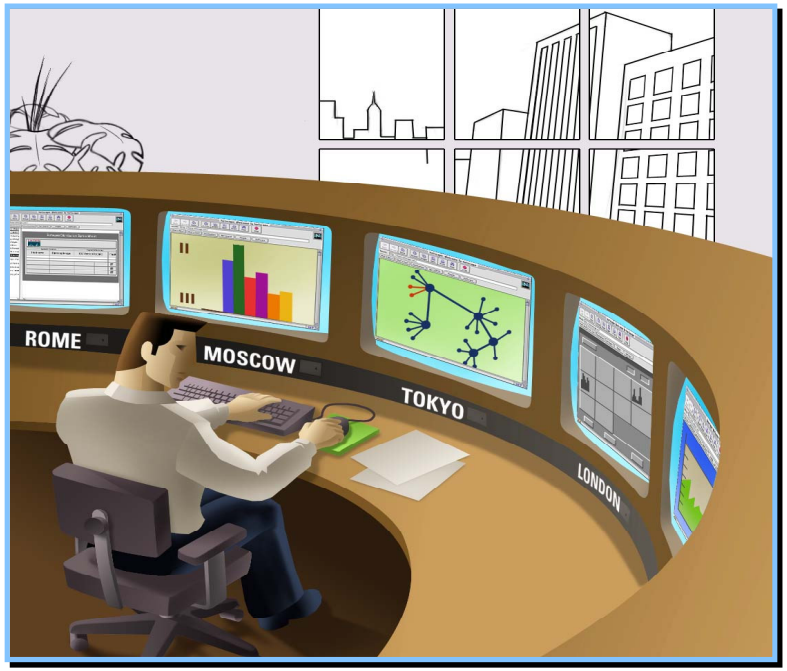
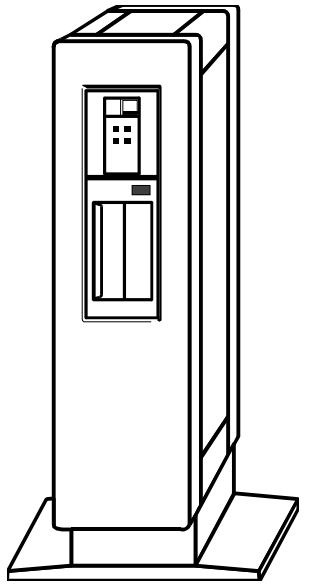
Gerenciando hosts e serviços

Liane Tarouco



Gerenciamento de hosts

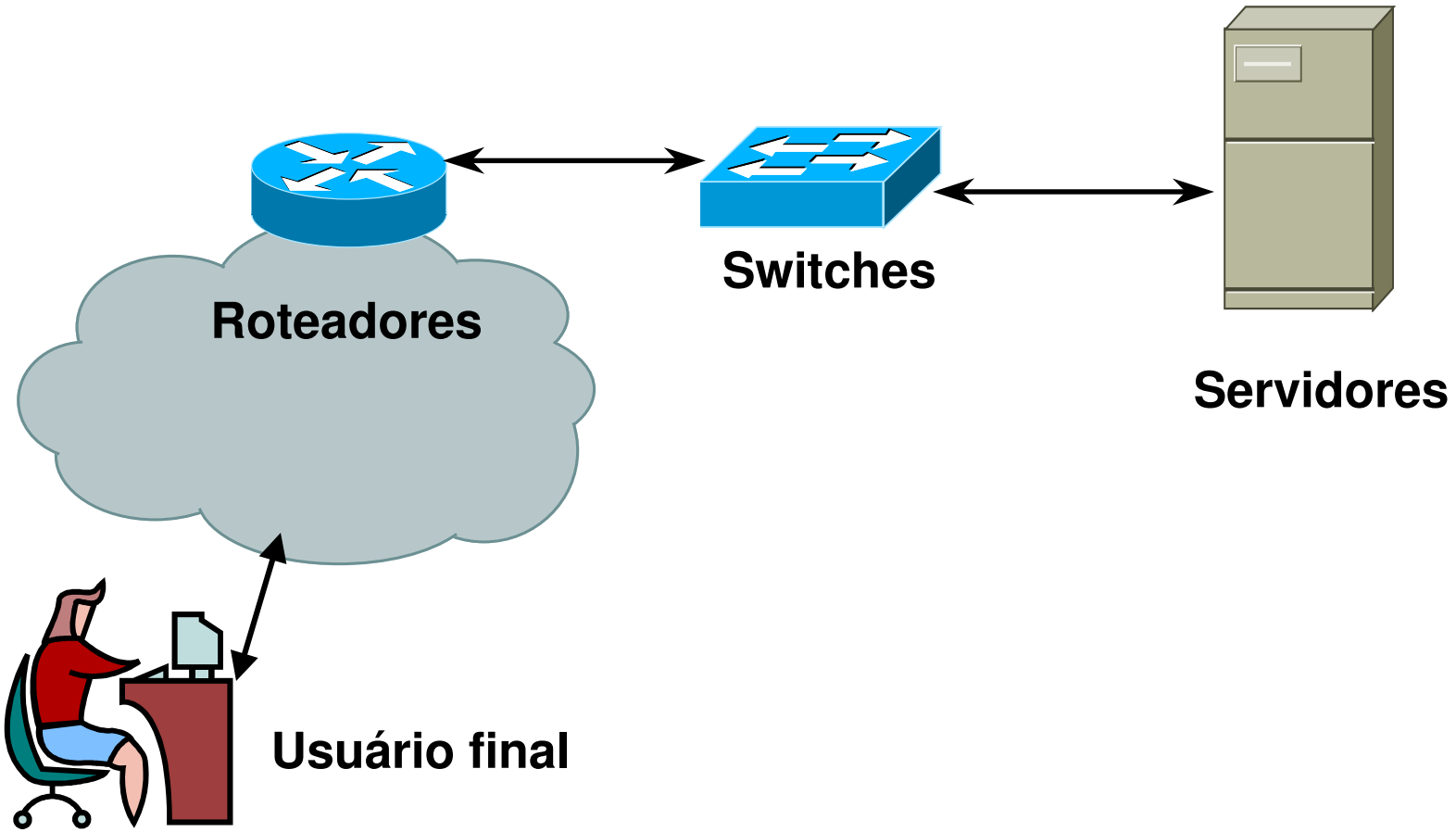
- Hosts representam parcela relevante no tempo de atendimento
- Precisam ser apropriadamente
  - configurados (planejamento de capacidade)
  - protegidos (segurança)
  - monitorados (contabilização de uso e gerenciamento pró-ativo)



Applications are important!

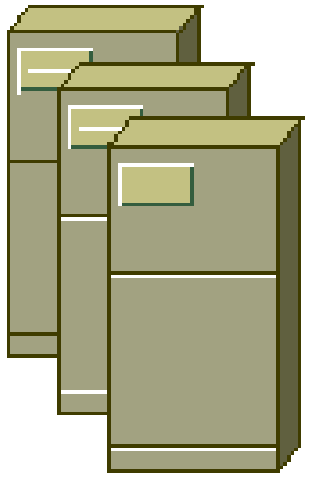
- According to recently published industry analyst reports, applications, more than any other components of an infrastructure, are responsible for downtime in critical business systems
- As a result, managing the availability and performance of your critical business applications has become more important than ever

