Gerenciamento de Redes

Introdução

- Necessidade de gerenciamento para redução dos riscos
  - Crescente aumento do risco de falhas e de ineficiências na rede
    - Crescimento em escala, complexidade e velocidade dos sistemas de rede
  - Falhas têm grande impacto
    - Crescente dependência das organizações nas redes que suportam suas operações

Introdução

- Funções do gerenciamento
  - Monitorar e controlar o estado dos sistemas e da rede
    - Configuração
    - Detecção de falhas
  - Gerar informações estatísticas para análise e planejamento
    - Gerenciamento de tráfego
    - Tarifação
    - Planejamento de capacidade
    - Planejamento de topologia
    - Avaliação de investimentos em redes

Motivação

- Organizações investem quantias razoáveis de tempo e dinheiro em redes de computadores
  - Crescente dependência das organizações nas redes que suportam suas operações
- Necessidade
  - garantir disponibilidade, segurança e desempenho dos serviços oferecidos

Introdução

- Em ambiente de redes, gerenciar é:
  - Obter informações da rede
  - Tratar as informações de forma adequada
    - Visualização da situação operacional da rede
    - Identificar problemas
    - Gerar alertas
  - Diagnosticar os possíveis problemas
  - Encontrar as soluções necessárias

Áreas Funcionais da Gerência de Redes

- Gerenciamento de Redes dividido em cinco áreas funcionais (ISO):
  - Gerenciamento de Falhas
  - Gerenciamento de Configuração
  - Gerenciamento de Desempenho
  - Gerenciamento de Segurança
  - Gerenciamento de Contabilidade

Gerenciamento de Falhas

- Mecanismos para detectar, isolar e corrigir problemas em uma rede de computadores
- Inclui funções para:
  - Detecção e notificação de falhas pelos sistemas gerenciados (eventos)
  - Manter e examinar log dos eventos recebidos
  - Isolar dispositivo defeituoso ou o segmento problemático da rede, de modo que ela continue funcionando normalmente
  - Diagnosticar e corrigir as causas da falha retornando a rede a seu estado normal

Gerenciamento de Configuração

- Objetiva o controle sobre a configuração dos elementos que compõem a rede
- Inclui funções para:
  - Identificação dos componentes de rede (endereçamento e atribuição de nomes)
  - Registrar configurações atuais e suas eventuais alterações
  - Alterar parâmetros da rede
  - Habilitar e desativar sistemas da rede

Gerenciamento de Desempenho

- Mecanismos para medir, monitorar, avaliar e relatar os níveis de performance do sistemas e da rede
- Coleta e armazenamento de estatísticas de desempenho para medir:
  - Percentual de utilização
  - Tempo de resposta
  - Taxas de erros
- Avaliação de investimentos em redes

Gerenciamento de Segurança

- Facilidades para controlar o acesso a informações na rede de computadores
  - autorização de uso
  - controlar o acesso aos recursos da rede e às informações
  - autenticação
  - controle de auditoria (logs de auditoria)
  - gerar, distribuir e armazenar chaves de criptografia

Gerenciamento de Contabilidade

- Mecanismos para identificar custos de implantação e utilização dos recursos da rede
  - informação aos usuários sobre o custo dos recursos consumidos
  - estabelecimento de limites no uso de recursos disponíveis (cotas)
  - bloqueio de acesso quando ultrapassados os limites estabelecidos.

Padrões

- International Standards Organization (ISO)
  - Common Management Information Protocol (CMIP)
- Internet Engineering Task Force (IETF)
  - Simple Network Management Protocol (SNMP)

Padrões de gerenciamento

- CMIP
  - Padrão de gerenciamento da ISO
  - Largamente utilizado em redes de telecomunicações
  - Padrão antigo, já consolidado
  - Excelente mecanismo de segurança
  - Complexo
    - Demanda muitos recursos computacionais
    - Exige pessoal treinado para sua operação

Padrões de gerenciamento

- SNMP
  - Padrão de gerenciamento do IETF (Internet Engineering Task force)
  - Padrão de facto da internet
  - Não proprietário, público e de fácil implementação
  - As principais vantagens são a simplicidade e a facilidade de implementação

Simple Network Management Protocol

Histórico

- Protocolo ICMP --> diagnóstico de problemas
  - gargalos na rede (ping - round trip time)
  - alcançabilidade de equipamentos e redes (ping)
  - verificação de roteamento (traceroute)
- Crescimento das redes
  - necessário o desenvolvimento de ferramentas mais poderosas para gerenciamento
  - facilidade de aprendizado e de uso.

Histórico

- Em 1988, a IAB (Internet Activities Board) avaliou as seguintes propostas de protocolo de gerenciamento
  - Simple Network Management Protocol (SNMP), versão aprimorada do Simple-Gateway Monitoring Protocol (SGMP)
  - High-Level Entity-Management System (HEMS), generalização do Host-Monitoring Protocol (HMP)
  - CMIP over TCP/IP (CMOT), tentativa de utilização do padrão OSI para gerência de redes sobre TCP/IP

Histórico

- SNMP evoluiu, atendendo às necessidades de gerência Internet
- SNMP acabou sendo adotado em larga escala pelos fabricantes (padrão de *facto*)
- Em 1993, é proposto o padrão SNMPv2
  - solucionar deficiências da primeira versão
  - não houve um acordo sobre segurança
- Em 1998, é definido o padrão SNMPv3

Histórico

Data	Evento	RFC
Outubro 1987	High Level Entity Management System	1023
Novembro 1987	Simple Gateway Monitoring Protocol	1028
Fevereiro 1988	IAB SNMP Working Group	1052
Agosto 1988	Primeira especificação SNMP	1065-1067
Maio 1990	SNMP versão 1 (Community)	1155-1157
Março 1991	Management Information Base II	1213
Abril 1993	SNMP Versão 2 (Party)	1441-1452
Janeiro 1996	SNMP Versão 2 (Community)	1901

