Aula 19 - Conceitos, SNMP, MIBs

Diego Passos

Universidade Federal Fluminense

Redes de Computadores II

Na Última Aula (I)...

- Dimensionamento:
  - Criar **capacidade** compatível com a **demanda**.
  - Mas quanto é **suficiente**?
- Classes de Serviço:
  - Tráfego é dividido em **classes**.
  - Classes recebem **tratamentos diferentes**.
  - **Escalabilidade**.
- Marcação de pacotes:
  - Pacotes recebem marcas.
  - Identificação de classe.
- Isolamento:
  - Classes não devem se interferir.
  - Mas **recursos não usados devem ser aproveitados**.
- Escalonamento:
  - Política de escolha de pacotes para uso do enlace.
    - FIFO, *Priority Scheduling*, *Round Robin*, WFQ, ...
- Mecanismos de regulação:
  - Garantem que tráfego atende parâmetros declarados.
  - *e.g.*, *Token Bucket*.

Na Última Aula (II)...

- Diffserv: arquitetura para diferenciação de serviços.
  - **Escalabilidade:** maior esforço nas bordas.
    - Marcação de pacotes, condicionamento.
  - Roteadores de núcleo: obedecem ao PHB.
    - Aplicam políticas de compartilhamento de banda, *buffer*.
    - Políticas diferentes para classes diferentes.
- Garantias de QoS por fluxo: necessita de **controle de admissão**.
  - Garantir que rede/enlace possui **capacidade suficiente** para atender a **todos os fluxos**.
  - Configuração de chamada.
  - Cada elemento da rede deve prover garantias.

Objetivos do Capítulo 9

- Introdução ao gerenciamento de redes.
  - Motivação.
  - Componentes principais.
- *Framework* de gerenciamento de redes na Internet.
  - MIB: *Management Information Base*.
  - SMI: linguagem de definição de dados.
  - SNMP: protocolo para gerência de redes.
  - Segurança e administração.
- Serviços de apresentação: ASN.1.

Agenda do Capítulo 9

- O que é gerência de redes?
- *Framework* padrão de gerenciamento de redes na Internet.
  - *Structure of Management Information*: SMI
  - *Management Information Base*: MIB.
  - SNMP: operação do protocolo e Mapeamentos de Transporte.
  - Segurança e administração.
- ASN.1.

O que é gerência de redes?

O Que É Gerência de Redes

- **Sistemas autônomos ("redes"): milhares de componentes de *hardware*/*software* interagindo.**
- Outros sistemas complexos requerem monitoramento, controle:
  - Avião.
  - Usina nuclear.
  - Outros?

"**A gerência de redes** inclui o desenvolvimento, integração e coordenação do *hardware*, *software* e elementos humanos para monitorar, testar, indagar, configurar, analisar, avaliar e controlar a rede e seus recursos para alcançar os requisitos de tempo real, desempenho operacional e qualidade de serviço com custos razoáveis."

Gerência nos Primórdios da Internet

- Gerência era um processo quase inexistente.
  - Rede era um artefato de pesquisa
  - Não um "produto" usado por milhões de pessoas simultaneamente.
    - Incluindo transações financeiras e outras aplicações sensíveis.
- Problemas eram identificados de forma *ad hoc*.
  - Ferramentas básicas como o *ping* eram usadas para tentar localizar a fonte.
- *e.g.*, RFC 789 (primeira grande queda da ARPAnet).

Gerência de Redes: Casos de Uso (I)

- Detecção de falha em interface de rede de um *host* ou roteador.
  - Dispositivo com interface problemática pode enviar alerta ao administrador.
  - Administrador pode monitorar desempenho, detectar previamente degradação.
- Monitoramento de *hosts*/serviços.
  - Administrador pode verificar periodicamente se *hosts*/serviços estão ativos, funcionais.
- Monitoramento de tráfego.
  - Administrador pode monitorar continuamente o tráfego nos enlaces da rede.
  - Permite identificar padrões de tráfego, otimizar localização de elementos da rede.
  - Permite identificar necessidade de aumento de capacidade antes que rede se torne um gargalo.