Elementos envolvidos

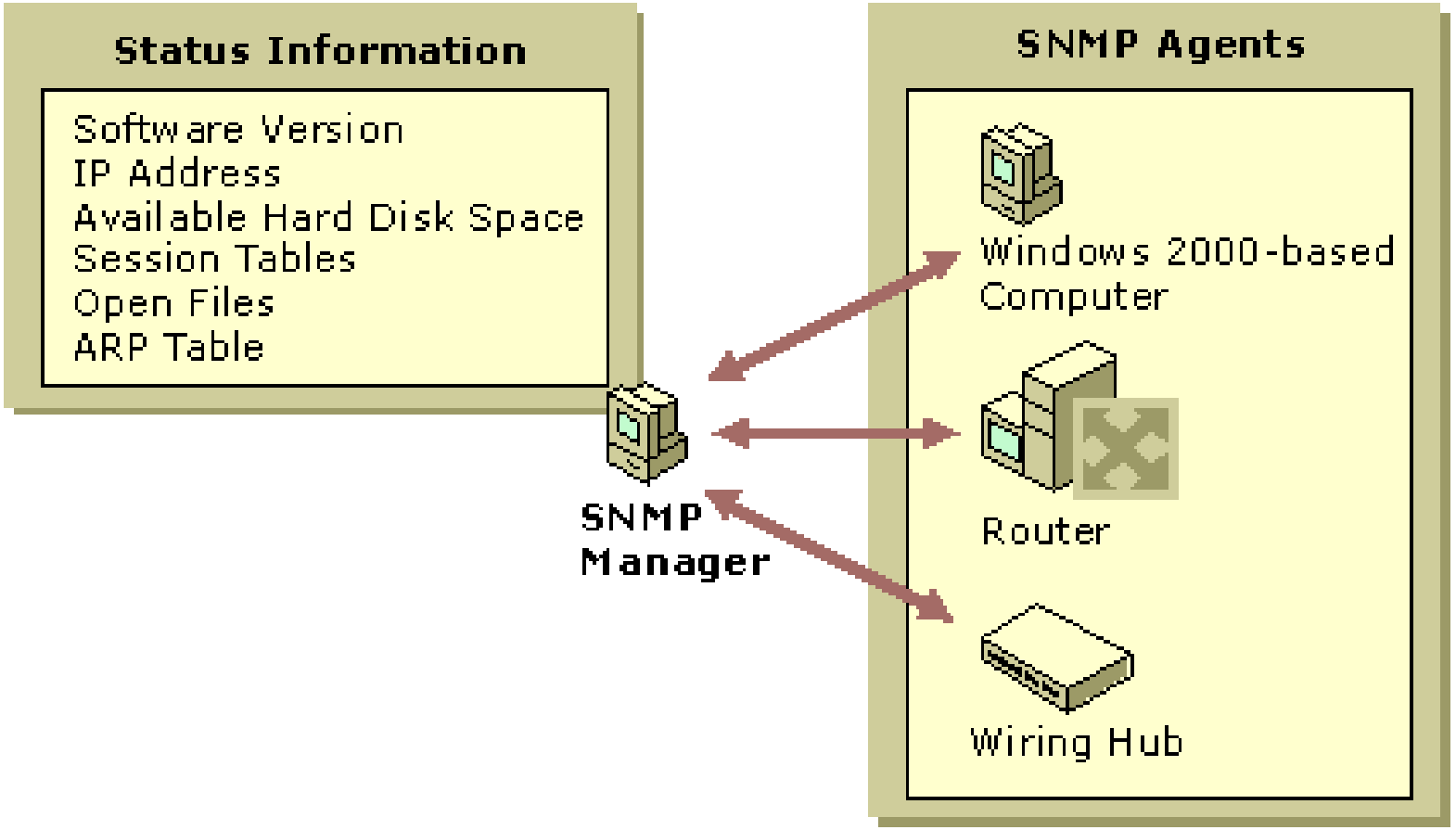


Host

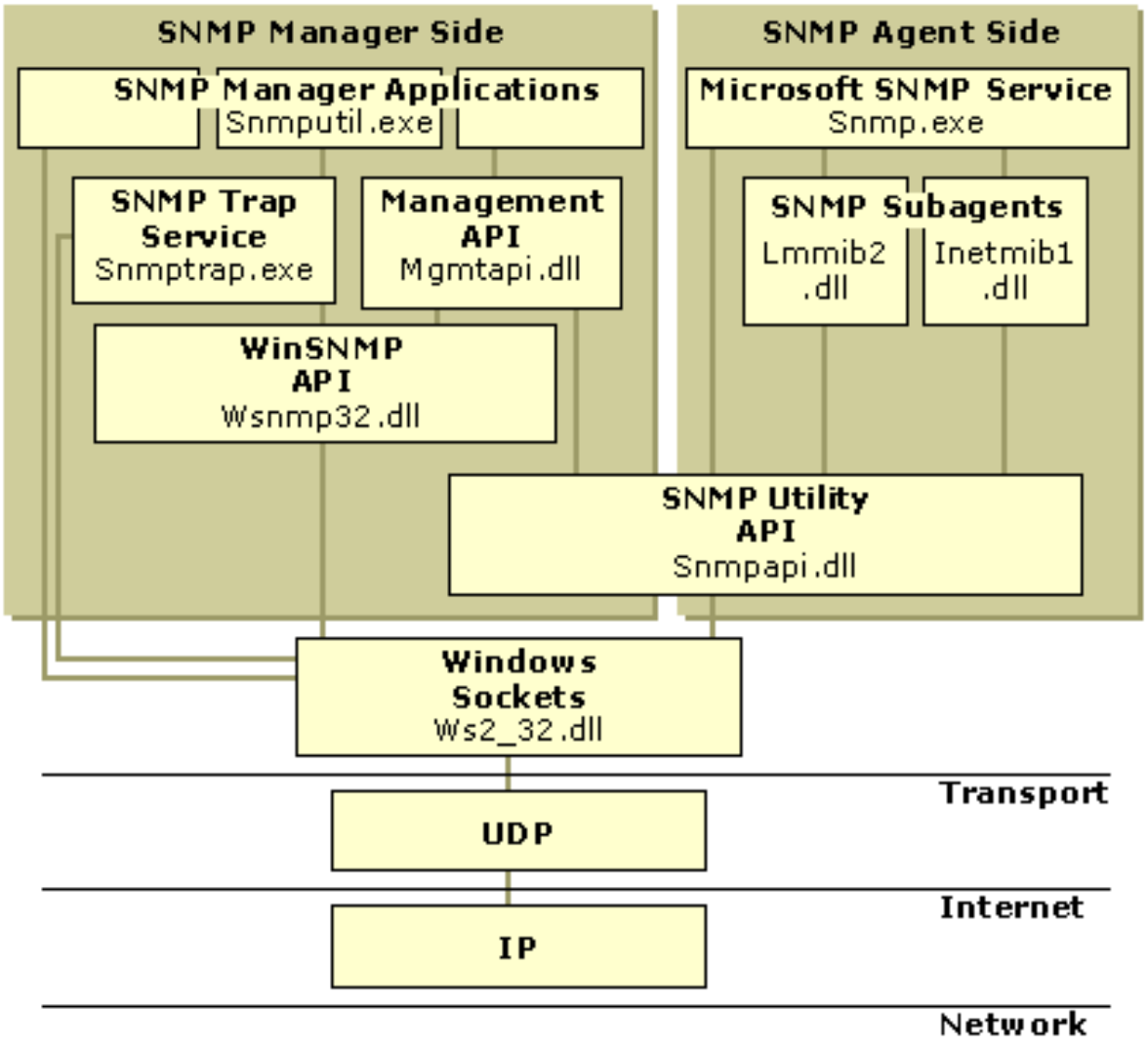
- O termo "host" implica em um computador qualquer que comunica-se com outros computadores interligados via Internet e é diretamente utilizado por usuários humanos.