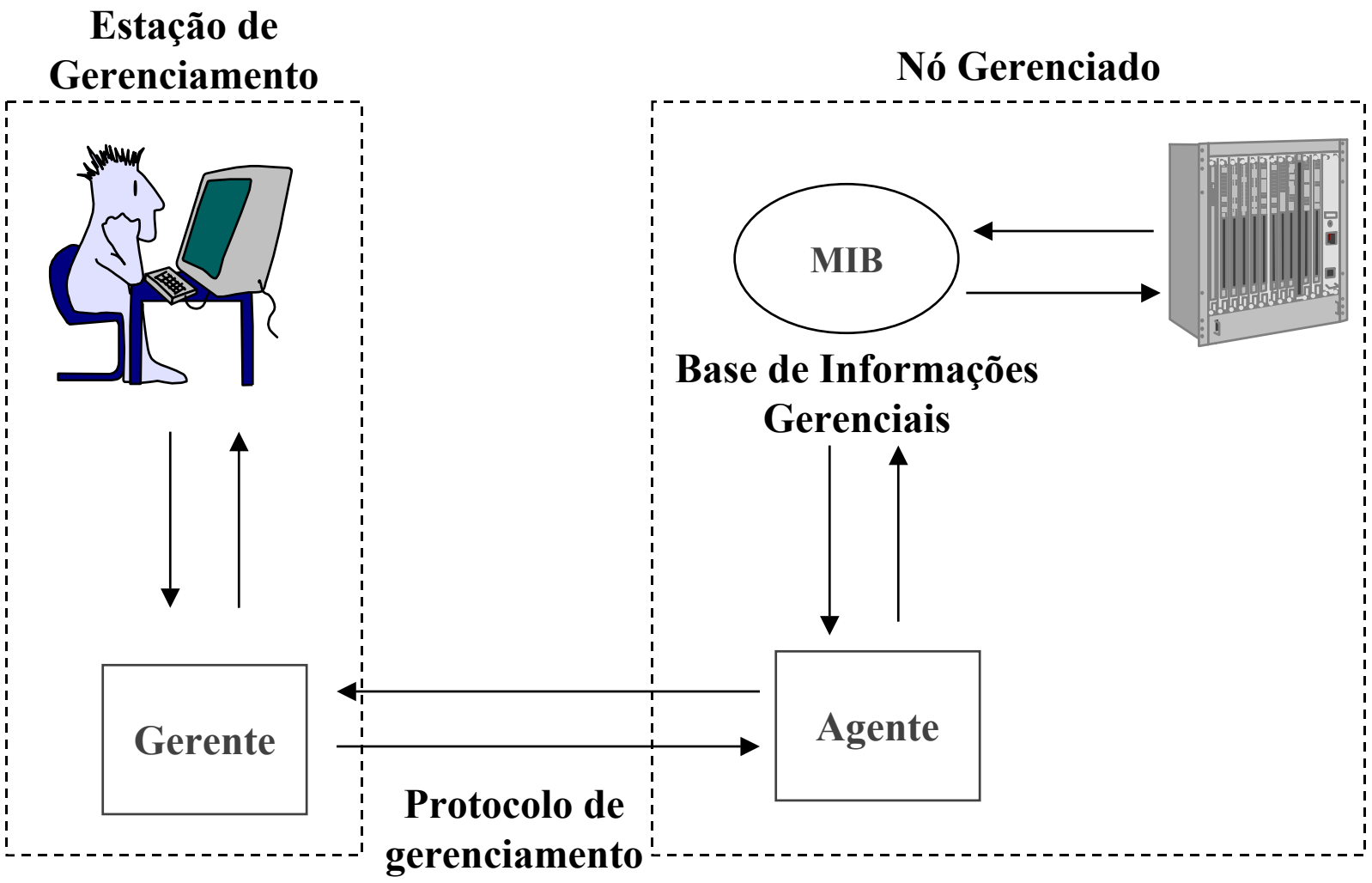
Histórico

Data	Evento	RFC
Janeiro 1996	SNMPv2 (revisão)	1902-1908
Janeiro 1998	SNMPv3	2271-2275

Arquitetura SNMP

- O modelo adotado no gerenciamento de redes é composto de:
  - Um ou mais nós gerenciados, cada um contendo um agente
  - Estação de gerenciamento
  - Base de informações Gerenciais (MIB)
  - Protocolo de comunicação

Arquitetura SNMP



Estação de Gerenciamento

- Implementa protocolo de gerenciamento
- Aplicações de gerenciamento responsáveis por monitorar e controlar a rede
  - interface entre o administrador de redes e o sistema de gerenciamento
  - descoberta automática e controlada de dispositivos e da topologia de rede
  - mapas gráficos da rede
  - base de dados das informações extraídas das MIBs de todas as entidades gerenciadas na rede

Agentes

- Atendem às requisições de gerenciamento enviadas pelos gerentes
- Implementados em:
  - estações de trabalho, servidores
  - equipamentos de rede
    - roteadores
    - switches, hubs, bridges, repetidores, etc.
- Podem enviar notificações assíncronas de eventos importantes (traps)
  - mudança de estado de um enlace
  - inicialização do equipamento

Base de Informações Gerenciais

- Management Information Base (MIB)
- Define as informações acessíveis através de um protocolo de gerenciamento
- Utiliza formato hierárquico e estruturado para definir as informações de gerenciamento
- Todos os agentes devem usar o formato definido pela MIB

Base de Informações Gerenciais

- Informações padrão
  - Management Information Base II (MIB-II)
- Informações proprietárias
  - Extensões definidas pelos fabricantes