Gerência de Redes: Casos de Uso (II)

- Detecção de instabilidades de roteamento.
  - Administrador pode monitorar continuamente certas rotas.
    - Ou estatísticas compiladas sobre o protocolo de roteamento.
  - Pode identificar mudanças muito frequentes, prejudicando desempenho.
- Monitoramento de SLAs.
  - Administrador pode monitorar métricas de desempenho estabelecidas em contratos de serviço.
  - Identificar que determinado acordo não está sendo seguido.
- Detecção de intrusos/tentativas de intrusão.
  - Administrador pode monitorar tentativas suspeitas de acesso a recursos da rede.
    - *e.g.*, quantidades anormais de aberturas de conexão para porta 22 de um servidor.
  - Permite prevenir ataques/invasões.

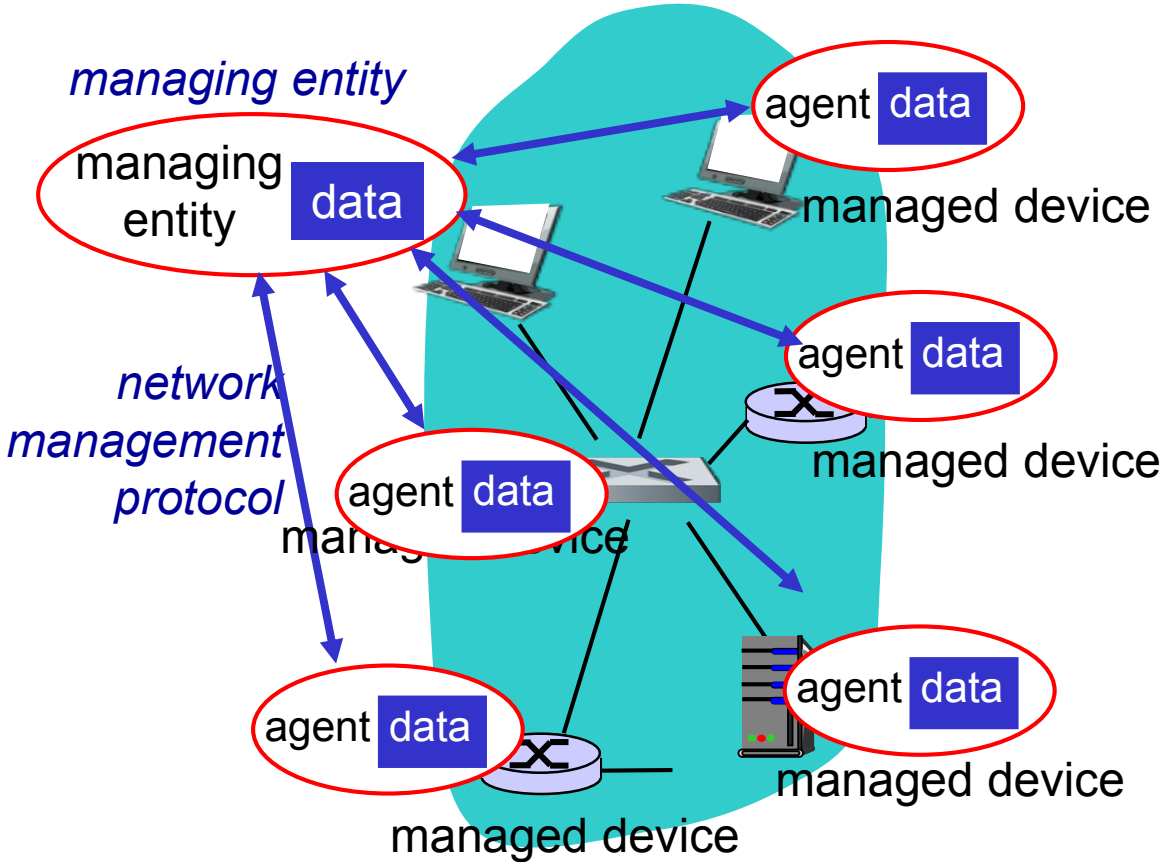
Áreas de Gerenciamento de Rede

- Cinco áreas definidas pela ISO:

