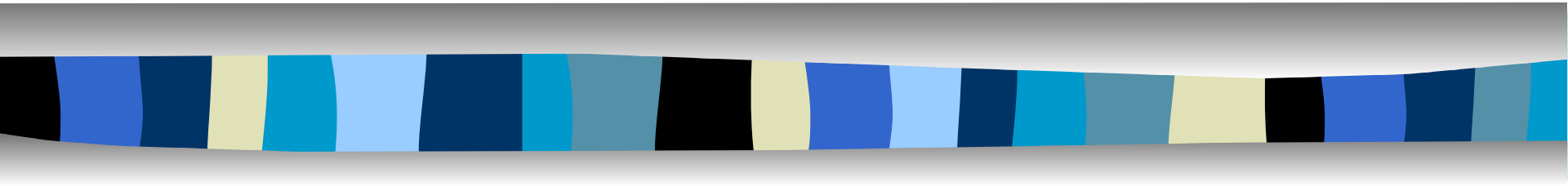
Gerência de Redes
Aula 05 - RMON

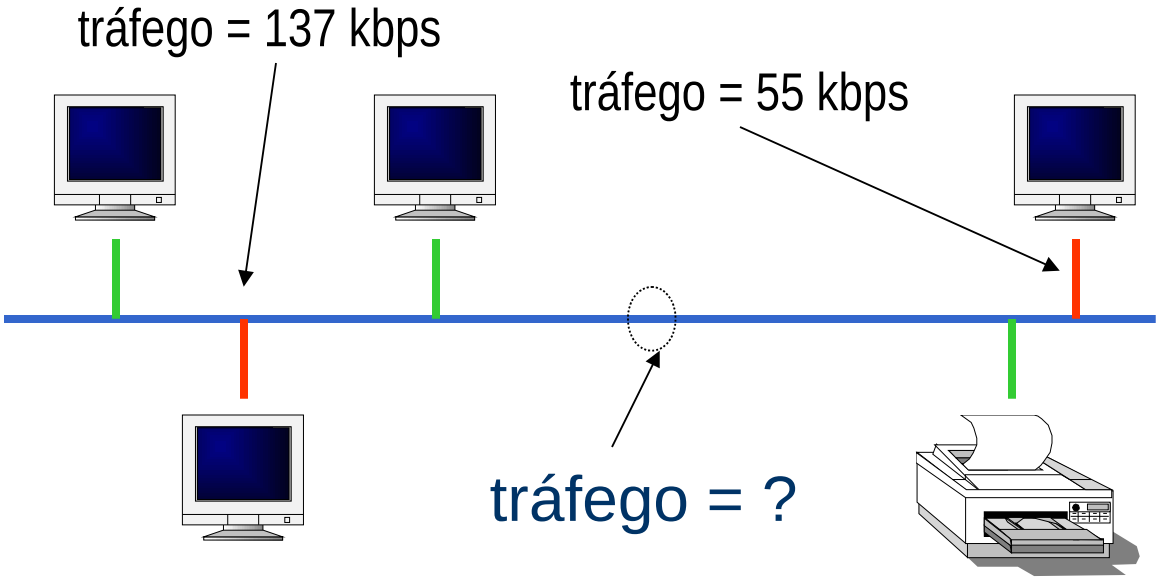


Prof. Carlos Maziero, PhD

DAINF – Departamento Acadêmico de Informática
UTFPR – Universidade Tecnológica Federal do Paraná

