Gerência de Redes de Computadores
RMON

Prof. Alex Furtunato

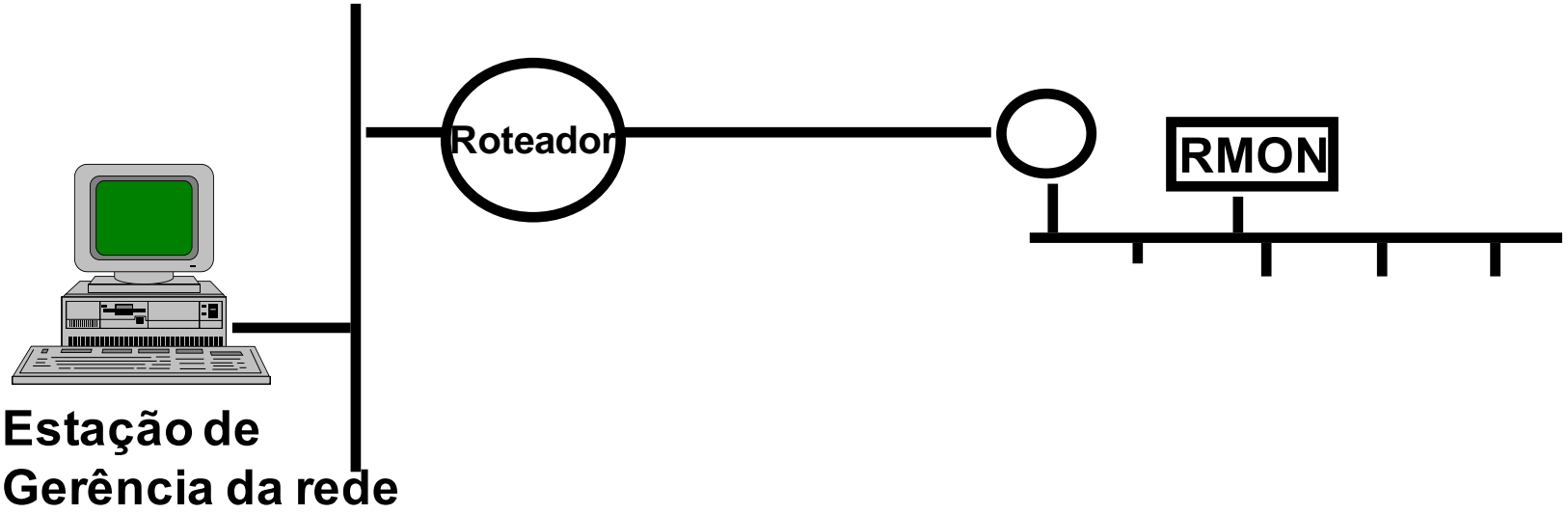
alex.furtunato@ifrn.edu.br

Limitações da MIB-II

- O gerenciamento é realizado em cada dispositivos individualmente
- 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 ser sobrecarregada
- Estatísticas geradas através dos dados colhidos podem ter problemas de precisão

MIB RMON

- RMON – Remote Monitoring
- Definida pela RFC 2819
- Apresenta mecanismos para um gerente configurar e controlar um monitor remoto, coletar seus dados e receber seus alarmes



Monitores

- São equipamentos e/ou softwares utilizados para observar e controlar uma determinada segmento de rede ou conjunto de dispositivos
- Também denominados PROBES
- Possuem independência. Em caso de falhas no gerente, continuam a coletar dados.
- Pode ser um dispositivo dedicado a captura de dados e a sua analise.
- O Monitor suporte a MIB II para poder ser monitorado e também dá suporte a MIB RMON para poder monitorar o segmento de rede

