticas que podem ser recuperadas por um gerente assim que esse desejar

9

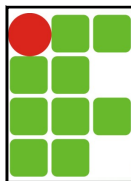


Objetivos

■ Monitoramento Proativo

- O monitor pode executar diagnósticos contínuos e registrar seus resultados
- Na ocorrência de uma falha o monitor pode notificar o gerente e prover informações importantes para seu diagnóstico
- Logs de performance da rede podem ser disponibilizados para o gerente

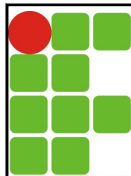
10



Objetivos

- **Deteccão e Monitoramento de Problemas**
 - O monitor deve ser capaz de reconhecer certas condições (por exemplo congestionamento) com base no tráfego que observa
 - Sua ocorrência deve ser registrada e pode-se notificar um gerente
- **Múltiplos Gerentes**
 - Um monitor deve ser capaz de lidar com vários gerentes simultaneamente

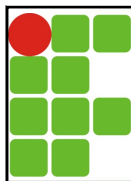
11



Objetivos

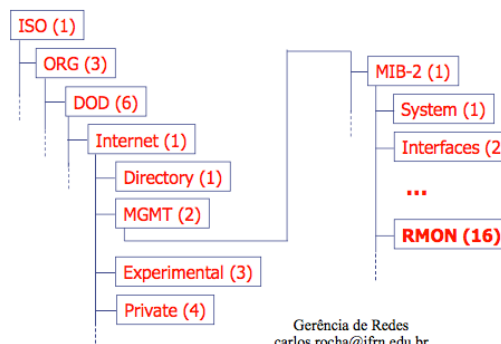
- **Análise de Dados**
 - O monitor deve coletar e analisar dados que trafegam na rede, retirando esta responsabilidade do gerente
 - O monitor pode então gerar estatísticas e determinar, por exemplo, qual host gera mais tráfego ou erros na rede

12



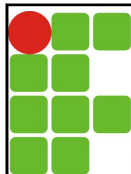
MIB RMON

- O "coração" do RMON está na especificação da sua MIB, um dos ramos da MIB-2

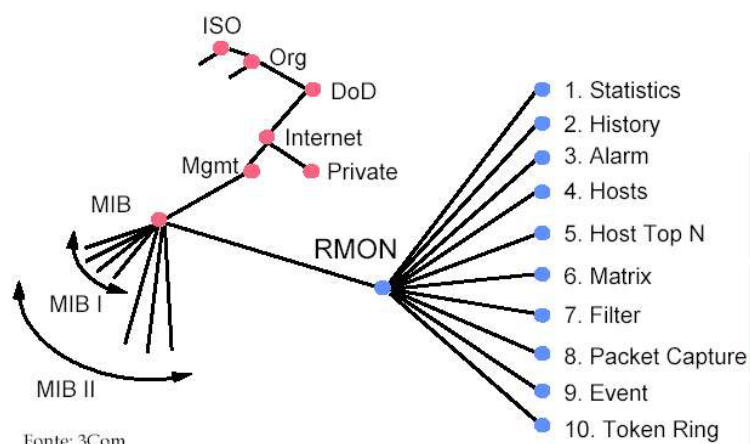


Gerência de Redes
carlos.rocha@ifrn.edu.br

13

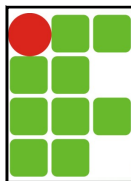


MIB RMON



Fonte: 3Com

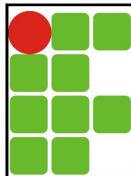
14



Grupos

- Grupos de estatísticas de tráfego:
 - statistics(1)
 - history(2)
 - host(4)
 - hostTopN(5)
- Matriz de tráfego entre sistemas
 - matrix(6)
- Grupos de filtragem e captura de tráfego
 - filter(7)
 - packet capture(8)
- Grupos de alarmes e eventos
 - alarm(3)
 - event(9)

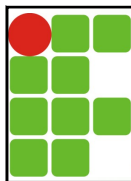
15



Grupos

- Cada grupo RMON é usado para armazenar dados e estatísticas derivadas das informações coletadas pelo monitor em uma ou mais redes
 - O conjunto de dados armazenados em cada grupo dependem de como o monitor foi configurado
- Todos os grupos são opcionais, contudo existem dependências
 - alarm(3) requer event(9)
 - hostTopN(5) requer host(4)
 - packetCapture(8) requer filter(7)