- **Gerenciamento de desempenho**:
  - Medir/quantificar desempenho dos componentes de rede.
  - Roteadores, *switches*, *hosts*, ...
  - Vazão, atraso, perda de pacotes, ...
- **Gerenciamento de falhas**:
  - Detectar, registrar, reagir a eventos de falha.
  - *e.g.*, interrupção de serviços.
- **Gerenciamento de configuração**:
  - Conhecer dispositivos administrados.
  - Consultar, alterar configurações de *hardware*, *software*.
- **Gerenciamento de contabilização**:
  - Registrar, controlar acesso a recursos da rede.
- **Gerenciamento de segurança**:
  - Detectar tentativas de ataques/invasões.
  - Restringir acesso a recursos.
    - Objetivando segurança.

Infraestrutura para o Gerenciamento de Redes

- Definições:



Dispositivos gerenciados contêm **objetos gerenciados** cujos dados são reunidos em um ***Management Information Base* (MIB)**.

- Outros componentes:
  - **Entidade gerenciadora**.
  - **Agente de gerenciamento**.
  - **Protocolo de gerenciamento**.

Padrões de Gerência de Rede

- **OSI CMIP.**
  - *Common Management Information Protocol.*
  - Projetado nos anos 80: o padrão de gerência de redes unificado.
  - Padronização muito lenta.
- **SNMP: *Simple Network Management Protocol*.**
  - Raízes na Internet (SGMP).
  - Começou simples.
  - Rapidamente adotado, implantado.
  - Crescimento: tamanho, complexidade.
  - Atualmente: SNMPv3.
  - Padrão de fato para gerenciamento de redes.

Framework padrão de gerenciamento de redes na Internet

Visão Geral do SNMP: 4 Partes Chave

- ***Management Information Base* (MIB):**
  - Repositório distribuído de informações de gerenciamento de rede.
- ***Structure of Management Information* (SMI):**
  - Linguagem de definição de dados para objetivos MIB.
- **Protocolo SNMP:**
  - Transporta comunicação entre objeto gerenciado e gerenciador, incluindo informações e comandos.
- **Capacidades de segurança e administração.**
  - A grande adição no SNMPv3.

SMI: Linguagem de Definição de Dados

- **Propósito:** sintaxe e semântica dos dados de gerência é bem definida, sem ambiguidade.
  - Tipos básicos:
    - Óbvios, chatos.
  - OBJECT-TYPE:
    - Tipo do dado, status, semântica do objeto gerenciado.
  - MODULE-IDENTITY:
    - Agrupa objetos relacionados em um módulo MIB.

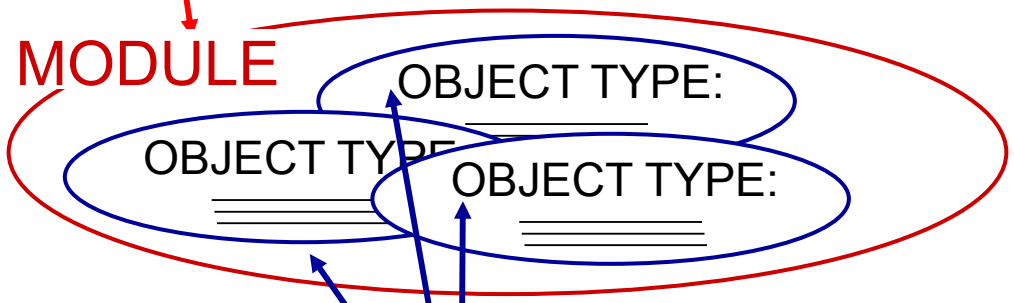
- **Tipos Básicos:**
  - INTEGER.
  - Integer32.
  - Unsigned32.
  - OCTET STRING.
  - OBJECT IDENTIFIER.
  - IPaddress.
  - Counter32.
  - Counter64.
  - Gauge32.
  - Time Ticks.
  - Opaque.