Gerenciando tudo

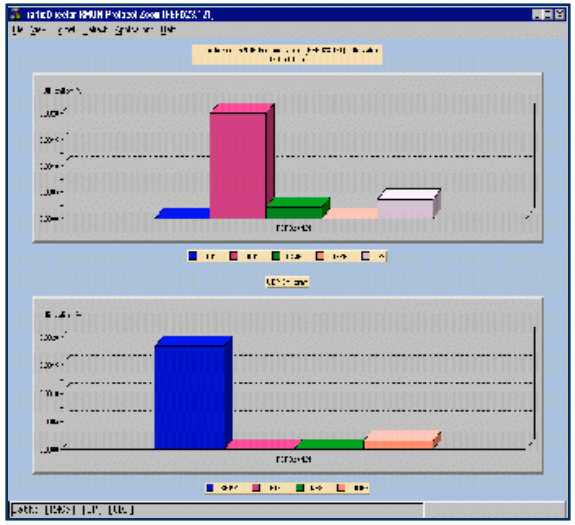


Windows 2000 SNMP Architecture



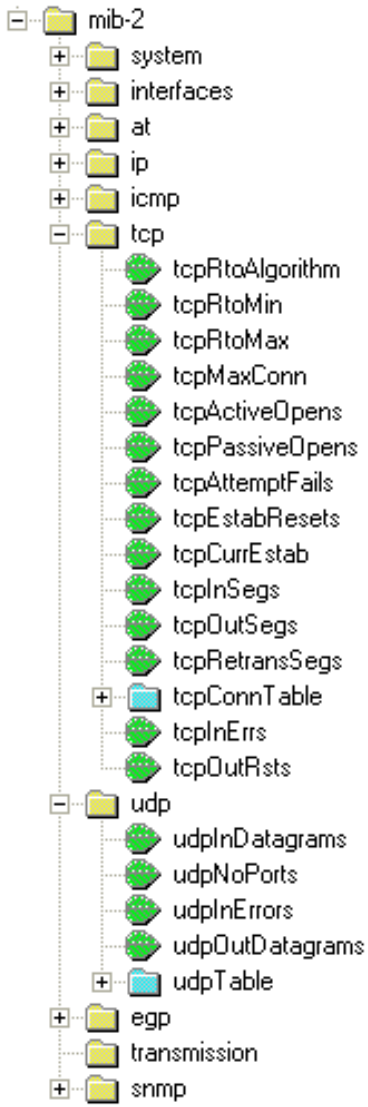
Aplicações críticas precisam ser preservadas

- É preciso monitorar as aplicações críticas e conter em tempo degradações de serviço isolando aplicações, segmentos de rede ou prevenindo uso frívolo da rede



Dados básico que podem ser obtidos da MIB II

- Grupo TCP
- Grupo UDP

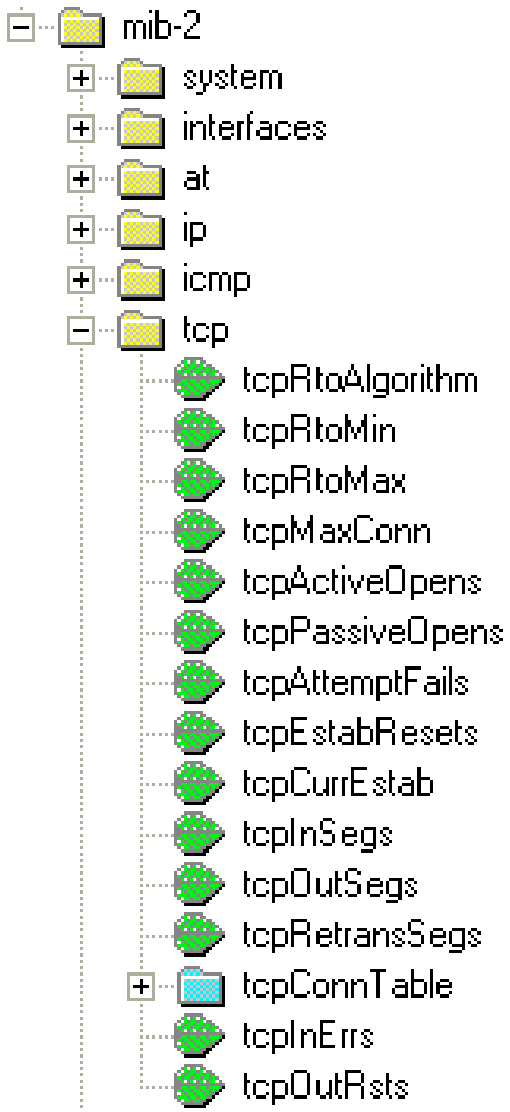


Grupo TCP - gerenciamento de configuração

Objeto	Informação usada para gerenciamento de configuração
tcpRtoAlgorithm	algoritmo utilizado para determinar o "time out" de retransmissão de octetos TCP não confirmados
tcpRtoMin	valor mínimo permitido para o "time-out"de retransmissão TCP, em milissegundos
tcpRtoMax	valor máximo permitido para o "time-out"de retransmissão TCP, em milissegundos
tcpMaxConn	limite de conexões que podem se abertas pela entidade de transporte do dispositivo
tcpCurrEstab	número de conexões de transporte corretamente abertas

Gerenciamento de performance e limites

- O objeto tcpMaxConn ajuda a configurar a rede para suportar o número de conexões TCP remotas necessárias.
- Este número pode ser calculado observando-se o objeto tcpCurrEstab que informa o número de conexões TCP estabelecidas no momento.



Gerenciamento de performance

Objeto	Informação usada para gerenciamento de performance
tcpAttempt Fails	número de tentativas de conexao falhadas
tcp EstabResets	número de reinicializacoes de conexoes estabelecidas
tcpRetransSegs	número de segmentos retransmitidos
tcpInErrs	número de pacotes recebidos com erro
tcpOutRsts	número de vezes que a entidade tentou reinicializar uma conexao
tcpInSegs	taxa de segmentos TCP recebidos
tcpOutSegs	taxa de segmentos TCP enviados

Observações sobre os objetos do grupo TCP

- **tcpAttemptFails** - confiabilidade da rede
  - um número menor de falhas indicam uma rede mais confiável.
- **tcpEstabResets** - confiabilidade da rede, sendo que quanto maior o número de conexões estabelecidas reinicializadas, menos confiável é a rede.

Observações sobre os objetos do grupo TCP

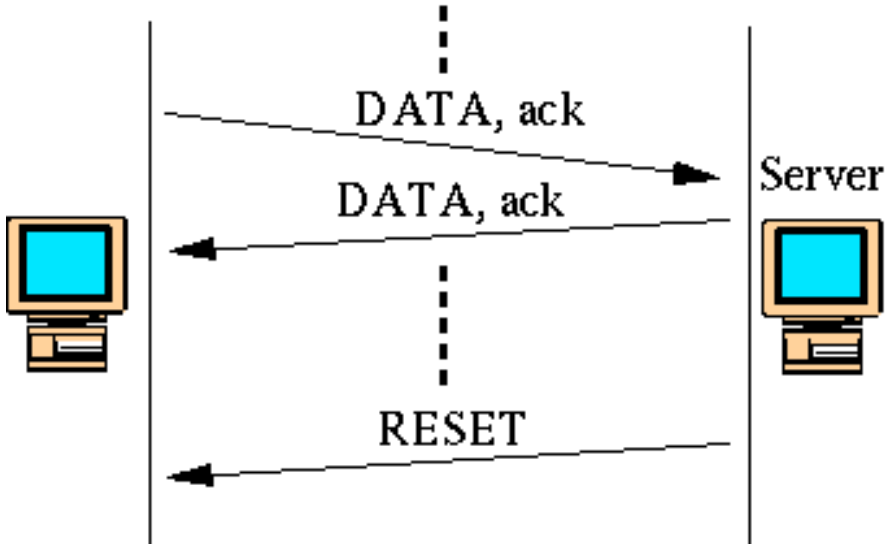
- **tcpRetransSegs** - informa o número de segmentos TCP que o sistema está retransmitindo, esta informação pode indicar se uma entidade está tendo que fazer várias retransmissões para garantir a confiabilidade.