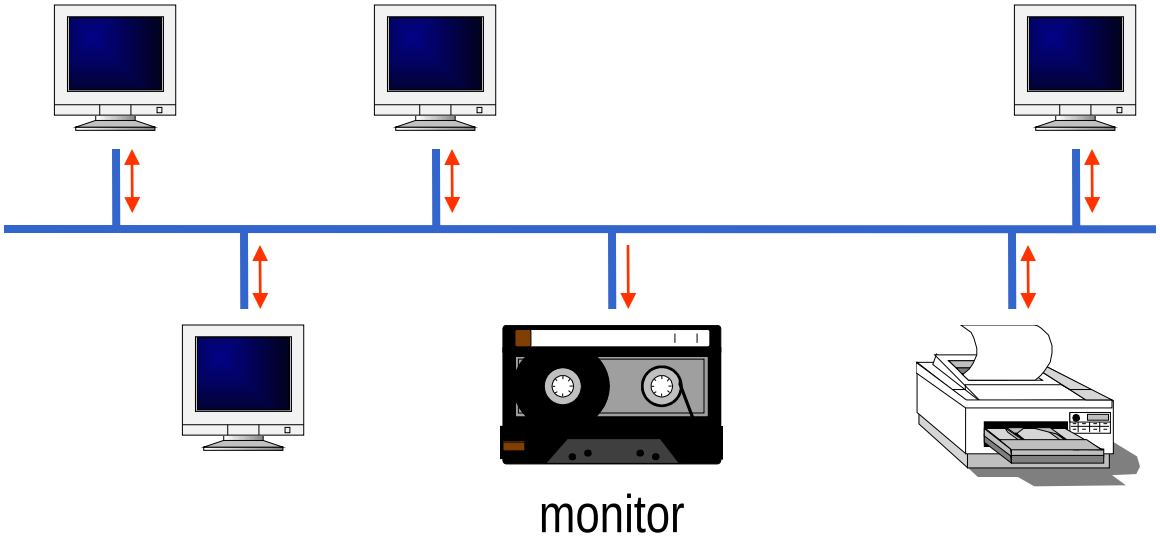
Monitoração de redes

- SNMP e MIBs em agentes só permitem analisar valores isolados (nos agentes)
- Como medir o tráfego na rede ?



Monitores de rede

- Ouvem a rede continuamente
- Podem ouvir várias redes
- Não interferem nas redes monitoradas