MIB SNMP

MIB module specified via SMI

MODULE-IDENTITY

(100 standardized MIBs, more vendor-specific)



objects specified via SMI

OBJECT-TYPE construct

SMI: Exemplo de Objeto

```
ipSystemStatsInDelivers OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        The total number of datagrams successfully delivered to IP
        user-protocols (including ICMP).

        When tracking interface statistics, the counter of the
        interface to which these datagrams were addressed is
        incremented. This interface might not be the same as the
        input interface for some of the datagrams.

        Discontinuities in the value of this counter can occur at
        re-initialization of the management system, and at other
        times as indicated by the value of
        ipSystemStatsDiscontinuityTime."
    ::= { ipSystemStatsEntry 18 }
```

SMI: Exemplo de Módulo

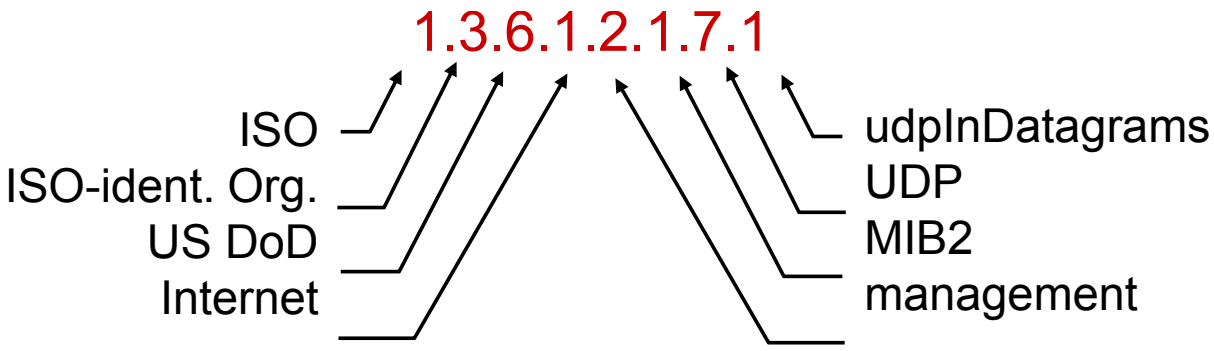
```
ipMIB MODULE-IDENTITY
    LAST-UPDATED "200602020000Z"
     ORGANIZATION "IETF IPv6 MIB Revision Team"
     CONTACT-INFO
         "Editor:
         Shawn A. Routhier
         Interworking Labs
...
     DESCRIPTION
         "The MIB module for managing IP and ICMP implementations, but
         excluding their management of IP routes.
...

     REVISION "200602020000Z"
     DESCRIPTION
         "The IP version neutral revision with added IPv6 objects for
...
     ::= { mib-2 48}
```