Observações sobre os objetos do grupo TCP

- **tcpInErrs** - número de segmentos recebidos com erro.
  - O aumento deste objeto pode ser causado pelo encapsulamento incorreto dos segmentos pelo sistema de origem, alguma rede repassando os segmentos com erro, ou outras razões.

Observações sobre os objetos do grupo TCP

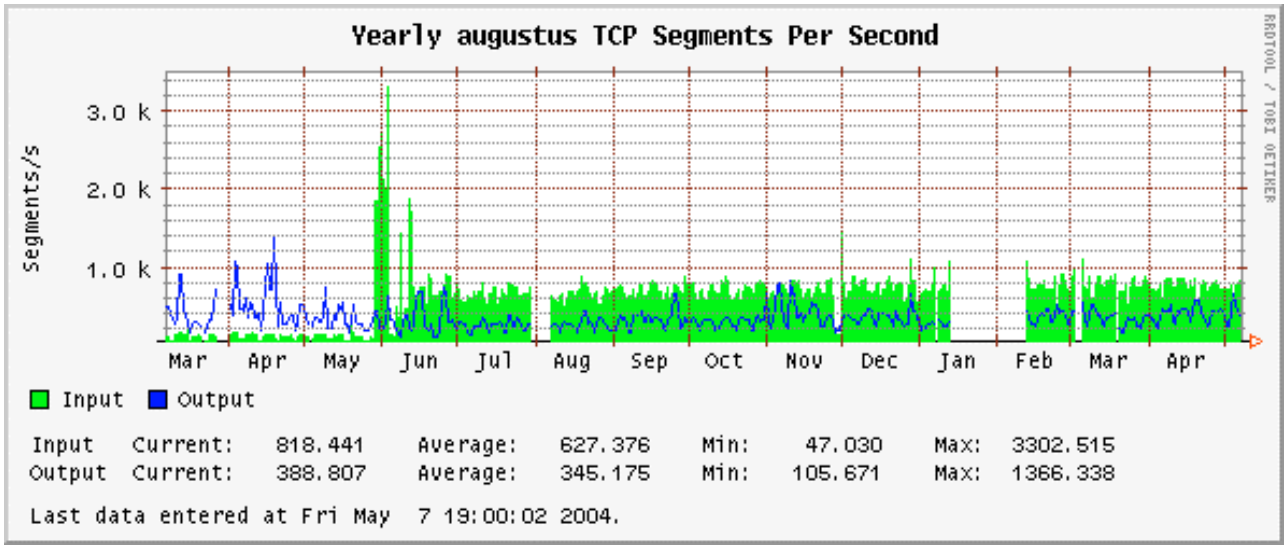
- **tcpOutRsts** - número de vezes que a entidade tentou reinicializar uma conexão.



Quais as causas de um reset?

Observações sobre os objetos do grupo TCP

- **tcpInSegs** e **tcpOutSegs** permitem a contabilização da taxa de segmentos TCP que entram e saem da entidade.

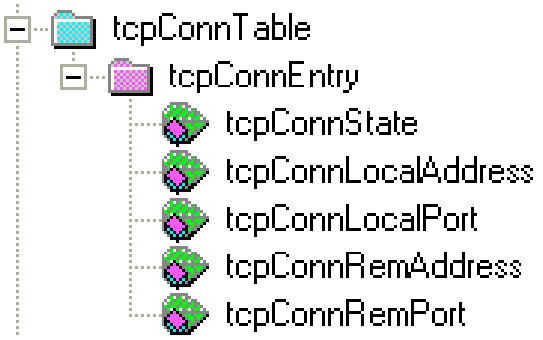


Gerenciamento de contabilização

Objeto	Informação usada para gerenciamento de contabilização
tcpActiveOpens	número de vezes que o sistema abriu uma conexão
tcpPassiveOpens	número de vezes que o sistema recebeu um pedido de abertura de conexão
tcpInSegs	número total de segmentos TCP recebidos
tcpOutSegs	número total de segmentos TCP emitidos
tcpConnTable	tabela das conexões TCP correntes

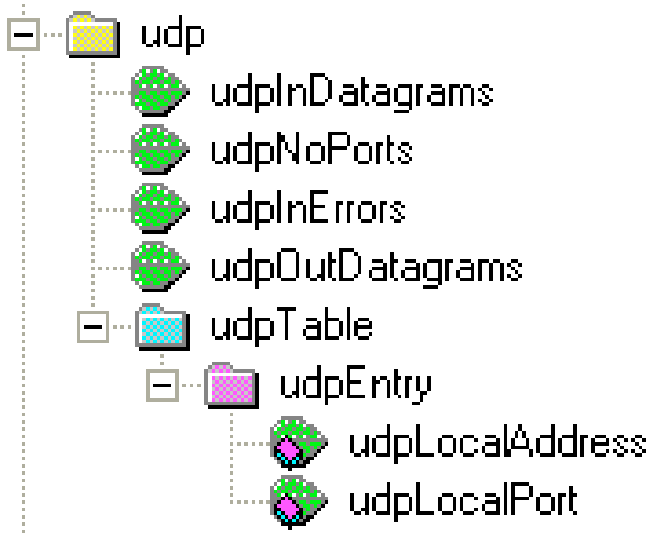
Gerenciamento de segurança

- As informações da tabela tcpConnTable também podem ser usados para gerenciamento de segurança, pois permite o conhecimento dos sistemas que acessam recursos via TCP.



- O tempo de polling influenciará grandemente na eficiência do gerenciamento, pois um intruso pode levar apenas alguns segundos para pegar as informações que deseja e fechar a conexão.
  - Se nenhum poll for feito neste intervalo, o intruso não será detectado.

Grupo UDP



- Objeto — Informação usada para gerenciamento de performance

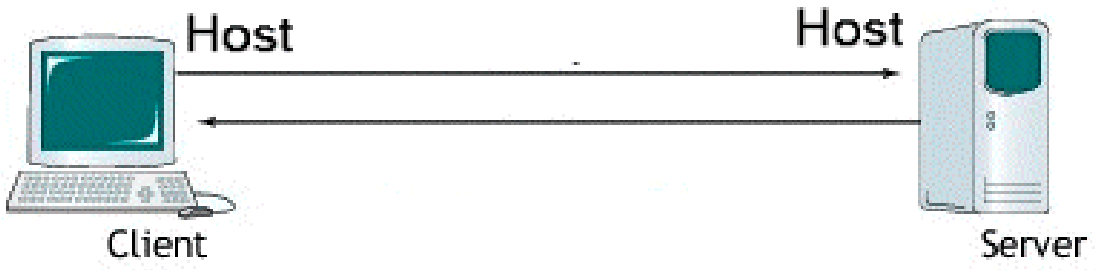
- udpInDatagrams — taxa de datagramas recebidos
- udpOutDatagrams — taxa de datagramas enviados
- udpNoPorts — taxa de datagramas que não foram enviados para uma porta valida
- udpInErrors — taxa de datagramas UDP recebidos com erro

Observações sobre o grupo UDP

- A consulta periódica aos objetos udpInDatagrams e udpOutDatagrams pode determinar a taxa de entrada e saída de datagramas.
- O objeto udpNoPorts informa quando a entidade está recebendo datagramas de uma aplicação inválida.
  - Uma taxa alta desses datagramas pode resultar em problemas de performance.