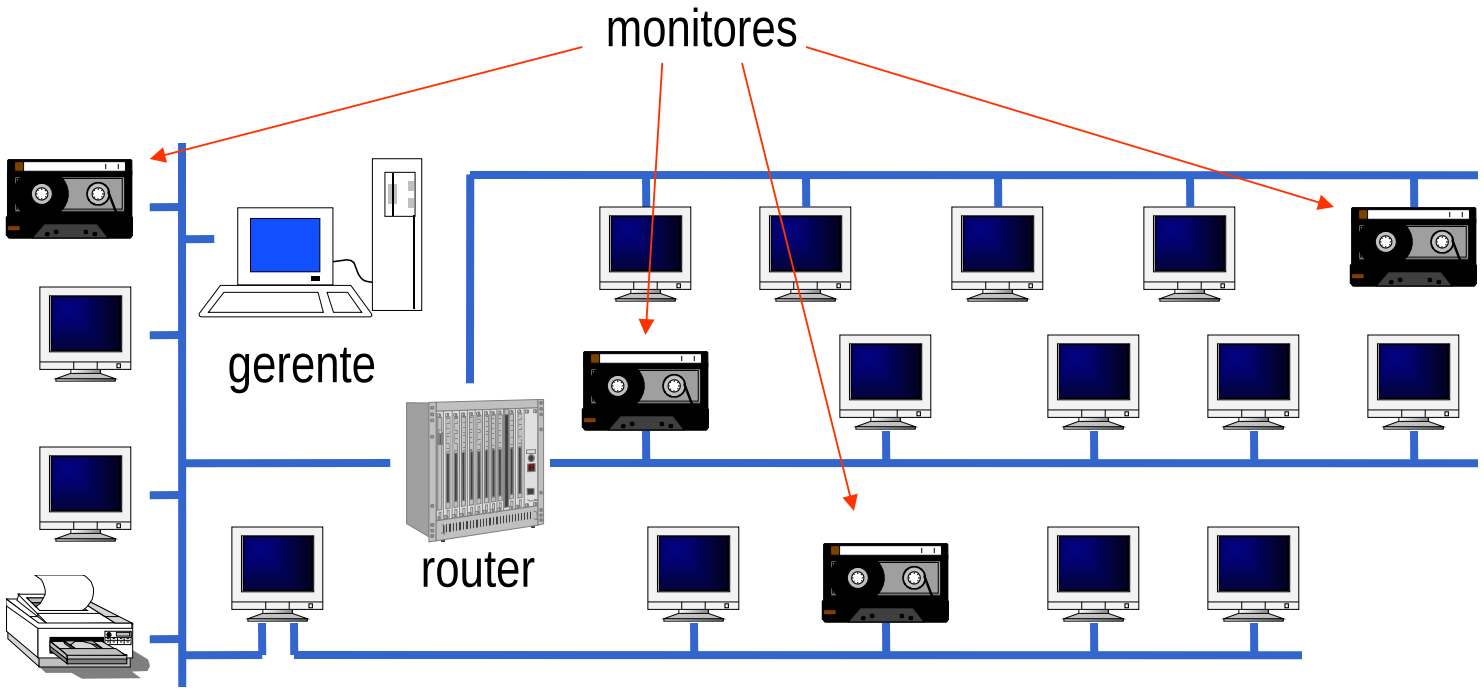


Informações monitoradas

- Todos os pacotes são ouvidos
- Podem ser aplicadas filtragens
  - tipo de pacote, protocolo, origem, destino, ...
- Produção de dados estatísticos
  - distribuição por tipo de pacote
  - percentual de colisões
  - taxas de transferência
- Armazenagem de pacotes para análise

Monitorando múltiplas redes

- Um monitor para cada sub-rede
- Monitores devem ser acessíveis pelo gerente



Definindo um monitor

- Definir a informação a armazenar
  - significado dos dados
  - tipos dos dados
  - estrutura geral da informação
- Definir formas de acesso
  - leitura/escrita
  - configuração
  - relatar eventos
- Implementar
  - como um dispositivo dedicado
  - serviço adicionado a um elemento da rede

RMON

- RMON: Remote Monitoring

- Norma para monitores de redes
- Define uma (imensa) MIB
- Dados são acessados via SNMP
- Efetua a monitoração contínua de redes
- Versões:
  - RMON v1: monitoração MAC (ethernet, token ring, ...)
  - RMON v2: monitora camadas mais elevadas
- Monitor: agente RMON ou sonda RMON

Objetivos de RMON

- Operação off-line
  - autônoma (independe do gerente)
  - diminui o tráfego de rede
- Monitoração pró-ativa
  - diagnósticos contínuos
  - monitoração de desempenho
  - pode gerar alarmes enviados ao gerente

Objetivos de RMON (2)

- Informações de valor agregado
  - dados estatísticos
  - informações históricas
- Acesso por múltiplos gerentes
  - diferentes objetivos de gerência
  - tolerância a falhas
- Compatibilidade com padrões
  - informação na forma de MIBs
  - acesso via protocolo SNMP

Controle da sonda RMON

- Monitor é acessado remotamente para:
  - configuração geral
  - invocação de ações
- Configuração:
  - indicar tipo e forma dos dados a coletar
  - manipulação de tabelas de controle
- Ações:
  - leitura e escrita de valores
  - invocação de "*value triggered commands*"

Organização da MIB RMON

- Cada grupo consiste de:
  - uma ou mais tabelas de dados (*read-only*)
  - uma ou mais tabelas de controle (*read-write*)
- Tabelas de dados:
  - valores coletados da rede e processados
- Tabelas de controle
  - indicam que dados devem ser coletados
  - cada linha representa uma função de coleta
- Podem ser fundidas em uma só tabela