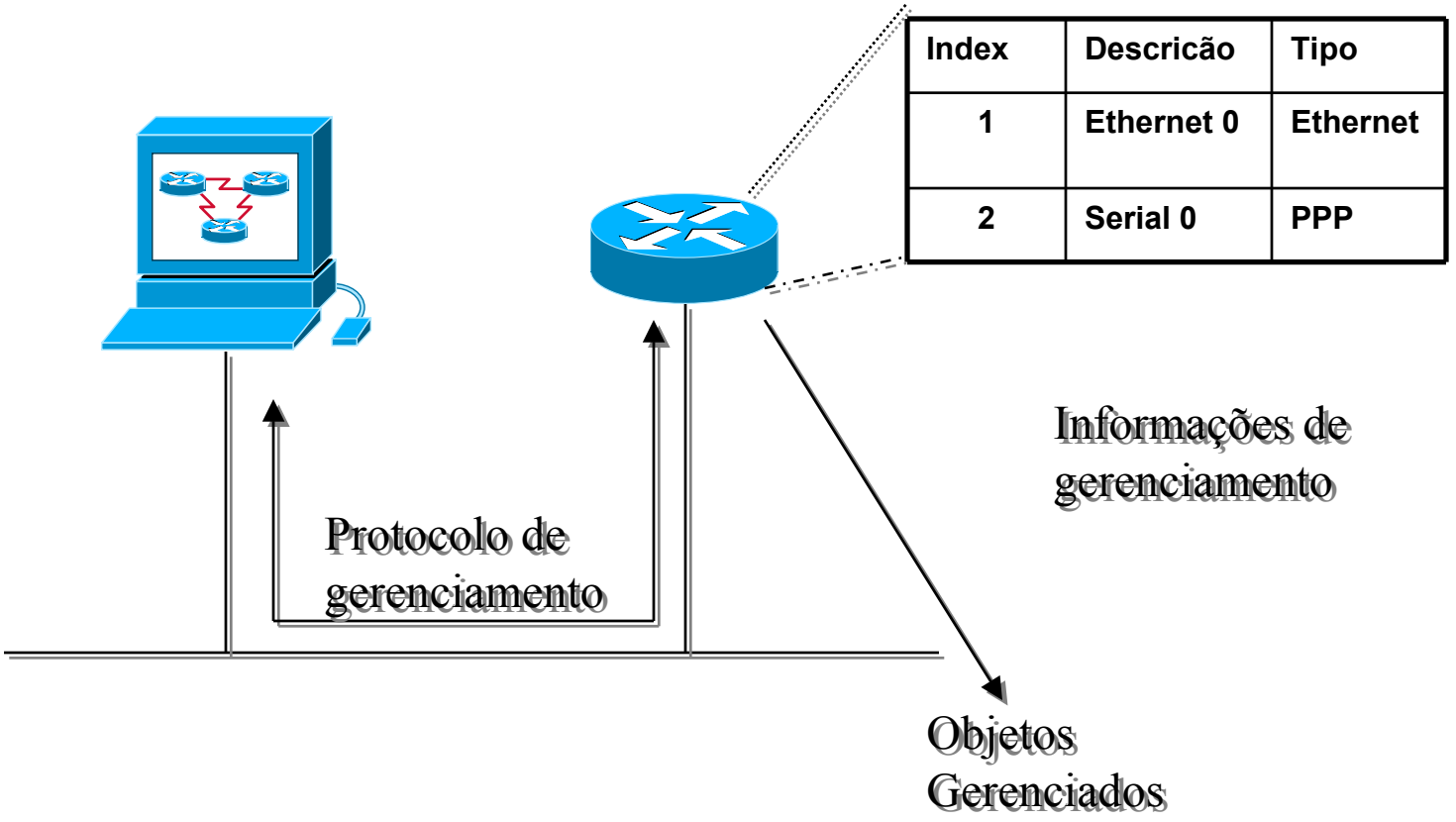
Management Information Base II (MIB-II)

- Grupos
  - system
  - interfaces
  - at
  - IP
  - ICMP
  - TCP
  - UDP
  - EGP
  - Transmission
  - SNMP

Protocolo de Gerenciamento

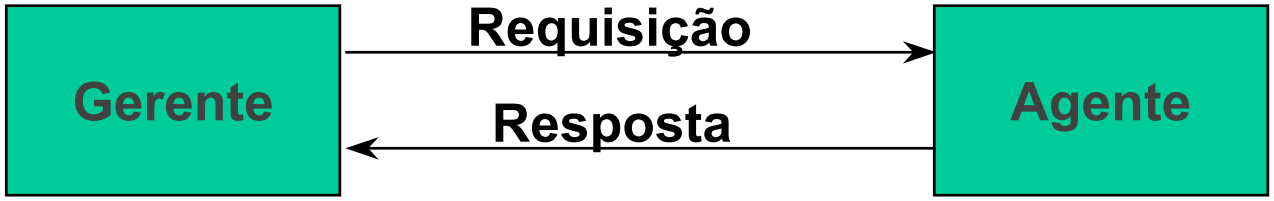
- Efetua a troca de informações entre gerente e agente
- Operações possíveis:
  - Obter dados da MIB para fins de monitoração
  - Alteração de dados da MIB, possibilitando o controle do dispositivo gerenciado
  - Notificação de eventos

Protocolo de Gerenciamento

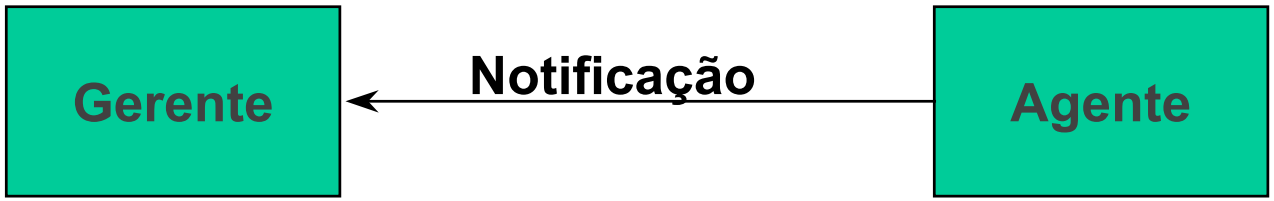


Comunicação entre entidades SNMP

- **“*polling*” síncronos**



- **Notificações assíncronas de eventos (trap)**



Polling versus Trap

- Polling
  - vantagem
    - gerente controla a taxa de consultas
  - desvantagem
    - grande número de agentes, cada um com um grande número de objetos (congestionamento da rede)