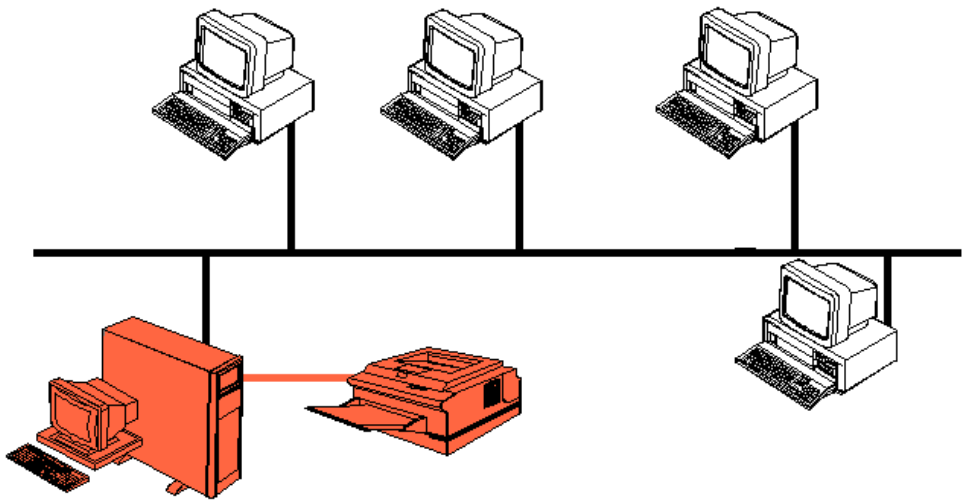
Host Resources MIB - RFC 1414

- Este RFC define o Host Resources MIB que é um conjunto uniforme de objetos completos , para o gerenciamento do sistema host.
- O termo Host é utilizado para significar qualquer computador que se comunique com outro computador.



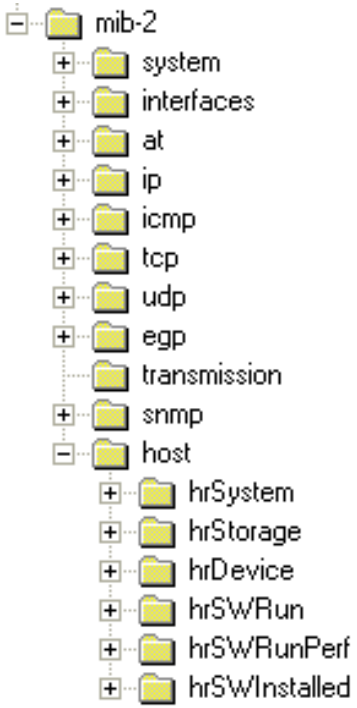
Host Resources MIB - RFC 1414

- A Host Resources MIB é independente de sistemas operacionais, serviços de rede, ou qualquer aplicação de software.
- Podem existir extensões da host MIB para servidores específicos (ver exemplo da MIB Novell).