16

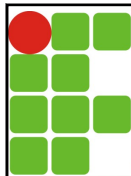


Grupos

■ Grupo **statistics**

- **Contém estatísticas básicas de cada sub-rede monitorada**
 - Contadores simples de tráfego (octetos, colisões, erros, broadcasts)
 - Pacotes descartados
 - Erros (Fragmentos, CRC, Undersize, Oversize)
- Reduz o tráfego agente-gerente e a carga de processamento no gerente
- SNMP recupera tabela inteira

17

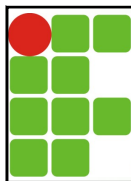


Grupos

■ Grupo **history**

- **Conjunto de estatísticas solicitadas, baseadas nas informações do grupo statistics**
- Coletadas em intervalos definidos
 - Configuração
 - Intervalo de amostragem
 - Quantidade de amostras
- Permite a análise de tendência de comportamento de uma rede
- Tabelas
 - HistotyControlTable – Detalhes de amostragem
 - EtherHistoryTable – Dados amostrados

18

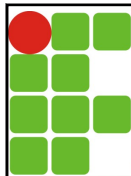


Grupos

■ Grupo **host**

- **Contadores de tráfego relativos à hosts descobertos em um determinado segmento de rede monitorada**
 - A observação dos hosts se dá através dos MACs de origem e destino
- **Para cada host são mantidas uma série de estatísticas. Exemplos:**
 - Número de bytes transmitidos e recebidos
 - Número de pacotes transmitidos e recebidos
 - Número de pacotes com erro transmitidos
- **Tabelas**
 - HostTable – Cada linha possui informações estatísticas de cada host descoberto
 - HostControlTable – Tabela de controle do monitor
 - HostTimeTable – Ordem relativa em que os hosts foram descobertos

19

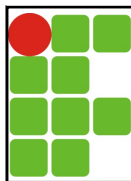


Grupos

■ Grupo **hostTopN**

- **Com base no grupo hosts, apresenta estatísticas ordenadas (do maior para o menor) em função de um determinado objeto**
 - Os objetos podem ser: inPkts, outPkts, inOctets, outOctets, outErrors, outBroadcast e outMulticast
 - Exemplos:
 - As 10 máquinas que mais transmitiram pacotes na rede hoje;
 - As 5 máquinas que mais transmitiram pacotes com erros nas últimas 2 horas;
 - As 20 máquinas que mais geraram tráfego de broadcast na semana.
- **Requer a configuração de tamanho da tabela resultante, intervalo de amostragem e objeto de ordenação**
- **Tabelas**
 - HostTopNTable
 - HostTopNControlTable

20

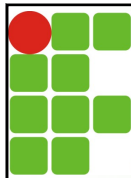


Grupos

■ Grupo **matrix**

- Estabelece tabelas com volume de tráfego entre pares de hosts com base no endereço MAC
- Uma entrada é criada para cada nova informação de comunicação entre dois endereços obtida de pacotes recebidos
- Tabelas
 - MatrixControlTable
 - MatrixSDTable – Estação Origem-Destino
 - MatrixDSTable – Estação Destino-Origem

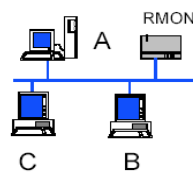
21



Grupos

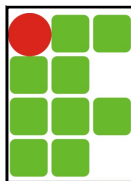
■ Grupo **matrix**

- ◆ Exemplo:
 - ❖ Servidor A
 - ❖ Estações B e C



		Origem		
		A	B	C
Destino	A	—	10400 oct 1200 pkts 5 error pkt	10400 oct 1200 pkts 5 error pkt
	B	2400 oct 480 pkts 2 error pkt	—	1028 oct 47 pkts 0 error pkt
	C	3200 oct 210 pkts 1 error pkt	10400 oct 1200 pkts 5 error pkt	—