Exemplo de MIB: Módulo UDP

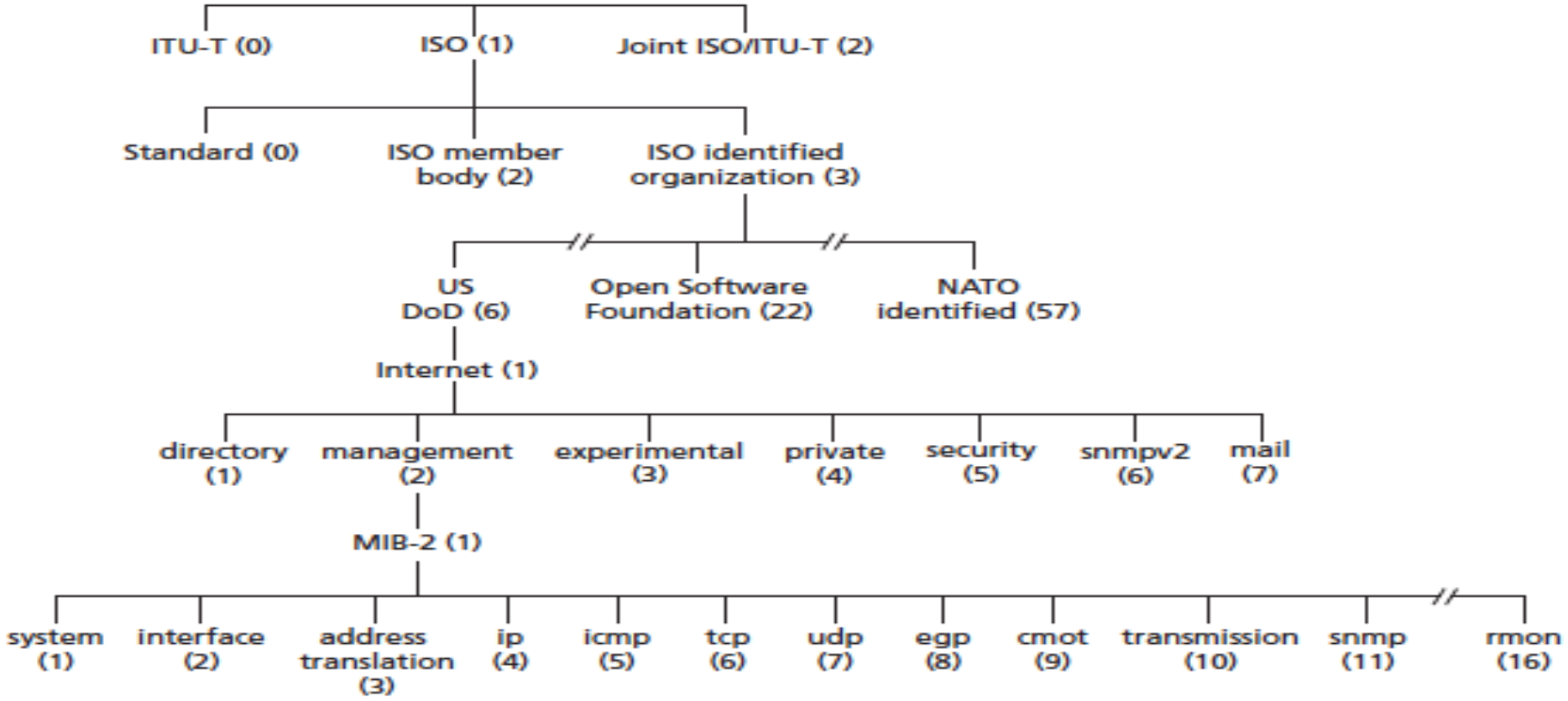
Object ID	Nome	Tipo	Comentário
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	# total de datagramas entregues a este nó
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# de datagramas não entregues: não há aplicação na porta
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	# de datagramas não entregues: qualquer outra razão
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# de datagramas enviados
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	Uma entrada para cada porta em uso por aplicações, apresenta # de porta e endereço IP

SNMP: Nomeação

- **Pergunta:** como nomear todos os possíveis objetos (protocolos, dados, mais...) em todos os possíveis padrões de redes?
- **Resposta:** com a estrutura em árvore do ISO Object Identifier.
  - Nomeação hierárquica de todos os objetos.
  - Cada ponto de ramificação possui um nome e número.