Múltiplos gerentes

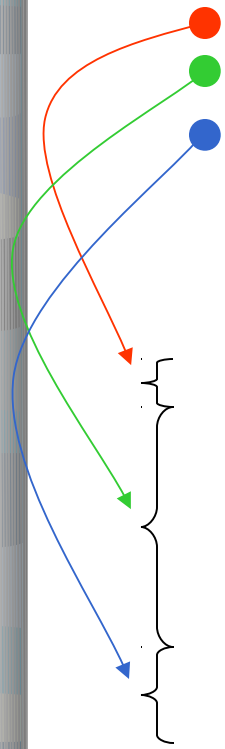
- Vários gerentes podem acessar uma sonda
  - acessos concorrentes podem saturar a sonda
  - um gerente pode monopolizar a sonda
- Para o controle de múltiplos gerentes:
  - cada linha da tabela de controle possui um *owner*
  - propriedade: IP do gerente, localização, telefone, ...
  - informação de propriedade não limita o acesso
  - o monitor pode ser proprietário de algumas linhas

Gerência de tabelas

- Complexo e pouco claro (Stallings 96 !)
  - Inserção e remoção de linhas nas tabelas de controle
- Cada linha de tabela de controle possui:
  - OwnerString: o proprietário da linha de controle
  - EntryStatus: situação daquela linha:
    - valid
    - create request
    - under creation
    - invalid
  - Demais informações

Indexação de tabelas

xyzControlTable



xyzControlIndex	xyzControlParameter	xyzControlOwner	xyz

xyzDataTable

XyzDataControlIndex	XyzDataIndex	xyzDa
1	1	
2	1	
2	2	
2	3	
2	4	

Inserção de linhas

- Através do método SNMP set:

```
set [index, (tipo, valor), (tipo, valor), ...]
```

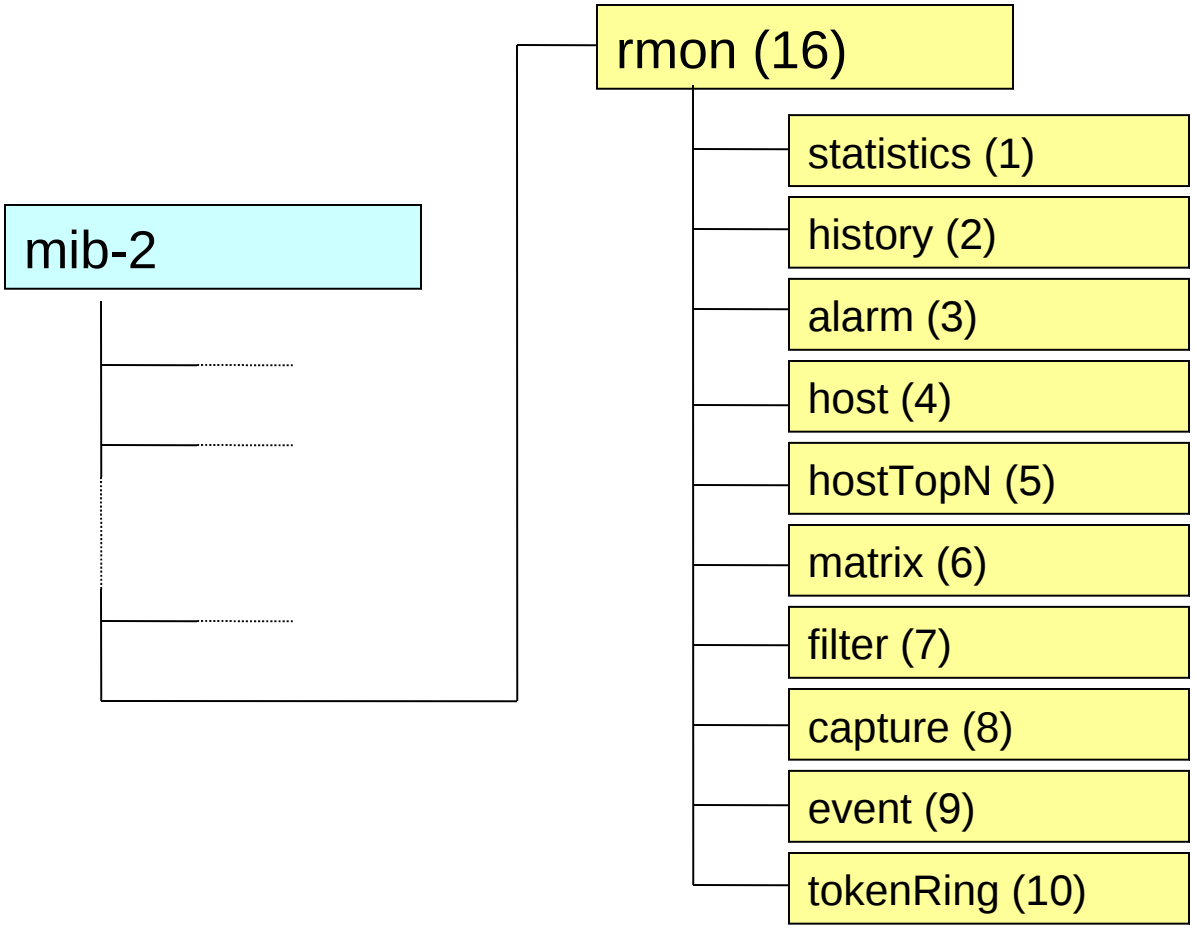
- erro *badValue* em caso de dado inválido ou impossibilidade de criação

