

1

INTERCONEXÃO DE REDES DE COMPUTADORES

Parte 7 Introdução à Gerência de Redes

Prof. Pedro S. Nicolletti (Peter), 2017

Resumo

- Conceitos Básicos de SNMP
 - Introdução
 - Arquitetura
 - MIB
- Segurança SNMPv1, SNMPv2
- Segurança SNMPv3

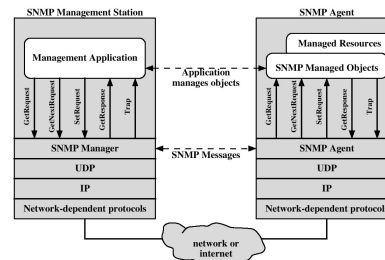
Conceitos Básicos de SNMP Introdução

- Com o crescimento das redes
 - Elas se tornam mais indispensáveis às organizações
 - Mais coisas podem dar errado e levar a rede a uma operação inaceitável
- Com redes grandes
 - Gerenciamento ad-hoc torna-se impraticável (com ping e traceroute)
 - Gerenciamento instrumentado é imprescindível
 - Simple Network Management Protocol (SNMP) é o instrumento para gerência de redes TCP/IP
- Um sistema de gerência de redes é uma coleção de ferramentas para monitoração e controle de redes com
 - Interface única (idealmente WEB)
 - Quantidade mínima de equipamentos distintos
 - Software e capacidade de comunicação embutida em equipamentos gerenciados
- Elementos ativos da rede fornecem informação regular sobre estado de operação para o centro de controle e supervisão da rede

Conceitos Básicos de SNMP Arquitetura

- Elementos chaves
 - **Estação de gerência** – uma (ou mais) estação servidora que realiza a monitoração e controle da rede, disponibilizando informação sobre o estado da mesma
 - **Agente de gerência** – software disponível nos elementos gerenciados que responde as consultas da estação de gerência
 - **Base de Informação de Gerência** (Management Information Base - MIB) – coleção de informação (conjunto de "objetos") disponível em um elemento gerenciado
 - Descrita através da "linguagem" Structure Management Information (SMI)
 - Implementada conceitualmente como uma árvore
 - **Protocolo de Gerência de Rede** – padrão de comunicação entre estação e agente de gerência para a troca de informação entre os mesmos
 - Get - recupera informação de um agente sobre um objeto
 - Set - define o valor de um objeto em um agente
 - Notify - permite ao agente informar o gerente de eventos importantes

Conceitos Básicos de SNMP Arquitetura



Conceitos Básicos de SNMP Arquitetura

- SNMP opera sobre UDP (não orientado a conexão) e é, ele próprio, não orientado a conexão
- Um agente SNMP pode agir como intermediário (proxy) para dispositivos sem suporte a SNMP
- Mais de uma estação de gerência pode atuar em uma rede muito grande
 - cada uma responsabilizando-se pela monitoração de uma parte da rede (distribuição de carga)
 - Duas ou mais concentrando a informação sobre toda a rede (tolerância a falhas)

Conceitos Básicos de SNMP MIB

Detalhamento da MIB...

OBJECT-TYPE

- Nome que identifica um objeto na MIB (Object Identifier - OID).

SYNTAX

- Define que tipo de informação é armazenada no OID.

ACCESS

- Define o tipo de acesso (READ-ONLY, READ-WRITE).

STATUS

- Estado do objeto no contexto da comunidade SNMP.

DESCRIPTION

- Descrição do OID.

::= { <string> <number> }

- <string> = nome do objeto pai

- <number> = índice desse OID (qual filho eu sou)

Standard MIB Object:

sysUpTime **OBJECT-TYPE**

SYNTAX Time-Ticks

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Time since the network management portion of the system was last re-initialized."

::= { system 3 }

Conceitos Básicos de SNMP MIB

Object Identifier (OID)

- Example .1.3.6.1.2.1.1

- iso(1) org(3) dod(6) internet(1)
mgmt(2)
mib-2(1)
system(1)

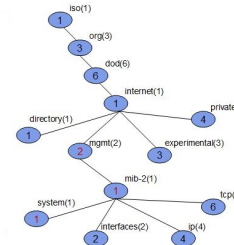
Nota:

- .1.3.6.1 ~100% presente.

- mgmt e private muito comum.

- MIB-2 successor do original MIB.

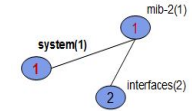
- STATUS 'mandatory'. Deve-se implementar tudo ou nada no grupo



Conceitos Básicos de SNMP MIB

Grupo system(1)

- Contém objetos que descrevem algumas informações básicas de uma entidade gerenciada.
- Uma entidade gerenciada pode ser o próprio agente (software) ou o equipamento onde o agente atua.

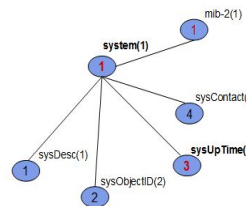


Alguns objetos do grupo system(1)

- **sysDescr(1)** → Descrição da entidade gerenciada.
- **sysObjectID(2)** → Campo definido pelo fabricante da entidade OID string.
- **sysUpTime(3)** → Tempo (segundos) decorrido desde a última inicialização.
- **sysContact(4)** → Nome da pessoa responsável pela entidade.