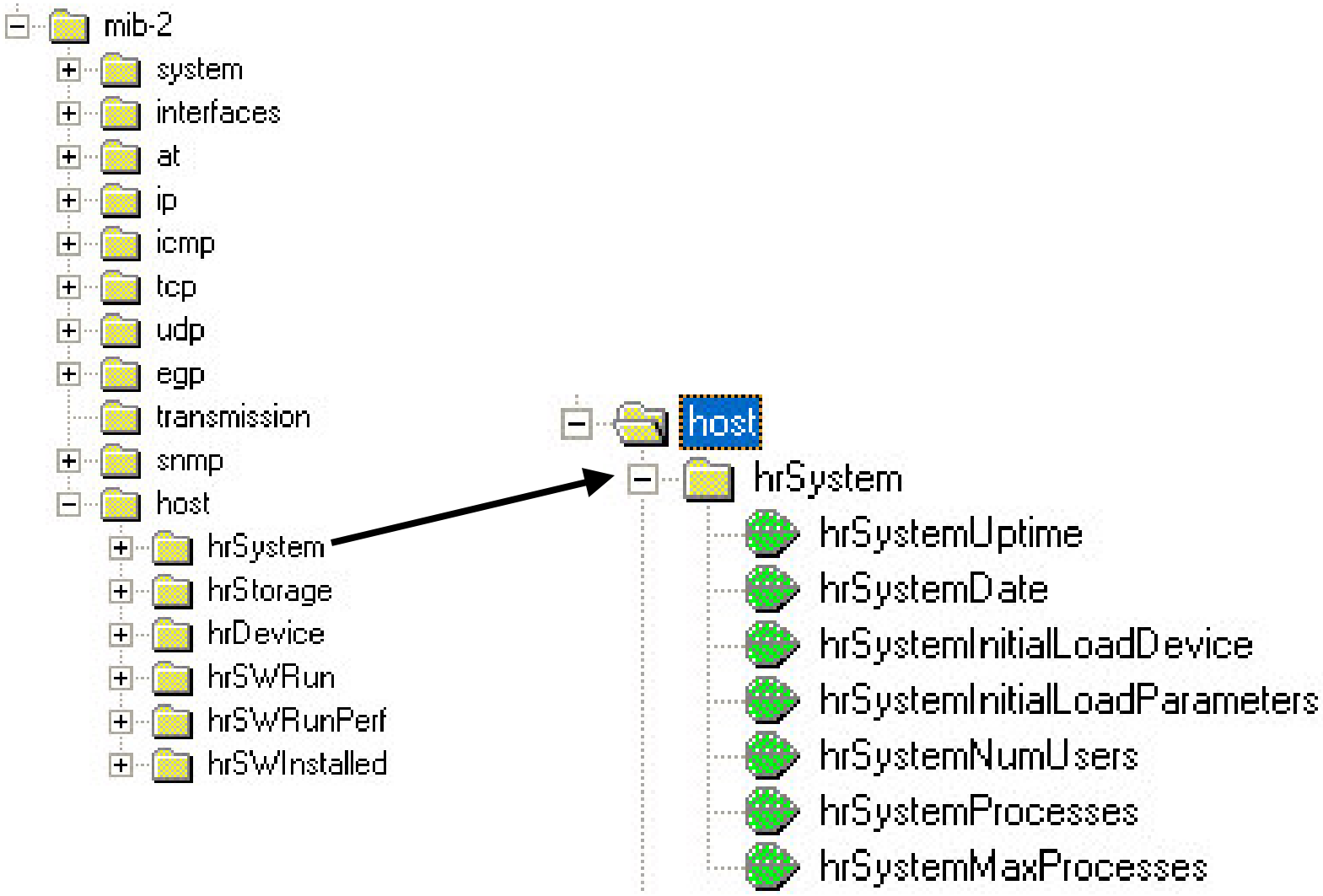


Host Resources MIB

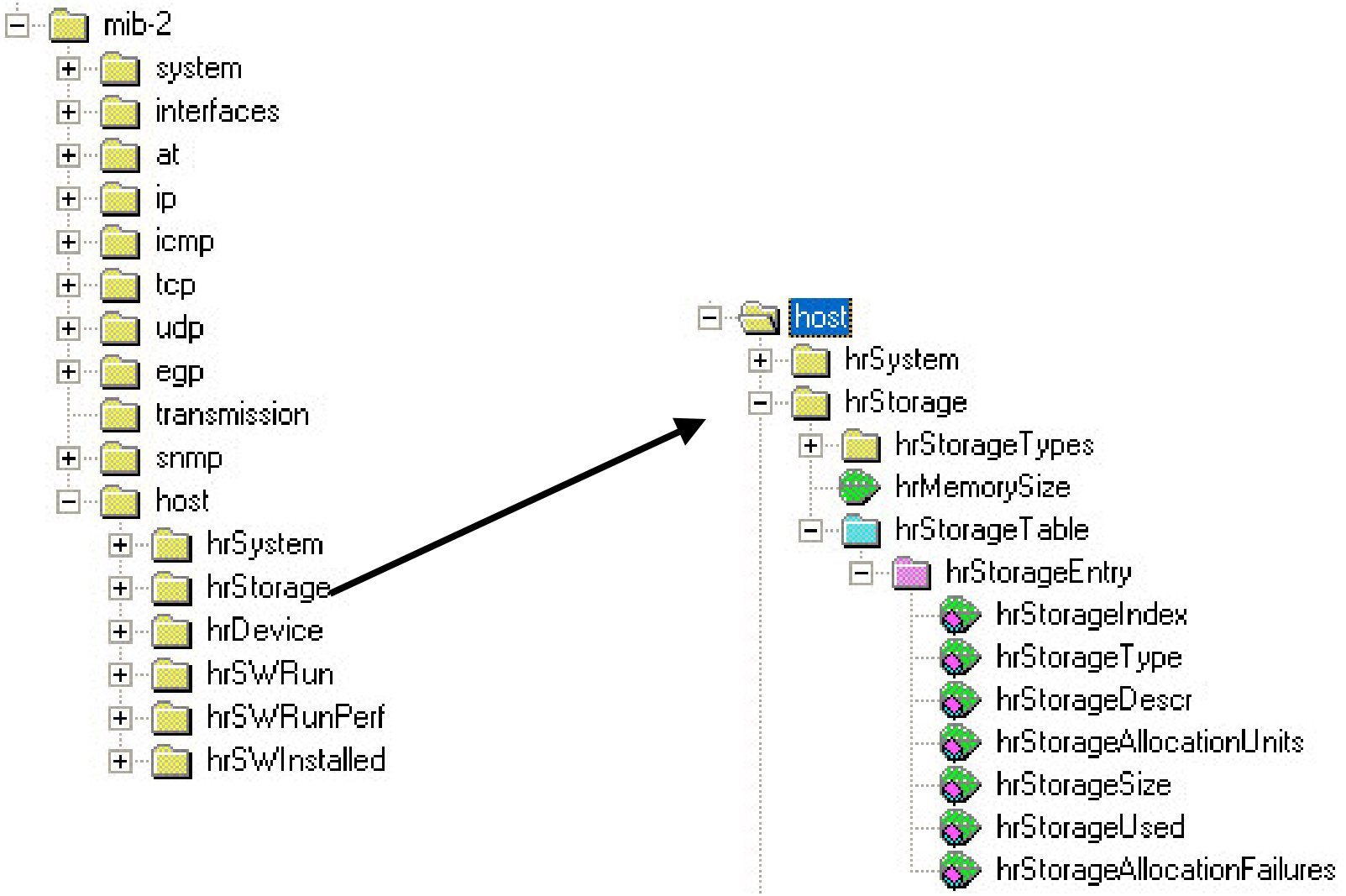
- O Host Resources MIB define objetos, qual são comuns para muitas arquiteturas de computador.
- Grupos da Host Resources MIB:
  - 1- hrSystem --> grupo sistema
  - 2- hrStorage --> grupo armazenagem
  - 3- hrDevice --> grupo unidade
  - 4- hrSWRun --> grupo execução de software
  - 5- hrSWRunPerf --> grupo performance de execução de software
  - 6- hrSWInstalled --> grupo de software instalado