- tratamento de conflitos em acessos simultâneos torna-se necessário

Passos para a criação de linhas

- Sequência de passos para criar linhas:
  1. se a linha solicitada não existe (índice inexistente), ela é criada e seu status recebe o valor "*createRequest*";
  2. imediatamente após a criação o monitor muda o status da linha para "*underCreation*";
  3. as novas linhas permanecem nesse estado até o gerente terminar de criar todas a linhas desejadas;
  4. ao final o gerente seta o campo de status das linhas criadas por ele para o valor "*valid*";
  5. tentativas de criar linhas cujos índices já existem resultam em erro.

A MIB RMON


rmon (16)
statistics (1)
history (2)
alarm (3)
host (4)
hostTopN (5)
matrix (6)
filter (7)
capture (8)
event (9)
tokenRing (10)
mib-2

Grupo *statistics*

- Uma tabela para cada sub-rede monitorada
  - sub-rede referenciada por sua interface
- Informações mais importantes:
  - carga da sub-rede
  - saúde da sub-rede (erros, colisões)
  - pacotes fora de tamanho (*undersize*, *oversize*)
- Mais detalhado que mib-2.interfaces

Grupo *history*

- Amostragens do tráfego nas interfaces ao longo do tempo de operação
  - Cada linha da tabela de controle define um conjunto de amostras
  - Cada linha da tabela de dados corresponde a uma amostra

- Defaults:
  - cada amostra dura 1800 segundos
  - as 50 últimas amostras são mantidas

Outros grupos

- hosts
  - estatísticas sobre hosts na sub-rede
- hostTopN
  - estatísticas sobre hosts segundo algum critério
  - armazena dados sobre os N primeiros hosts em termos de tráfego, erros, tipos de pacotes, etc.
- matrix
  - armazenar dados sobre tráfego entre pares de hosts
- tokenRing
  - suporte a informações de redes *token-ring*