Polling versus Trap

- Trap
  - vantagem
    - notificação imediata de eventos excepcionais
  - desvantagem
    - desperdício de tempo para monitorar as condições que podem provocar o evento
    - não há garantia de entrega de traps

Trap-directed polling

- Mecanismo do SNMP que permite uso eficiente da rede
  - polling é efetuado normalmente na inicialização da estação de gerência
    - características das interfaces
    - informações estatísticas
  - eventos anormais são reportados via uma única notificação (trap)
  - gerente pode efetuar consulta (polling) após receber a notificação para obter maiores detalhes sobre a falha

Especificações SNMP

- Estrutura de Informações Gerenciais (SMI)
  - RFC 1155
- Base de Informações Gerenciais (MIB)
  - RFC 1156
  - RFC 1213 (MIB-II)
- Protocolo de Comunicação
  - RFC 1157

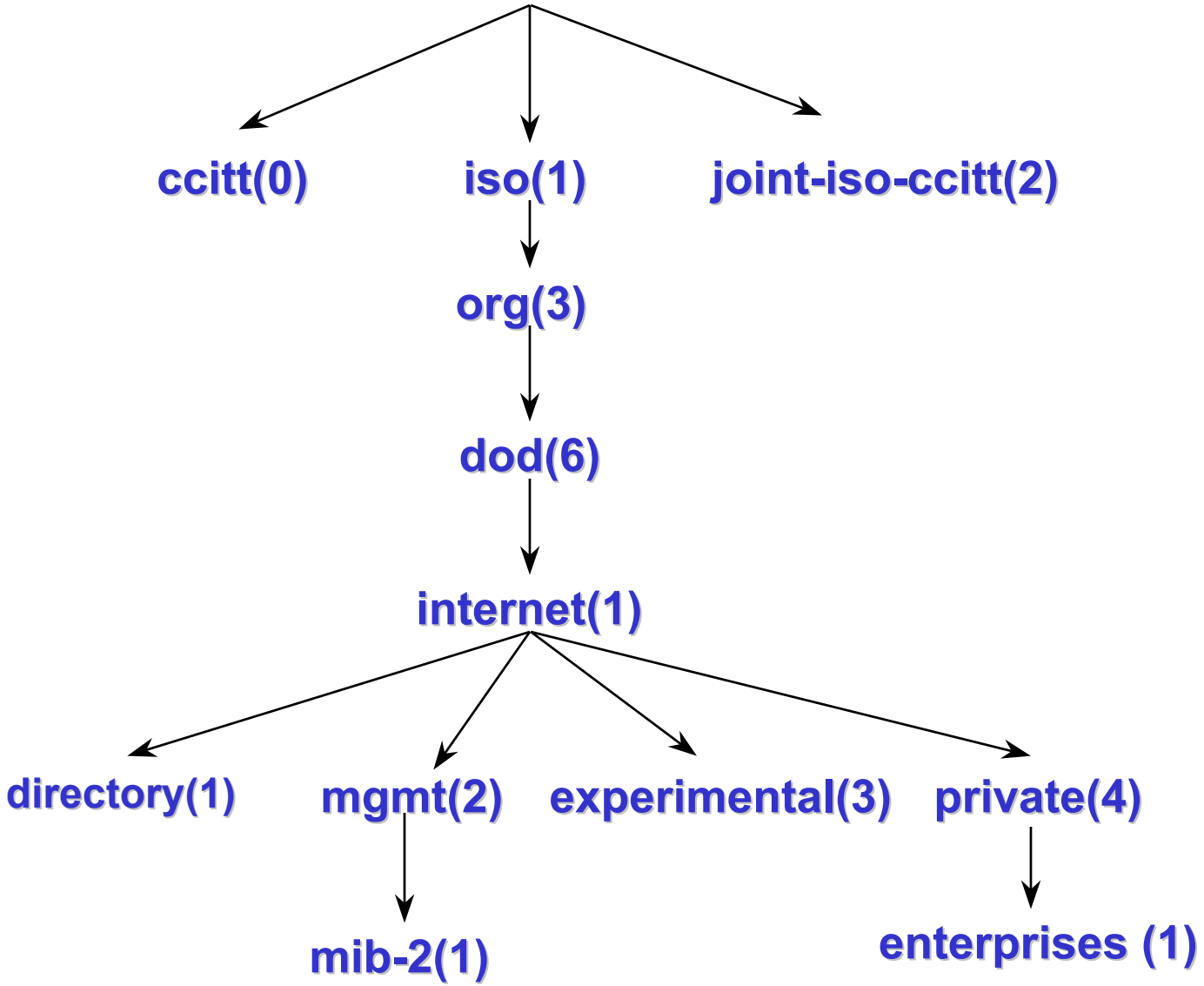
Estrutura de Informações Gerenciais

- Regras usadas para descrever as informações de gerenciamento
- Definições
  - estrutura da MIB
  - identificação e estrutura das informações de gerenciamento
    - identificação dos objetos
    - descrição da sintaxe dos objetos
    - forma de acesso aos objetos definidos

Estrutura da MIB

- Objetos que compõem a MIB são definidos pelo seu nome, sintaxe e codificação
- Identificação de objetos na MIB
  - Adotado esquema hierárquico de nomes para que cada objeto tenha uma identificação única
  - A hierarquia de nomes é implementada através de uma árvore hierárquica de uso global
  - Cada nó da árvore tem associado um número e um texto descritivo