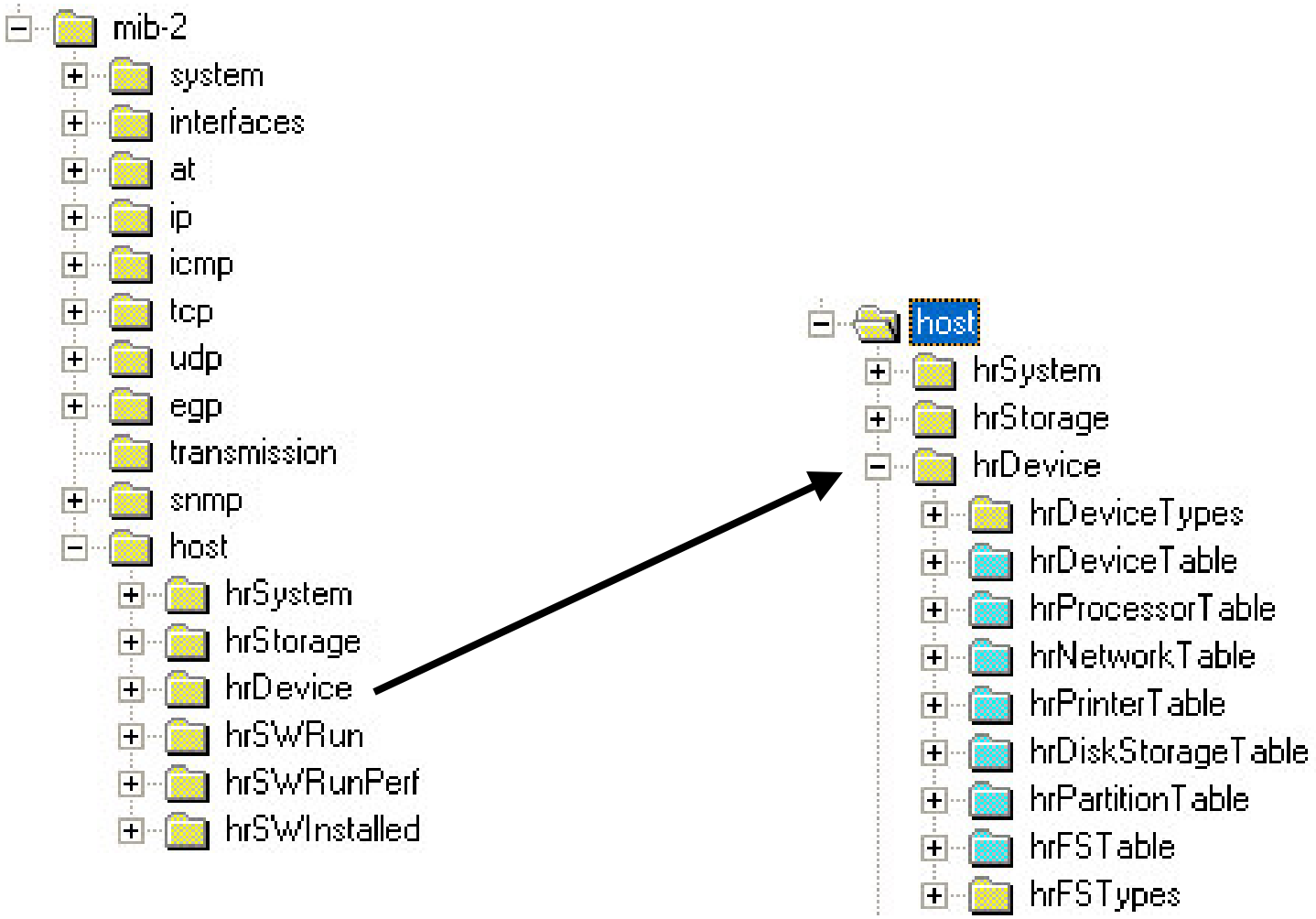
Host resources MIB



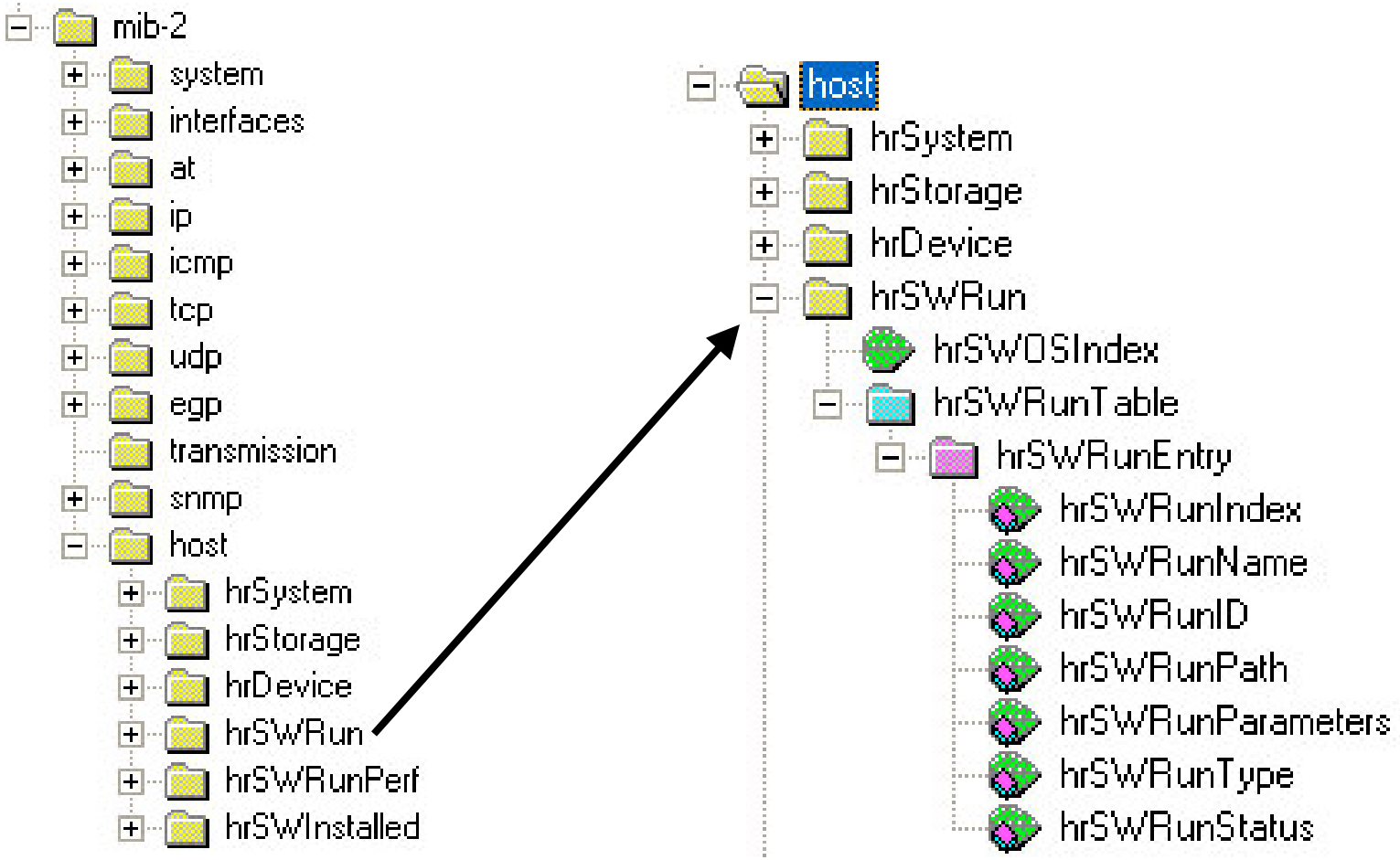
Host resources MIB



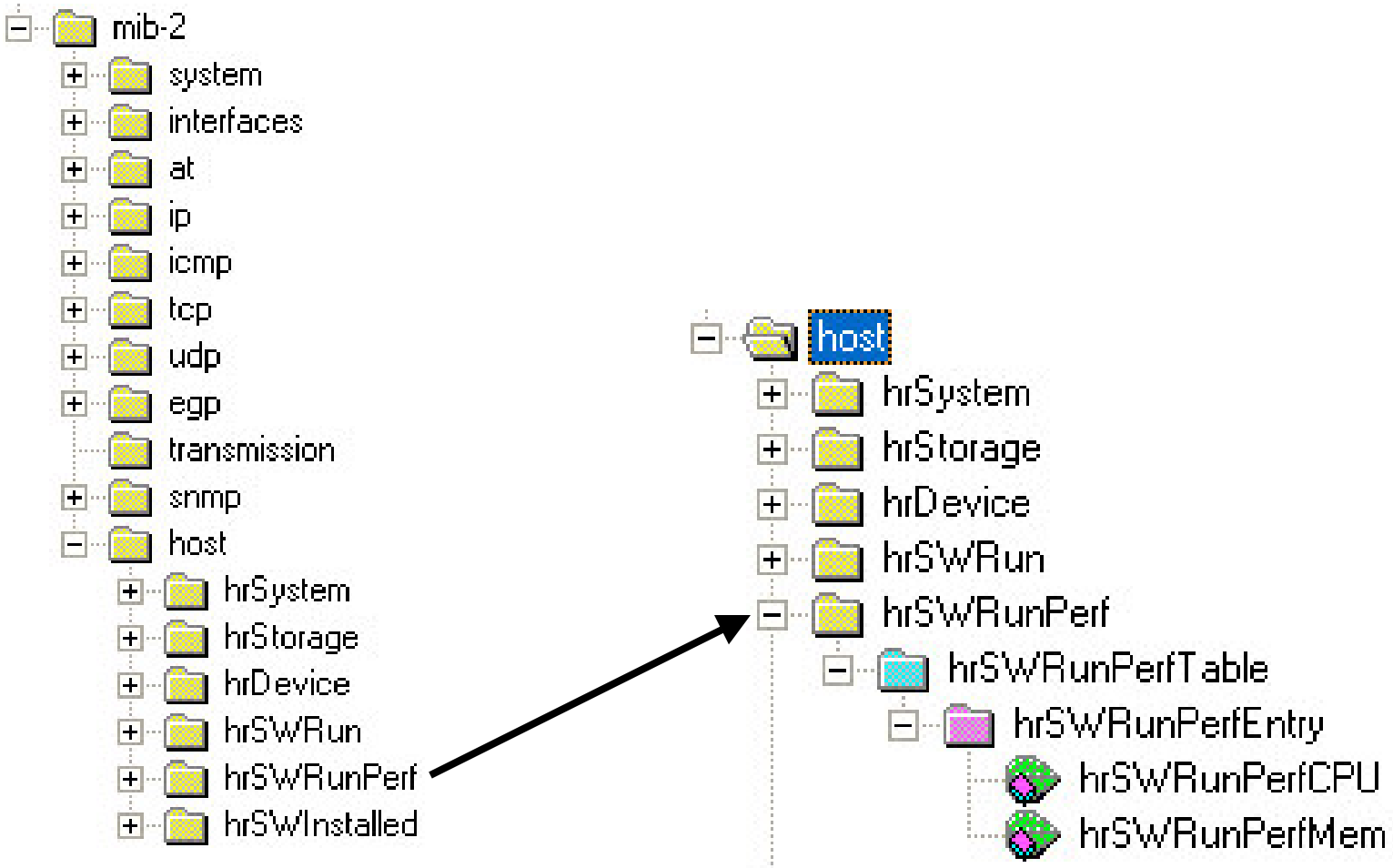
Host resources MIB



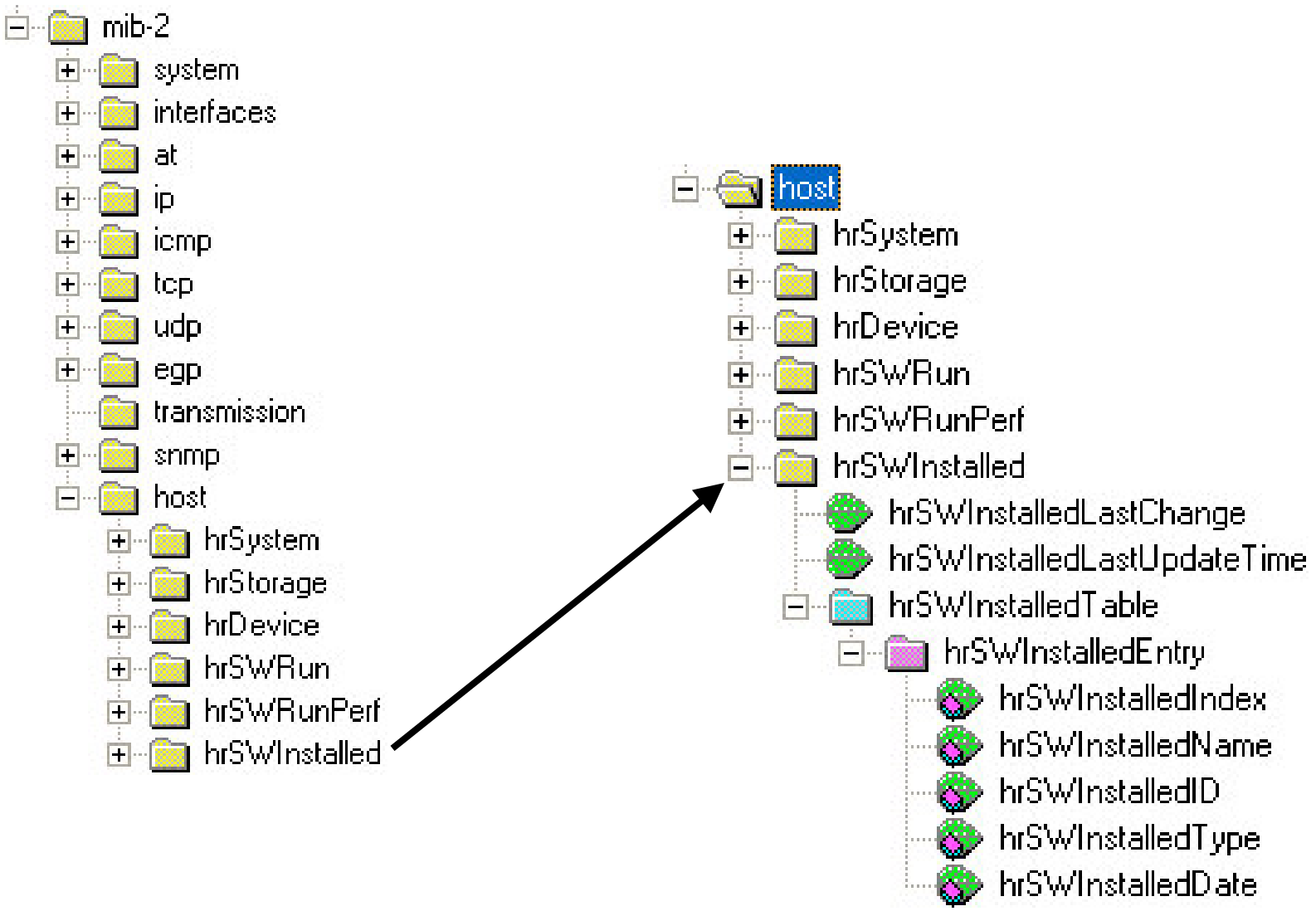
Host resources MIB



Host resources MIB

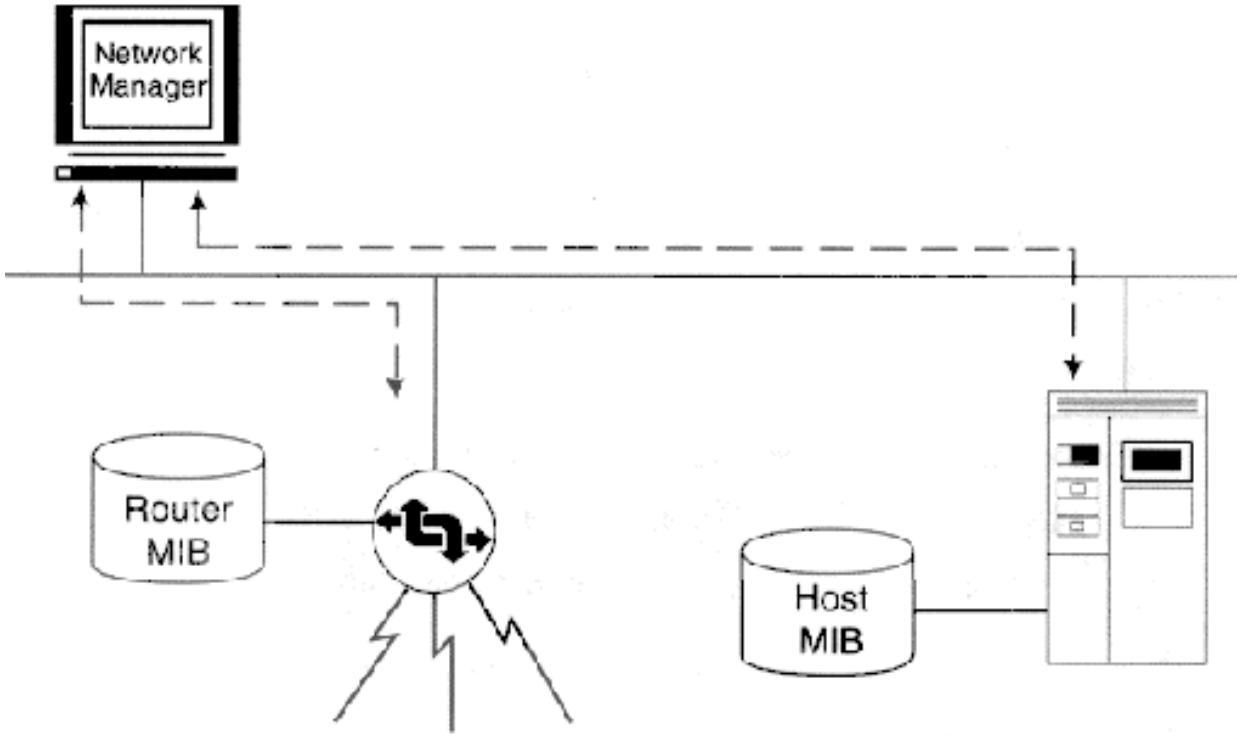


Host resources MIB



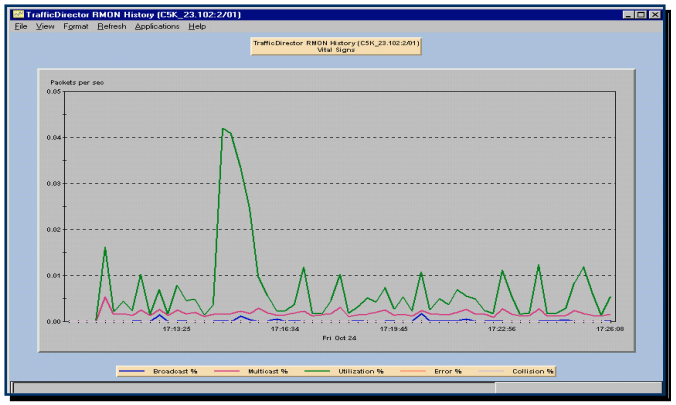
Investigando hosts