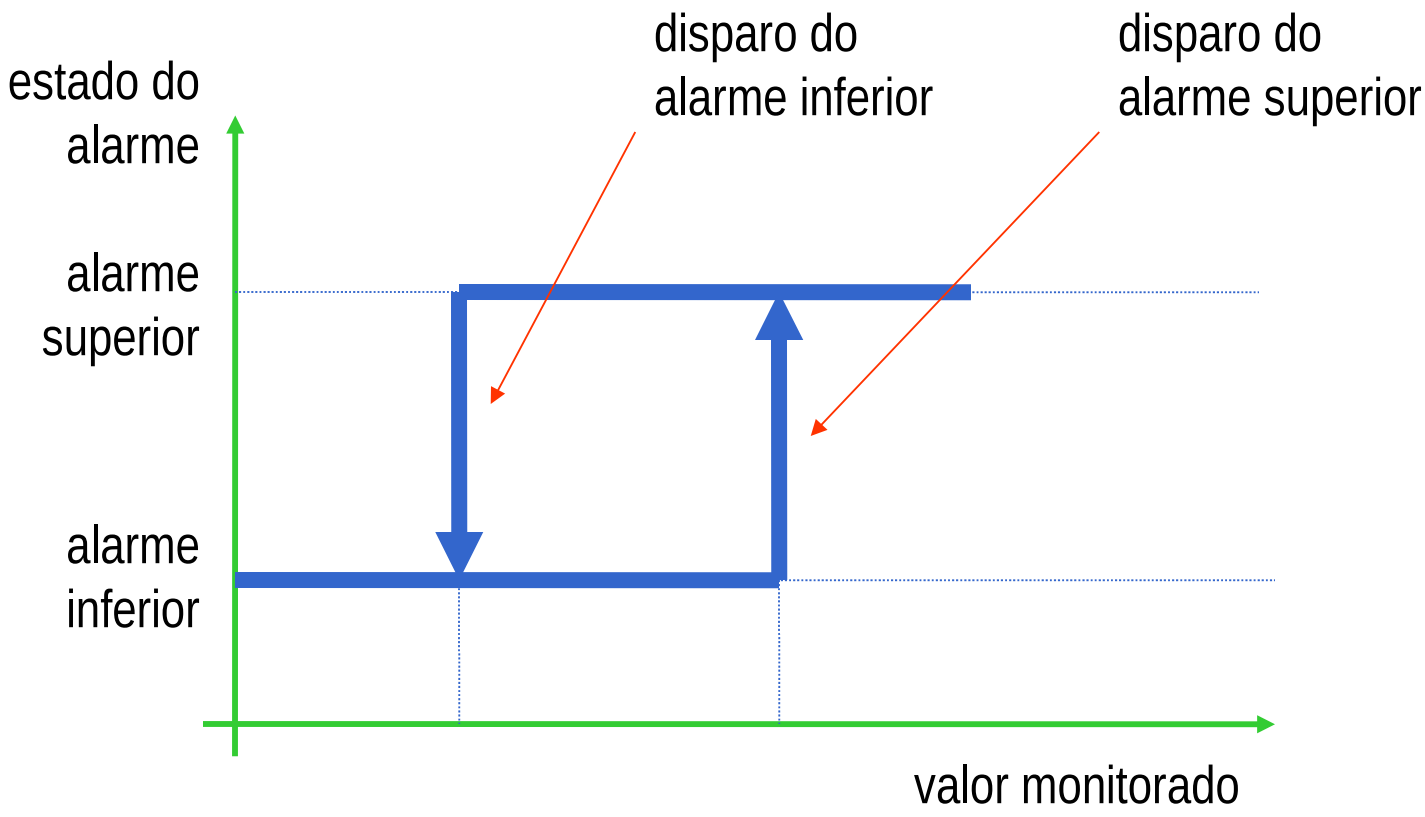
Alarmes

- Alarmes são registrados na MIB
  - gerados pelo grupo *alarm*
  - tratados pelo grupo *event*
  - podem ser enviados ao gerente via *traps*
- Cada entrada da tabela contém:
  - OID da variável a ser monitorada
  - intervalo de amostragem
  - parâmetros de limiar (*threshold*)
- Um exemplo:
  - + de 500 erros CRC nos últimos 5 minutos