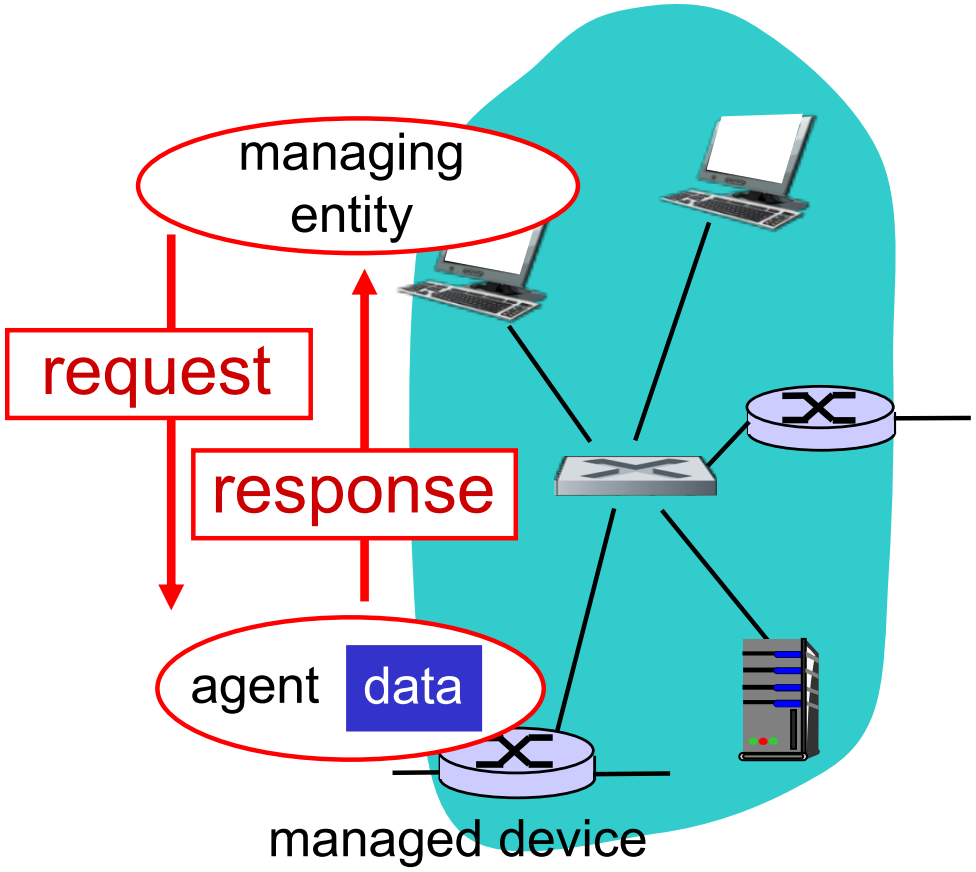


Estrutura em Árvore do ISO Object Identifier

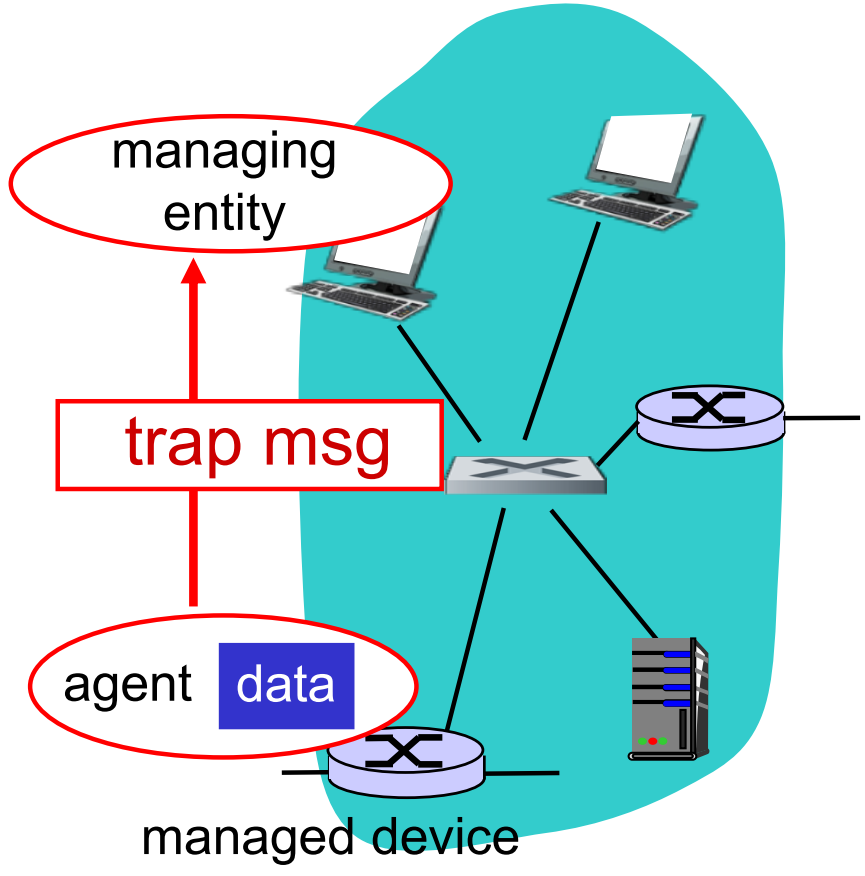


Protocolo SNMP

- Duas formas de enviar informações sobre MIBs ou comandos:



request/response mode

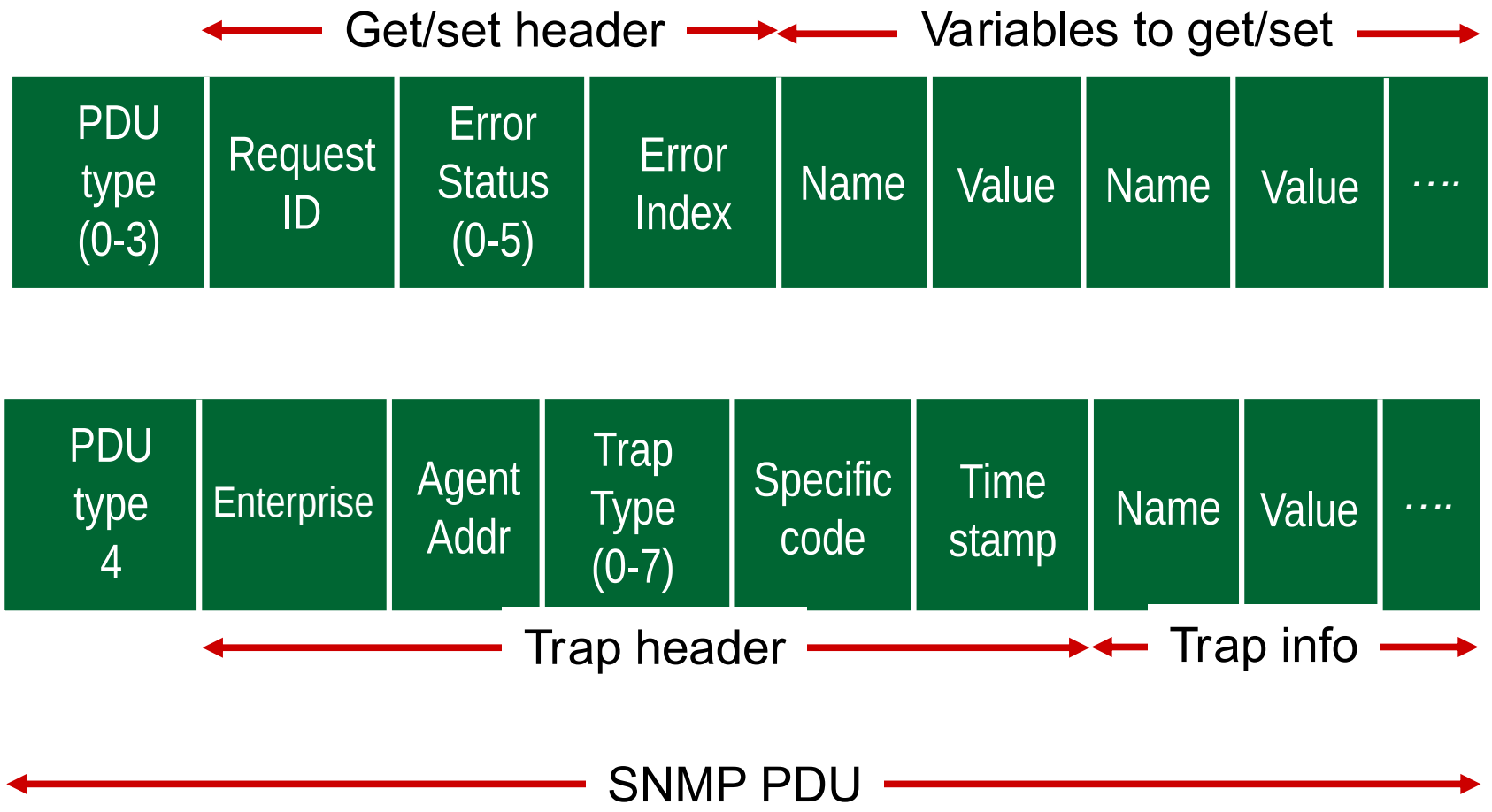


trap mode

Protocolo SNMP: Tipos de Mensagens

Tipo de Mensagem	Função
GetRequest GetNextRequest GetBulkRequest	Gerente para agente: “me envie dados” (uma instância específica, próximo da lista, bloco)
InformRequest	Gerente para gerente: aqui está o valor da MIB.
SetRequest	Gerente para agente: altere o valor da MIB.
Response	Agente para gerente: valor, resposta a requisição.
Trap	Agente para gerente: informar gerente de evento excepcional.

Protocolo SNMP: Formato de Mensagem



Protocolo SNMP: Segurança e Administração

- **Criptografia:** mensagem SNMP criptografada com DES.
- **Autenticação:** computa e envia MIC(m, k).
  - Hash da mensagem m com chave secreta k.
- **Proteção contra ataques de repetição:** usa nonce.
- **Controle de acesso baseado em visões:**
  - Entidade SNMP mantém base de dados de permissões de acesso e políticas para vários usuários.
  - A própria base de dados é acessível na forma de um objeto gerenciado.

Resumo da Aula (I)...

- Gerência de redes:
  - **Monitoramento**, análise, resposta do/ao **comportamento da rede**.
  - Redes são **sistemas complexos**, apresentam **problemas**.
  - Inicialmente, gerência era uma prática quase inexistente.
- Casos de uso:
  - Detecção de falha.
  - Monitoramento de serviços.
  - Monitoramento de tráfego.
  - Detecção de intrusão.
  - ...