Estrutura da MIB



Object Identifier (OID)

- Identificação única de um objeto na MIB
- Define a localização de um objeto na estrutura da árvore de nomes
- Formado pela sequência de valores de nó que se atravessa na árvore, indo da raiz até ao nó do objeto em questão
- Podem ser expressos de várias formas:

iso.org.dod.internet.mgmt.mib-2

ou

1.3.6.1.2.1

Definição de Objetos

- Exemplo

```
system OBJECT IDENTIFIER ::= { mib-2 1 }
sysUpTime OBJECT-TYPE
        SYNTAX TimeTicks
        ACCESS read-only
        STATUS  mandatory
        DESCRIPTION "The time (in hundreth of a  second)
          since the network management portion of the system
          was last re-initialized."
        ::= { system 3 }
```

  – OID do objeto sysUpTime: 1.3.6.1.2.1.1.3

Definição de Objetos

- Exemplo

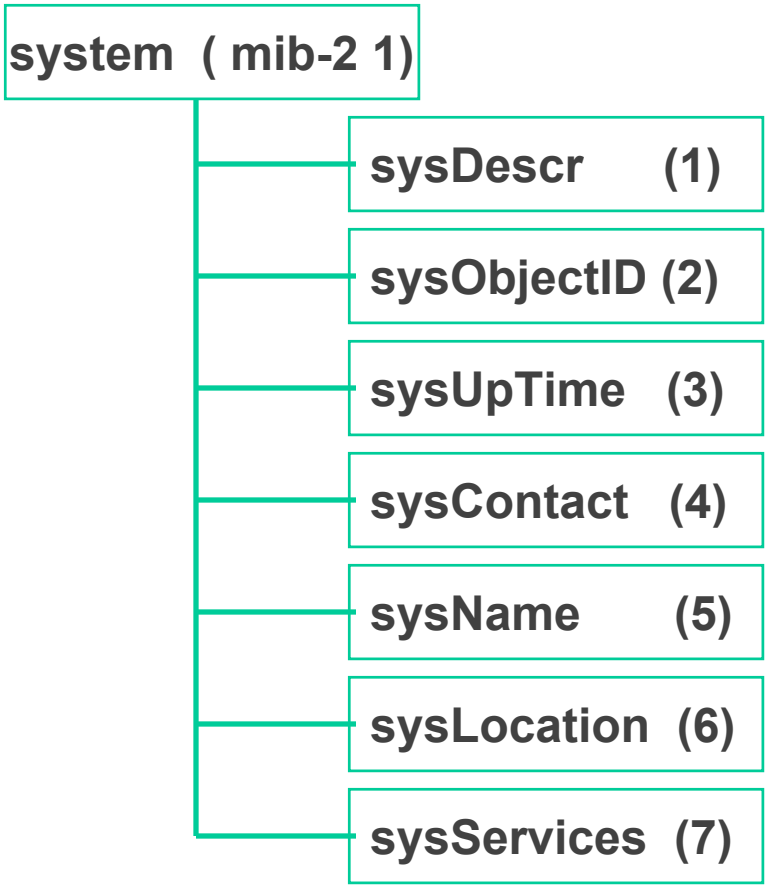
```
ipForwarding OBJECT-TYPE
    SYNTAX  INTEGER {
        forwarding(1),    -- acting as a gateway
        not-forwarding(2) -- NOT acting as a gateway
    }
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
      "The indication of whether this entity is acting as an IP gateway
       in respect to the forwarding of datagrams received by, but not
       addressed to, this entity.  IP gateways forward datagrams.“
        ::= { ip 1 }
```

Tabelas

Index (ifIndex)	Descrição (ifDescr)	Tipo (ifType)	Estado Operacional (ifOperStatus)
1	Laboratórios	Ethernet	UP
2	Administração	Ethernet	UP
3	Estácio	V35	UP
4	Barra Tijuca	V35	DOWN

Grupo system

- Disponibiliza informações sobre o nó gerenciado



Grupo interfaces

- Disponibiliza informações sobre cada uma das interfaces existentes no agente
- Dados da tabela permitem:
  - descrever e qualificar a interface
    - ifDescr(2)
    - ifType(3)
    - ifMtu (4)
    - ifSpeed (5)
    - ifPhysAddress (6)
  - monitorar e controlar estado das interfaces
    - ifAdminStatus (7)
    - ifOperStatus (8)
    - ifLastChange (9)

Grupos interfaces

- Dados na tabela permitem (continuação):
  - determinar utilização
    - ifInOctets (10)
    - ifInUcastPkts (11)
    - ifInNUcastPkts (12)
    - IfInDiscards (13)
    - ifOutQLen(21)
    - ifOutOctets (16)
    - ifOutUcastPkts (17)
    - ifOutNUcastPkts (18)
    - ifOutDiscards (19)
  - disponibilizar dados para gerenciamento de falhas
    - ifInErrors (14)
    - ifOutErrors (20)

Grupo IP

- Informações relevantes para a implementação e operação do protocolo IP
- Objetos
  - ipForwarding (ip 1)
  - ipAddrTable (ip 20)
    - uma entrada para cada endereço IP configurado no dispositivo
    - itens “read-only”
    - impossível a alteração do endereço IP usando SNMP
  - ipRouteTable (ip 21)
    - itens “read-write”
  - ipNetToMediaTable (ip 22)
  - ipForward (ip 24)