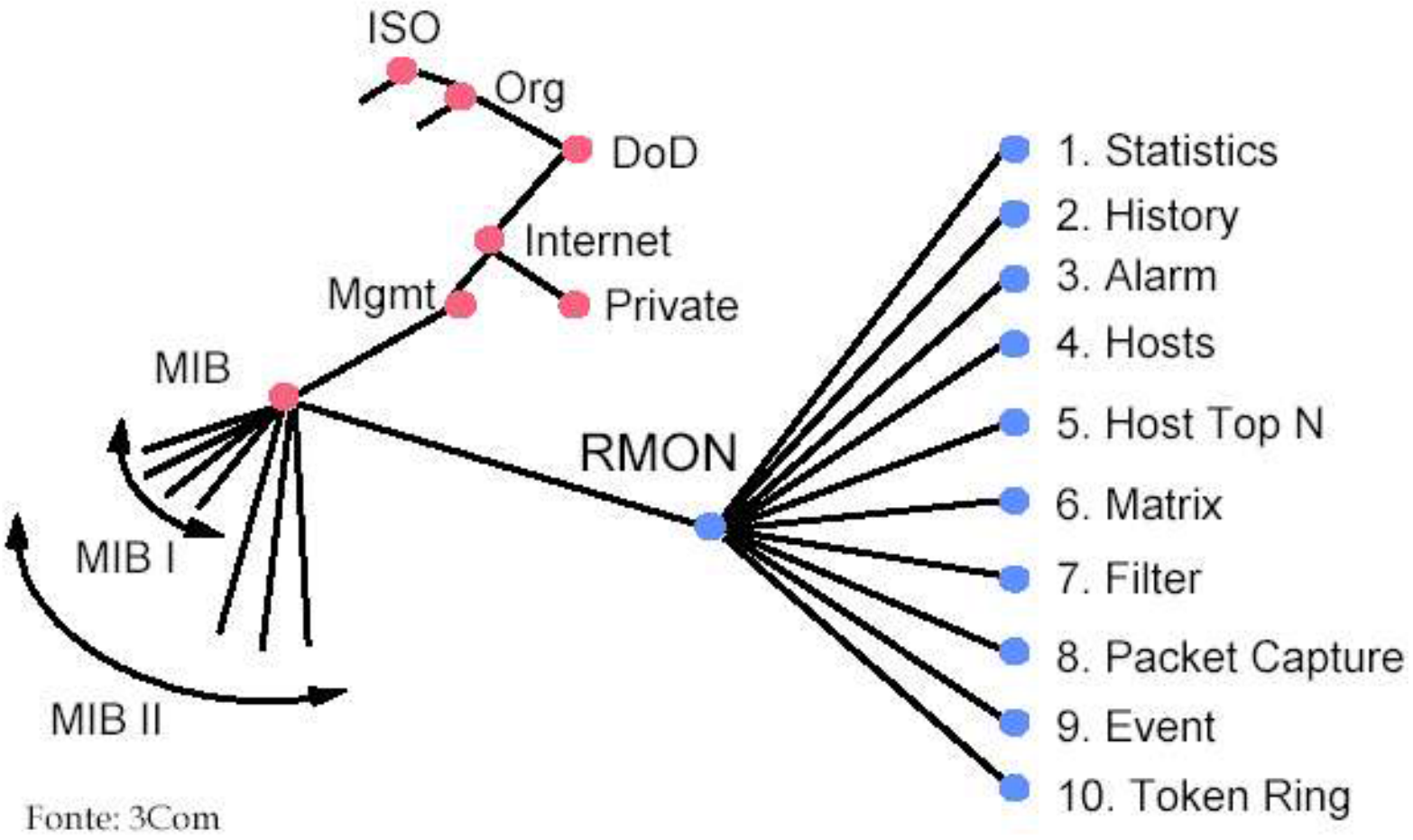
Metas RMON

- Extensão do SNMP que agrega novas funcionalidades
- Operação Offline
  - Coleta dados e acumula estatística
  - Recuperação posterior
  - Notificação de problemas
- Monitoração Pró-ativa
  - Diagnósticos
  - Log de performance de rede
  - Notificação em caso de exceção com dados para diagnóstico