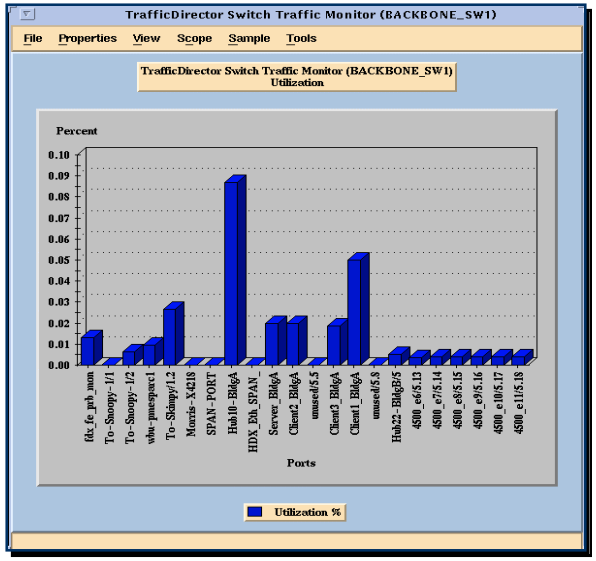
- O que é possível descobrir sobre um host, usando a host MIB?



Monitorando aplicações

- Inspecionar disponibilidade
- Gerar alertas (limiares ultrapassados)
- Isolar dados que auxiliem o diagnóstico antes que afetem a rede





Gerenciamento de performance

- Conhecer e compreender as condições normais e tendências
- Gerar relatórios