O ciclo de histerese

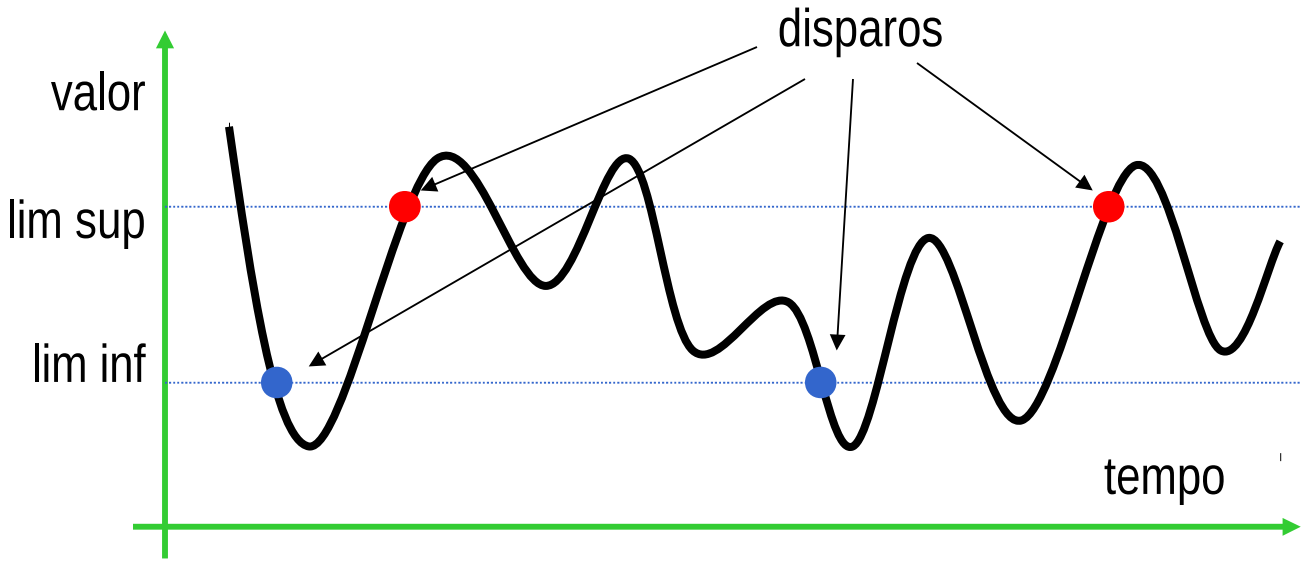
- Pequenas flutuações no valor monitorado poderiam gerar alarmes
  - excesso de alarmes sem utilidade
- Usa dois limiares de disparo do alarme:
  - inferior: valor mínimo em condições normais
  - superior: valor máximo em condições normais
- Gerar alarmes somente quando:
  - valor ultrapassar o limite superior
  - valor descer abaixo do limite inferior
  - de forma alternada !

O ciclo de histerese



Geração de alarmes

- Alarme é gerado quando:
  - valor maior que o limiar superior (*risingThreshold*)
  - valor menor que o limiar inferior (*fallingThreshold*)



O grupo *filter*

- Permite regras de filtragem dos pacotes
  - dois tipos de filtros:
    - *data filter*: padrões de bits nos pacotes
    - *status filter*: status dos pacotes (válido, erro de CRC, ...)
  - filtros podem ser combinados
    - operações lógicas AND, OR, seqüências
- Os pacotes filtrados:
    - constituem um fluxo chamado canal (*channel*)
    - podem disparar eventos
    - podem ser armazenados no grupo *capture*

Considerações práticas

- Uso correto da sonda e do gerente
  - evitar uso abusivo de alarmes e eventos
  - uso inteligente de filtros e captura
  - risco de saturar a sonda e a rede
  - poder de processamento da sonda é limitada

- Problemas de interoperabilidade
  - discrepância entre MIBs de fabricantes distintos
  - muitas funções são parcialmente implementadas

RMON v2

- RMON v1:
  - limitado à camada MAC
  - ethernet e token-ring
  - poucos recursos de configuração
- RMON v2:
  - suporte às demais camadas (3 a 7)
  - monitoração de protocolos de aplicação
  - visibilidade de tráfego vindo de fora (IP)
  - tabelas replicadas para cada protocolo
- Outras inovações
  - grupo MIB de configuração da sonda