Metas RMON

- Reconhecer condições de erro
- Determinar dispositivos que mais transmitem dados ou geram erros
- Permitir acesso de múltiplos gerentes

Árvore



Fonte: 3Com

Grupos RMON

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

Grupo de Statistics

- Contadores simples de tráfego (octetos, colisões, erros, broadcasts)
- Pacotes descartados
- Erros
  - Fragmentos
  - CRC
  - Undersize
  - Oversize
- Reduz o tráfego agente-gerente e carga de processamento no gerente
- SNMP recupera tabela inteira

Grupo de 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 tendência de comportamento de uma rede
- Tabelas
  - HistotyControlTable – Detalhes de amostragem
  - EtherHistoryTable – Dados amostrados

Grupo Hosts

- Contadores de tráfego relativas a host descobertos em um determinado segmento de rede monitorada
- Exemplos:
  - Número de bytes transmitidos e recebidos
  - Número de pacotes transmitidos e recebidos
  - Número de pacotes com erro transmitidos
- Tabelas
  - HostTable – Cada linha possue informações estatísiticas para cada host descoberto
  - HostControlTable – Tabela de controle do Monitor
  - HostTimeTable – Ordem relativa em que os Hosts foram descobertos

Grupo HostTopN

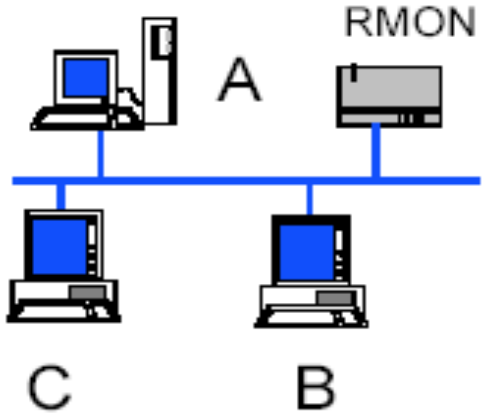
- Com base no grupo Hosts, apresenta estatísticas ordenadas em função de um determinado objeto
- Armazena tabela de hosts ordenados segundo os objetos: inPkts, outPkts, inOctets, outOctets, outErrors, outBroadcast e outMulticast
- Requer a configuração de tamanho da tabela resultante, intervalo de amostragem e Objeto de ordenação
- Requer a implementação do Grupo Hosts
- Exemplo:
  - 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.
- Tabelas
  - HostTopNTable – Cada
  - HostTopNControlTable

Grupo Matrix

- Estabelece tabelas com volume de tráfego entre pares de estação 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

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	——

Grupo Filter

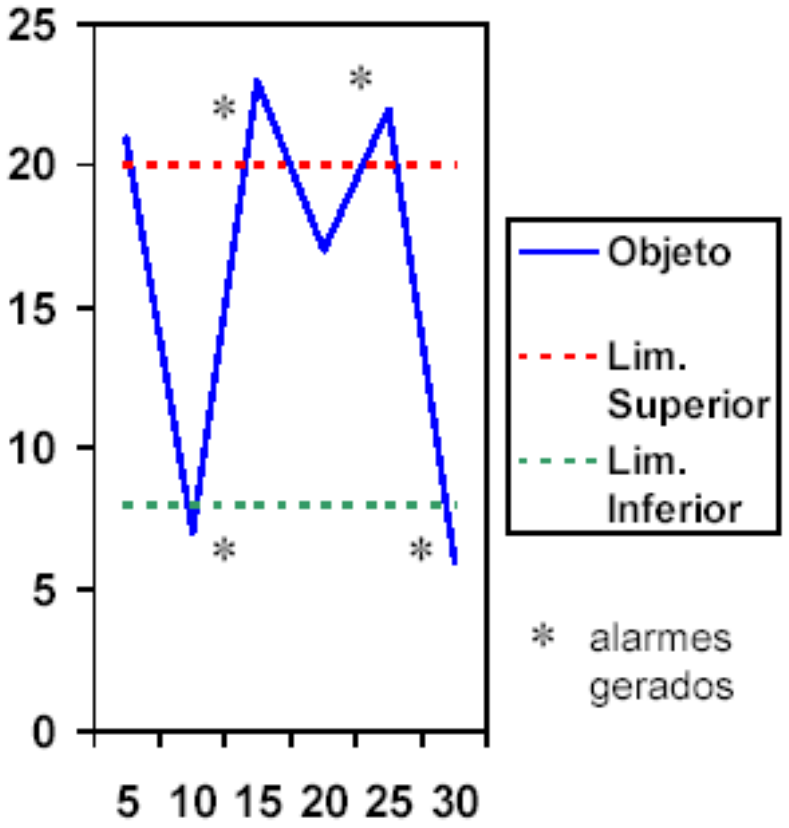
- Parâmetro que define critérios de filtragem de pacotes
- Se pacote atende às condições estabelecidas:
  - Captura o pacote ou
  - Registra estatísticas baseadas no mesmo
- Exemplo:
  - Filtra os pacotes que tenham como um destino o host A e não se originam no servidor
  - Filtra os pacotes IPX que possuem erros
  - Filtra os pacotes destinados ao servidor RARP