- Áreas de gerenciamento:
  - Desempenho.
  - Falhas.
  - Configuração.
  - Contabilização.
  - Segurança.
- Infraestrutura formada por:
  - Dispositivos gerenciados.
  - Agente de gerenciamento.
  - Objetos gerenciados.
  - Entidade gerenciadora.
  - Protocolo de gerenciamento.

Resumo da Aula (II)...

- SNMP: padrão de fato.
  - Transporta informações de gerência.
  - Requisição/resposta ou *traps*.
  - Evoluiu através de 3 versões.
  - Recentemente, preocupação maior com segurança.
- MIBs: bases de dados de gerência.
  - Conjunto de informações de gerência.
  - Semântica, sintaxe definida através de SMI.
  - Organizadas hierarquicamente.
    - *ISO Object Identifier*.

Leitura e Exercícios Sugeridos

- Conceitos básicos de gerência:
  - Páginas 553 a 558 do Kurose (até Seção 9.2, inclusive).
  - Exercícios de fixação 1 a 4 do capítulo 9 do Kurose.
- SNMP, MIBs, SMI:
  - Páginas 560 a 570 do Kurose (Seção 9.3).
  - Exercícios de fixação 5 e 6 do capítulo 9 do Kurose.
  - Problemas 1 a 5 do capítulo 9 do Kurose.
- Opcional: leitura da RFC 789.
  - Disponível em: https://tools.ietf.org/pdf/rfc789.pdf.
  - Questão dissertativa 3 do capítulo 9 do Kurose.

Próxima Aula...

- Última aula (de conteúdo) do período.
- Encerraremos nossa discussão sobre gerência de redes.
- Temas abordados:
  - Interoperabilidade de dados: ASN.1.
  - Exemplos práticos de gerência de redes.