22

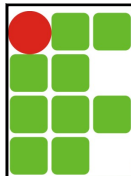


Grupos

■ Grupo **filter**

- Provê mecanismos para um monitor “observar” pacotes em uma sub-rede
 - Exige a definição de critérios de filtragem de pacotes
 - Filtros podem ser feitos com base nos dados ou no status do pacote
- Se o pacote atende às condições estabelecidas:
 - O pacote pode ser capturado ou registra estatísticas baseadas no mesmo
- O fluxo de pacotes que casam com um filtro é chamado de canal (channel)
- Exemplos:
 - Filtra os pacotes que tenham como um destino o host A e não se originam no servidor
 - Filtra os pacotes IPX que possuem erros
 - Filtra os pacotes destinados ao servidor RARP

23

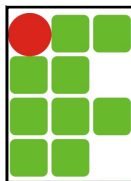


Grupos

■ Grupo **packetPacture**

- **Configuração e armazenamento dos resultados da filtragem (canais) feita pelo grupo filter**
 - Além do conteúdo do pacote capturado, ficam disponíveis informações como:
 - Tamanho do pacote
 - Momento da captura
- **Parâmetros da captura:**
 - Quantos bytes de cada pacotes serão armazenados?
 - Default são os 100 primeiros bytes
 - Qual filtro determina os pacotes a serem capturados?
 - Qual o tamanho do buffer a ser utilizado? Se o buffer encher, que ação deve ser realizada

24

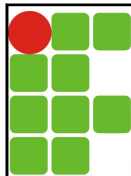


Grupos

■ Grupo alarm

- Permite a definição de limiares relacionados à performance da rede
 - Contém variáveis que devem ser "vigiadas" e relacionamentos com eventos que serão disparados
- Os limites podem ser indicativos de problemas ou volta à normalidade
 - Se um limiar for atingido, um alarme é gerado e enviado ao gerente

25

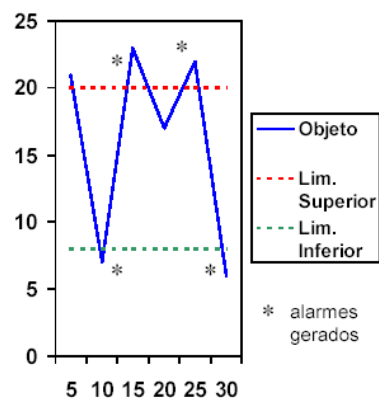


Grupos

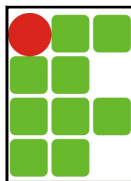
■ Grupo alarm

■ Exemplos

- Mais de 20 pacotes com erro nos últimos 5 minutos
- Mais de 100 pacotes com erro a cada 5 minutos
- Bytes enviados for menor que 100.000.000/5s



26

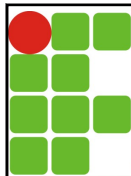


Grupos

■ Grupo **event**

- Permite a definição de "eventos" que serão desencadeados por uma condição descrita na MIB
 - Cada evento definido possui seu tipo e sua última ocorrência
 - Em geral eventos são gerados por:
 - Cruzamento de um limiar definido num alarme
 - Resultado de um filtro
- Pode definir ações como: notificar um gerente via trap, atualizar um arquivo de log ou adicionar uma captura de tráfego

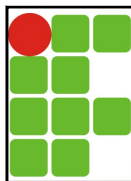
27



RMON2

- Um dos principais problemas da MIB RMON1 é o fato dele lidar apenas com informações de tráfego ao nível de enlace de rede
- **A MIB RMON2 torna cada monitor capaz de analisar e armazenar informações referentes às camadas 3 até 7 do RM-OSI**
 - MIB RMON2 -> RFC 4502
 - RMON2 pode analisar PDUs até a camada de aplicação

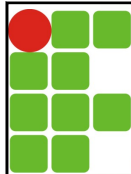
28



RMON2

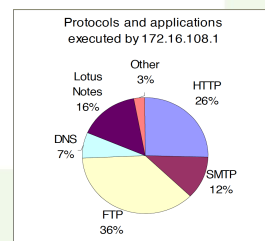
- Um monitor RMON2 pode monitorar tráfego com base no protocolo IP ou superiores, possibilitando assim a visualização de segmentos de rede além do qual ele está diretamente conectado
 - Um roteador pode, teoricamente, analisar e gerar estatísticas de todo tráfego vindo da Internet em direção a sua rede local

29

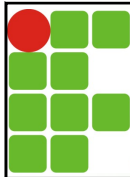


RMON2

- O monitoramento e geração de estatísticas no RMON2 também pode ser feito no nível de aplicação
- Exemplos:
 - Que serviços os usuários estão acessando;
 - Aplicações mais utilizadas;
 - Servidores mais acessados.