Conceitos Básicos de SNMP MIB

MIB - tree view



MIB - syntax view

sysUpTime **OBJECT-TYPE**

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The time (in hundredths of a second) since the network management portion of the system was last re-initialized."

::= { system 3 }

Conceitos Básicos de SNMP SNMPv1, SNMPv2 - Ações

SNMPv1	SNMPv2	Direção	Descrição
GetRequest	GetRequest	Gerente → Agente	Requisita informação para cada objeto indicado
GetNextRequest	GetNextRequest	Gerente → Agente	Requisita próxima informação para cada objeto indicado (caminhamento in-order)
-x-	GetBulkRequest	Gerente → Agente	Requisita bloco de informação para cada objeto indicado
SetRequest	SetRequest	Gerente → Agente	Define valor para cada objeto indicado
-x-	InformRequest	Gerente → Gerente	Solicita resumo de informação
GetResponse	Response	Agente → Gerente	Resposta a requisição de gerente
Trap	SNMPv2-Trap	Agente → Gerente	Transmite informação assincronamente

Conceitos Básicos de SNMP SNMPv1, SNMPv2 - Segurança

- SNMPv1/v2 tem mecanismo rudimentar de segurança baseado no conceito de "comunidade"
- Uma comunidade define em um agente, quais gerentes podem acessá-lo e que conjunto de informações podem ser recuperadas e/ou redefinidas
- Três aspectos de segurança
 - Autenticação** – gerente tem de se identificar através de uma comunidade
 - na prática acaba sendo uma senha (quem)
 - Nível de Acesso** – a comunidade define:
 - (a) que operações podem ser feitas (o que: read-only, read-write)
 - (b) sobre que conjunto de informações do agente (onde: a partir de que nó da árvore pode-se solicitar informação)

Conceitos Básicos de SNMP SNMPv1, SNMPv2 - Segurança

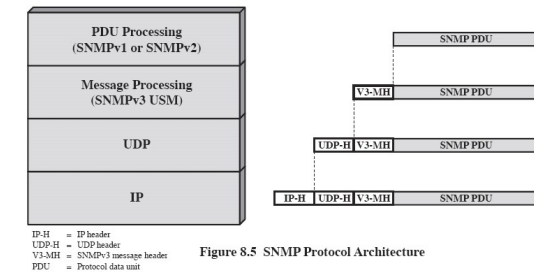
Problemas

- ❑ Todo o tráfego
 - Gerente → Agente,
 - Agente → Gerente,
 - Gerente → Gerente
- ❑ é não criptografado
 - A "comunidade" – uma cadeia de caracteres tipo uma senha – é transmitida como texto
- ❑ A comunicação é, normalmente, via UDP – sem orientação a conexão
 - A "comunidade" é enviada em cada comunicação
- ❑ A "comunidade" pode acabar sendo compartilhada com usuários distintos
- ❑ Não há autenticação rígida de origem (é fácil falsificar um gerente)
- ❑ Proposta de solução: SNMPv3

Conceitos Básicos de SNMP SNMPv3 - Introdução

- ❑ Proposição IETF de 1998 (RFC 2570 a 2576) para incorporar segurança ao SNMPv1 e SNMPv2 (preferencialmente)
- ❑ Não é uma substituição ao SNMPv1/v2
 - Não funciona isoladamente
- ❑ Tipicamente, seria como um SNMPv2 com capacidade de segurança e controle administrativo adicionais
- ❑ Na prática, é como a inserção de um módulo de segurança (tipo Secure Socket Layer) entre a camada SNMPv1/v2 e a camada de transporte (UDP)
 - Essa camada vai prover serviços de autenticação, confidencialidade e integridade na comunicação gerente ↔ agente e gerente ↔ gerente

Conceitos Básicos de SNMP SNMPv3 - Arquitetura



Conceitos Básicos de SNMP SNMPv3 - User Security Model (USM)

- ❑ Projetado para proteger contra
 - Modificação de informação (integridade)
 - Falsificação de origem (autenticação)
 - Modificação em trânsito (integridade)
 - Exposição de informação (confidencialidade)
- ❑ Não é projetado para proteger contra
 - Ataque de proibição de serviço (DOS)
 - Análise de tráfego
- ❑ Para oferecer os serviços necessários, faz uso de identificação individual de usuário, assinatura digital e criptografia simétrica
 - Cada usuário cadastrado em um agente tem identificação própria (login/senha)
 - Chaves para assinatura digital (MAC) e criptografia são definidas estaticamente nas entidades (gerente, agente) para cada usuário

Conceitos Básicos de SNMP SNMPv3 - View-based Access Control Model (VACM)

- ❑ Controle de acesso no SNMPv3 é regido pelo modelo baseado em visão - VACM
- ❑ VACM tem duas características
 - Determina se o acesso a um objeto gerenciado deve ser permitido ou não para um usuário
 - Faz uso da MIB que
 - Define a política de controle de acesso para o agente
 - Permite o uso de configurações de controle de acesso remotas