Formatos SNMP

- SNMPv1 messages

version	community	SNMP PDU

- GetRequest-PDU GetNextRequest-PDU SetRequest-PDU

PDU Type	request-id	0	0	variable bindings

- GetResponse-PDU

PDU type	request-id	error-status	error-index	variable bindings

Formatos SNMP

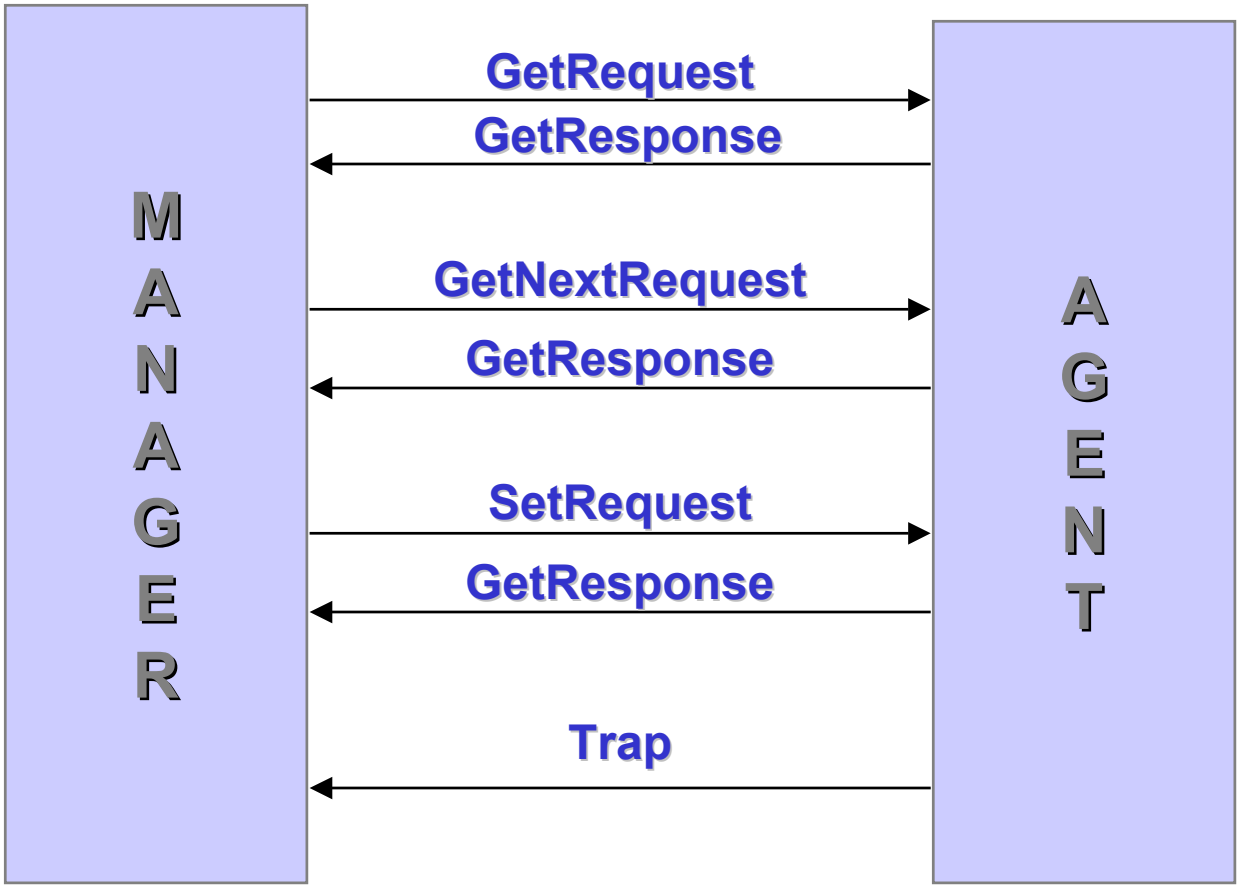
- Trap-PDU

PDU Type	enterprise	agent-address	generic-trap	specific-trap	time-stamp	variable-bindings