30

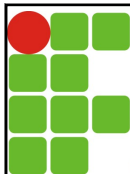


Histórico RMON2

■ Histórico

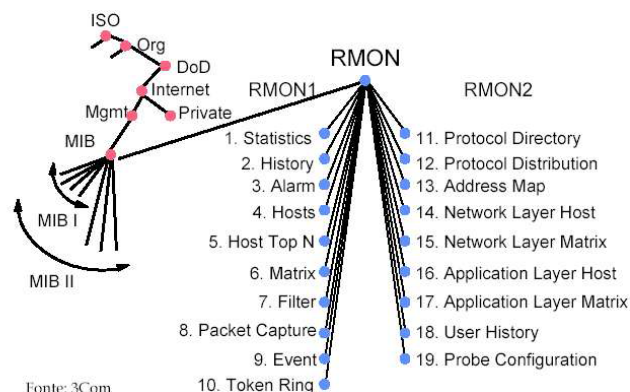
- Grupo de trabalho instituído pelo IETF em dezembro de 1994
- Novas e ampliadas funcionalidades
 - Possibilidade de selecionar pacotes tanto por seu endereço Ethernet quanto pelo endereço TCP/IP
 - Capacidade de filtro aumentada
 - Habilidade para rastrear protocolos (com campos de comprimento variável)
 - Possibilidade de efetuar decodificação nas 7 camadas

31



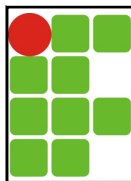
MIB RMON2

- A MIB RMON2 estendeu a MIB RMON adicionando um novo conjunto de grupos



Fonte: 3Com

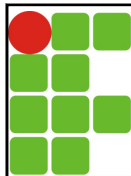
32



MIB RMON2

- **Protocol directory (11)**
 - Informações sobre os diversos protocolos analisados
- **Protocol distribution (12)**
 - Dados do tráfego apresentado por protocolo
- **Address map (13)**
 - Dados de mapeamento de endereços MAC em endereços de rede
- **Network layer host (14)**
 - Estatísticas de tráfego a nível de endereços de rede, num determinado host

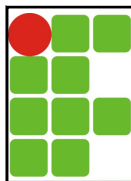
33



MIB RMON2

- **Network layer matrix (15)**
 - Estatísticas de tráfego de origem e destino no nível de endereços de rede
- **Application layer host (16)**
 - Estatísticas de tráfego a nível de aplicação, considerando entradas e saídas num determinado host
- **Application layer matrix (17)**
 - Estatísticas de tráfego de origem e destino no nível de aplicação

34



MIB RMON2

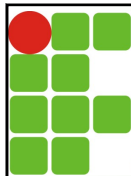
■ User history (18)

- Dados especificados pelo usuário (Gerente)
- Amostra periodicamente objetos especificados e armazena as informações

■ Probe configuration (19)

- Parâmetros operacionais de configuração do monitor RMON
- Exemplos
 - Data e Hora do agente;
 - Destino para envio de Traps.

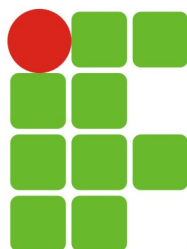
35



Referências

- LESSA, Demian – **O Protocolo de Gerenciamento RMON.** RNP – Boletim bimestral sobre tecnologia de redes, 1999. Disponível em:
<https://memoria.rnp.br/newsgen/9901/rmon.html>
- NETWORK WORKING GROUP. – **RFCs 2819 e 4502.** disponível em:
 - <https://www.ietf.org/rfc/rfc2819.txt>
 - <https://www.ietf.org/rfc/rfc4502.txt>

36



**INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE**



Gerência de Redes

Turma : 20172.5.01405.1N

RMON

Prof. Thiago Dutra <thiago.dutra@ifrn.edu.br>