Grupo Capture

- Configuração e armazenamento dos resultados da filtragem feita pelo grupo Filter
- Requer a implementação do grupo Filter
- Parâmetros da captura:
  - Quantos bytes de cada pacotes serão armazenados?
    - Default é 100 primeiros bytes
  - Qual filtro determina os pacotes a serem capturados?
  - Qual o tamanho do buffer a ser utilizado?

Grupo Alarm

- Contém variáveis que devem ser vigiadas e relacionamentos com eventos que serão disparados
- Define limites que podem ser indicativos de problemas ou volta a normalidade
- Requer a implementaçao do grupo Event
- Exemplos:
  - Mais de 20 pacotes com erro nos últimos 5 minutos
  - Bytes enviados for menor que 100.000.000/5s



Grupo Event

- Define cada evento, seu tipo e a última ocorrência
- Normalmente 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

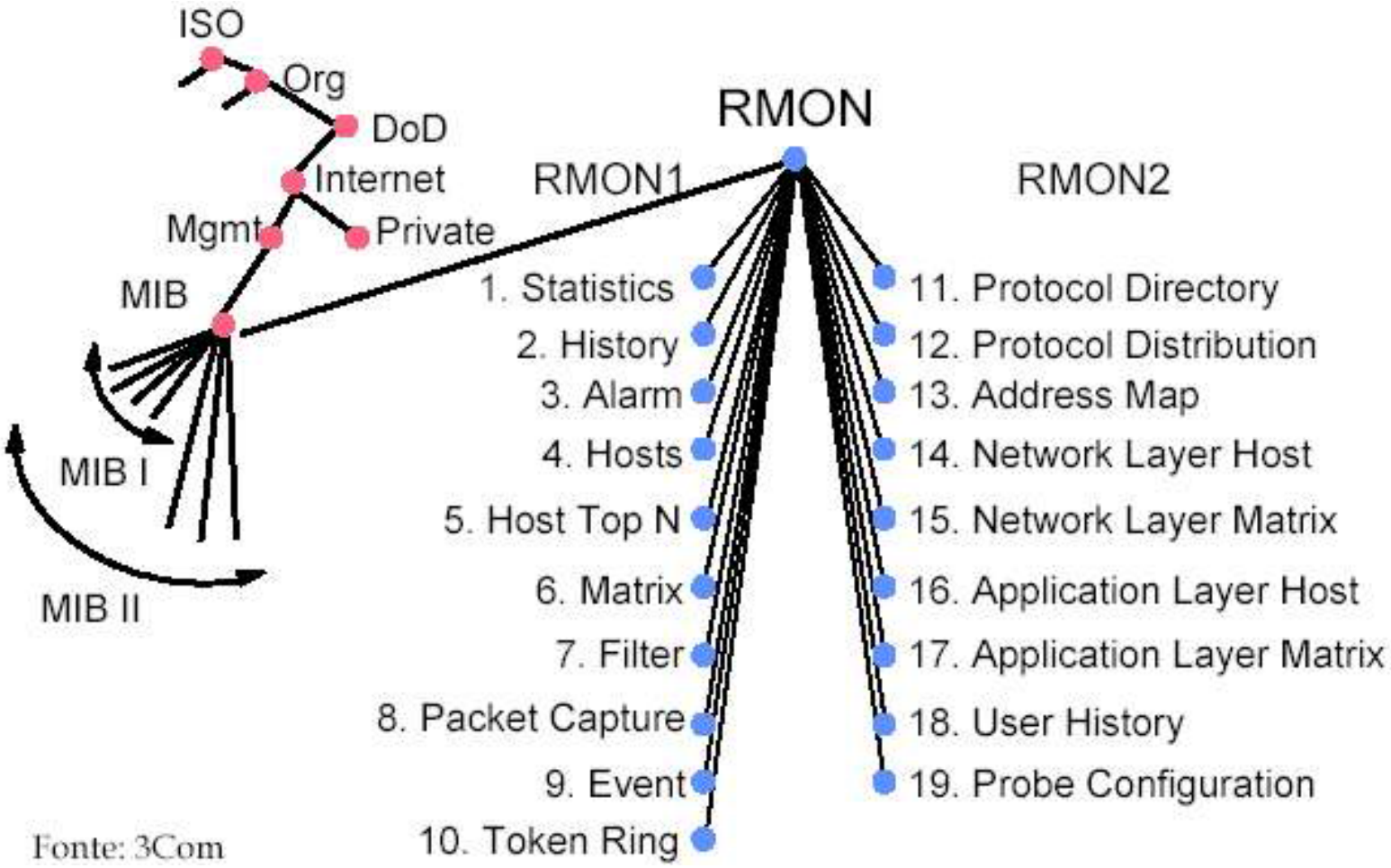
RMON 2

- RMON 1 basicamente lida com tráfego na camada de enlace (MAC)