- Variable bindings

name 1	value 1	name 2	value 2	name 3	value 3	...	name n	value n

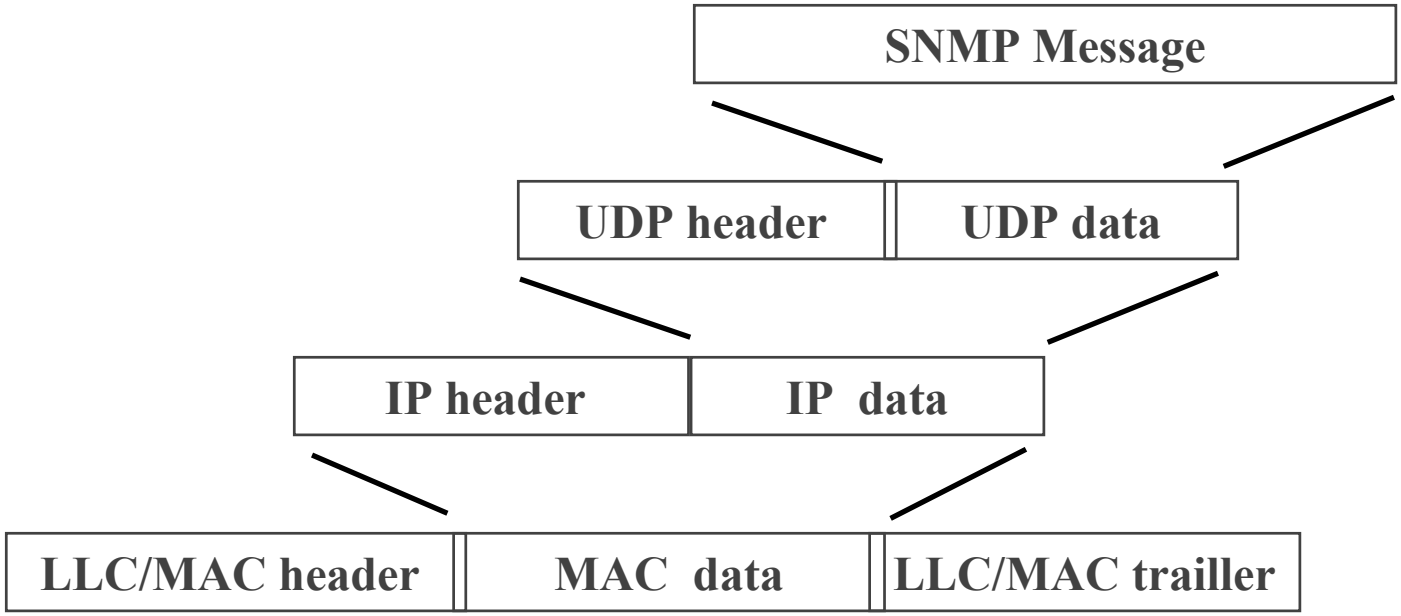
SNMP: Modelo Operacional



SNMP: Segurança

- Comunidade
  - Relação entre um agente e uma ou mais estações de gerenciamento que define características de autenticação e acesso
- Nome da comunidade usada para autenticação de mensagens SNMP
  - Funciona como senha de acesso ao agente
  - Gerente deve informar a *community name* em toda a requisição efetuada junto a um agente
  - Serviço trivial, não garantindo acesso não autorizado

SNMP: Serviço de Transporte



- Agentes aguardam requisições SNMP na porta 161
- Gerentes esperam por Traps na porta 162

Limitações Protocolo SNMP

- Baixa segurança limita uso do SNMP
  - uso somente para monitoração
- Uso problemático em redes de grande porte
  - mecanismo de *polling* pode causar problemas de congestionamento na rede
- Não há suporte à comunicação entre aplicações de gerenciamento (*manager to manager)*

Limitações Protocolo SNMP

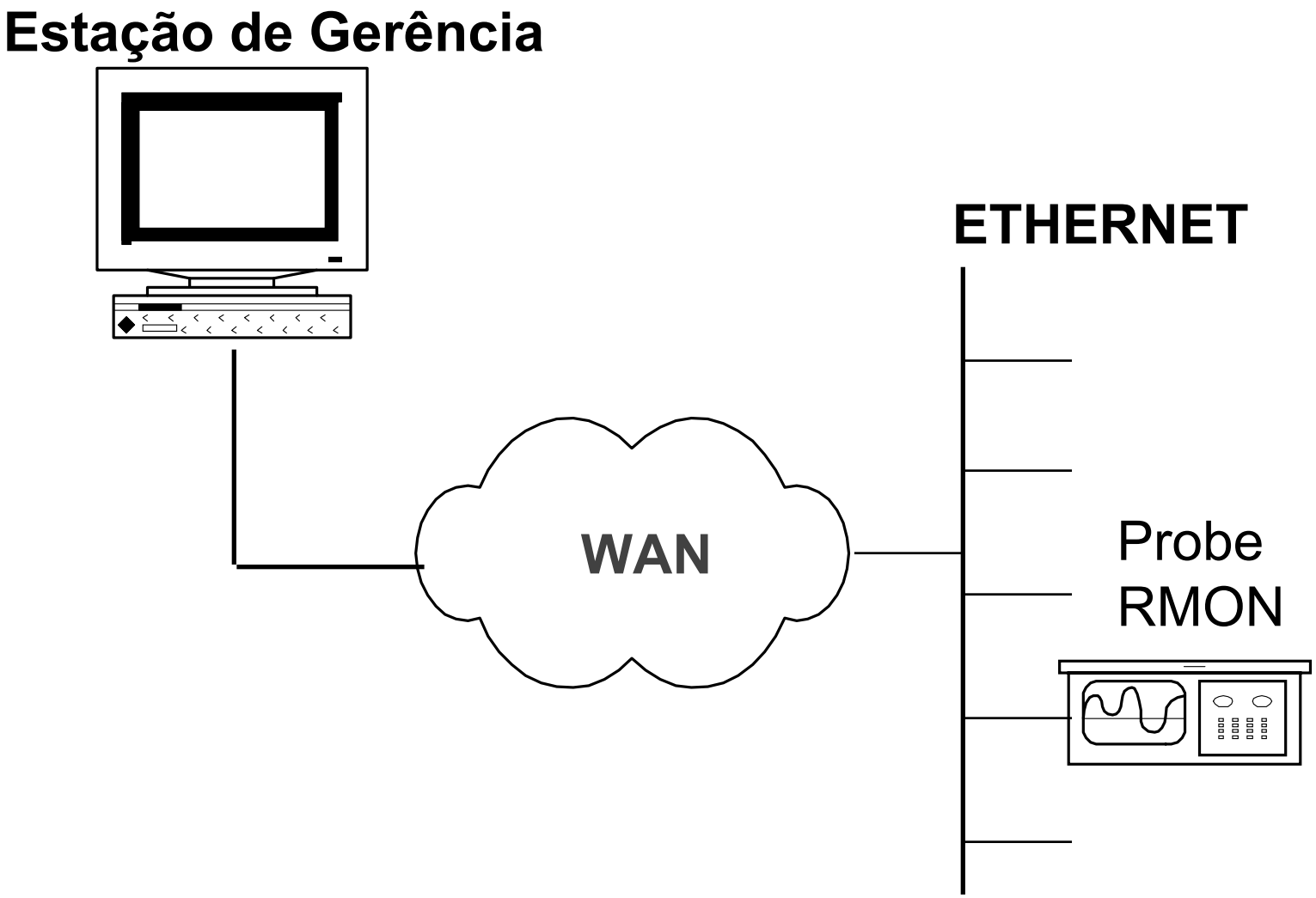
- Não há garantia de entrega de traps
- Modelo MIB é limitado, não suportando consultas baseadas em tipo ou valor dos objetos