- RMON 2 podem analisar PDUs em camadas superiores(até aplicação)
- Descrita pelo RFC 4502
- Com isso, podemos monitorar fenômenos com mais abragência
  - Aplicações mais utilizadas
  - Servidores mais acessados
  - Que serviços os usuários estão acessando

RMON 2

- 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

Árvore RMON 2



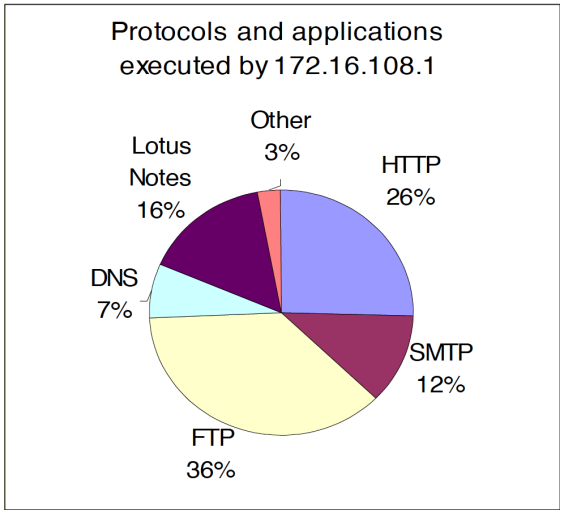
Fonte: 3Com

Grupos RMON 2

- 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

Grupos RMON 2

- Network layer matrix (15)
  - Estatísticas de tráfego de origem e destino, a nível de endereços de rede
- Application layer host (16)
  - Estatísticas de tráfego a nível de aplicação, considerando entradas e saídas num determinado host



Grupos RMON 2

- Application layer matrix (17)
  - Estatísticas de tráfego de origem e destino a nível de aplicação
- 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
  - Ex: Data e Hora do agente; Destino para envio de Traps