Remote Network-Monitoring
RMON

Remote Network-Monitoring RMON

- MIB específica para monitoração de redes
- Provê uma maneira efetiva e eficiente de monitorar comportamento de segmentos de rede
- Objetivos (segundo RFC 1271)
  - operação off-line
  - monitoramento pró-ativo
  - notificar à estação de gerência somente eventos significativos
  - o monitor deve suportar gerentes múltiplos

Monitores Remotos (RMON)



Padrões RMON

- RMON1
  - opera no nível da camada MAC
  - monitora o tráfego e coleta informações estatísticas da operação de um segmento de rede
  - diagnóstico remoto de falhas e erros ocorridos no segmento de rede

MIB RMON1

- Nove grupos básicos (RFC 1757)
  - Estatistico
  - Histórico
  - Alarmes
  - Hosts
  - HostTopN
  - Matriz
  - Filtros
  - Captura de Pacotes
  - Eventos

Padrões RMON

- RMON2
  - opera no nível da camada de rede e camadas superiores
  - coleta informações estatísticas e monitora a comunicação fim-a-fim e o tráfego gerado por diferentes tipos de aplicações

MIB RMON2

- ProtocolDir
- ProtocolDist
- AddressMap
- NlHost
- NlMatrix

- AlHost
- AlMatrix
- UsrHistory
- ProbeConfig

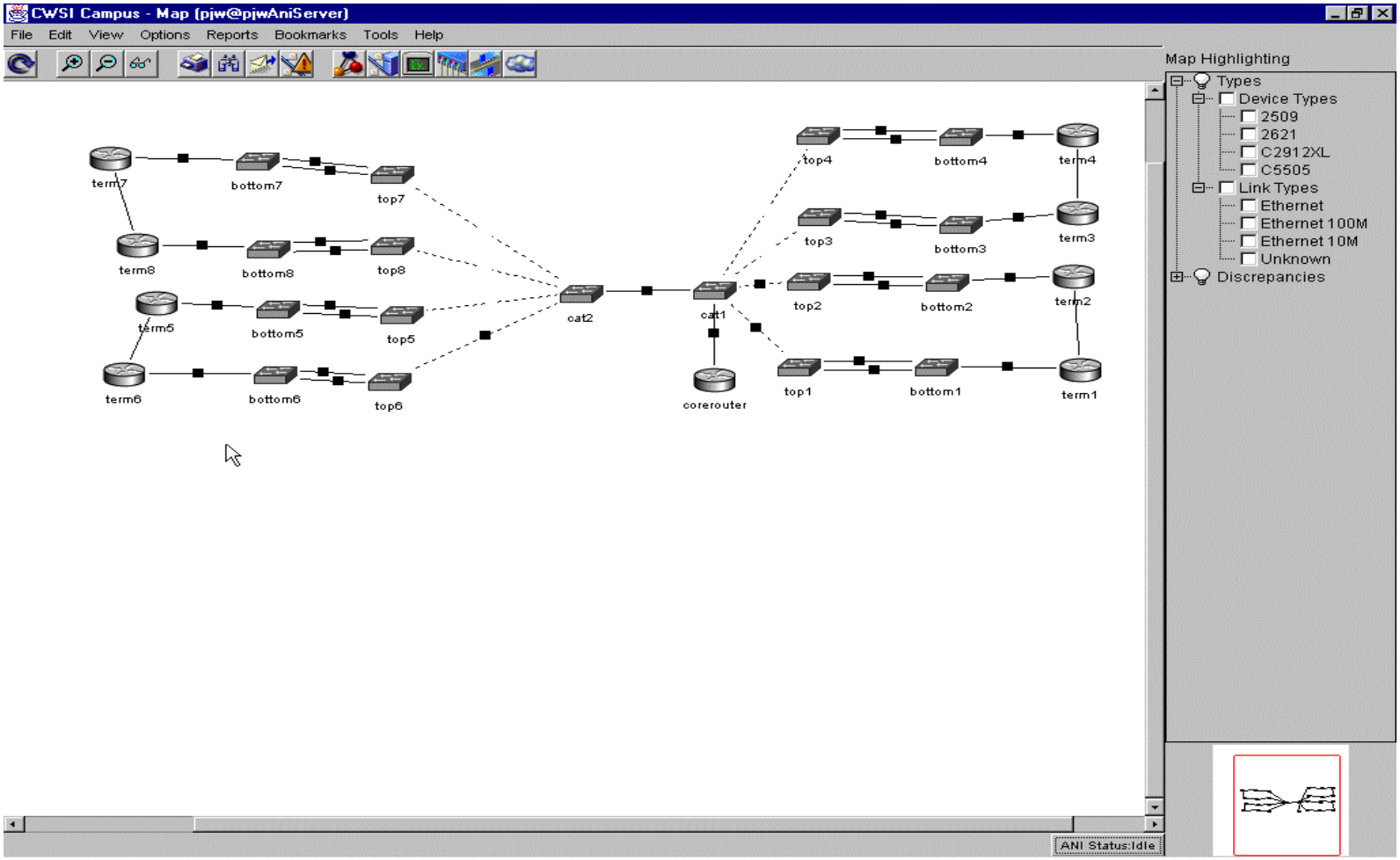
Plataformas de Gerenciamento

- Funções básicas:
  - mapas com a topologia da rede
  - descoberta automática de equipamentos - uso de ICMP e SNMP
  - alarmes que indicam, através de mensagens ou bips de alerta, anormalidades na rede
  - Application Program Interfaces (API) que permitem a integração de novas funções ao sistema de gerenciamento
  - emissão de relatórios estatístico

Plataformas de Gerenciamento

- HP Openview
- TME/Tivoli
- Unicenter TNG
- Cabletron Spectrum
- Sunsoft Solstice Enterprise Manager
- Especificios
  - CiscoWorks
  - Transcend

Plataformas de Gerenciamento



Plataformas de Gerenciamento