Redes de Computadores II

Aula 14 - Gerenciamento de Redes – Parte II

Apresentação

Na aula anterior iniciamos nosso estudo sobre gerenciamento de redes, parte fundamental da administração de uma rede de computadores. Nesta aula continuaremos nossos estudos do protocolo SNMP, estendendo nosso conhecimento em relação as MIBs (Base de Informações de Gerenciamento) citadas anteriormente. Veremos também o protocolo de gerenciamento RMON, assim como a ferramenta de gerência de redes conhecida como CACTI.

Objetivos

Ao final desta aula você será capaz de:

- Descrever a base MIB-II
- Identificar as mensagens SNMP
- Conhecer as diferentes versões do SNMP
- Instalar o SNMP em servidores Linux
- Conhecer o protocolo RMON e a ferramenta CACTI

MIB-II

Na aula anterior, aprendemos o que é MIB, ou Base de Informações de Gerenciamento. Cada MIB contém um conjunto de informações que de certo modo estão relacionadas de alguma forma. Uma das MIB mais utilizadas é a MIB-II. Essa MIB deve ser implementada por qualquer agente SNMP, ou seja, todos os equipamentos que suportam SNMP têm que suportar essa MIB.

Os objetos (variáveis) desta MIB são divididos nos grupos mostrados no Quadro 1.

Nome do Grupo	Contém informações sobre
System	Informações básicas sobre o sistema.
Interfaces	Interfaces de rede.
at	Tradução de endereços.
Ip	Protocolo IP.
Icmp	Protocolo ICMP.
Tcp	Protocolo TCP.
Udp	Protocolo UDP.
Egp	Protocolo EGP.
Transmission	Meios de transmissão.
snmp	Protocolo SNMP.

Quadro 1 - Grupos da MIB-II

Cada um desses grupos contém uma série de objetos. No Quadro 2, podemos ver exemplos de objetos de alguns grupos da MIB-II.

Grupo System	
sysDescr	Descrição do equipamento. Pode incluir fabricante e modelo.
sysUpTime	Tempo desde a última reinicialização.
sysContact	Nome de uma pessoa de contato responsável pelo equipamento.
Grupo Interfaces	
ifNumber	Número de interfaces de rede existentes na máquina.
ifOperStatus	Estado atual da interface (ativada ou desativada)
ifInOctets	Número de bytes recebidos pela interface.
Grupo IP	
ipForwarding	Se o roteamento está ativo (se atuando como roteador).
ipInHdrErrors	Número de pacotes recebidos e descartados devido a erros.
Grupo TCP	
tcpCurrentEstab	Número de conexões TCP estabelecidas no momento.

Quadro 2 - Exemplos de objetos da MIB-II

Identificadores de Objetos – OID

Você deve se lembrar, no nosso estudo sobre o DNS, que para ajudar a definir nomes únicos para as máquinas na Internet, os nomes são organizados em uma estrutura em árvore.

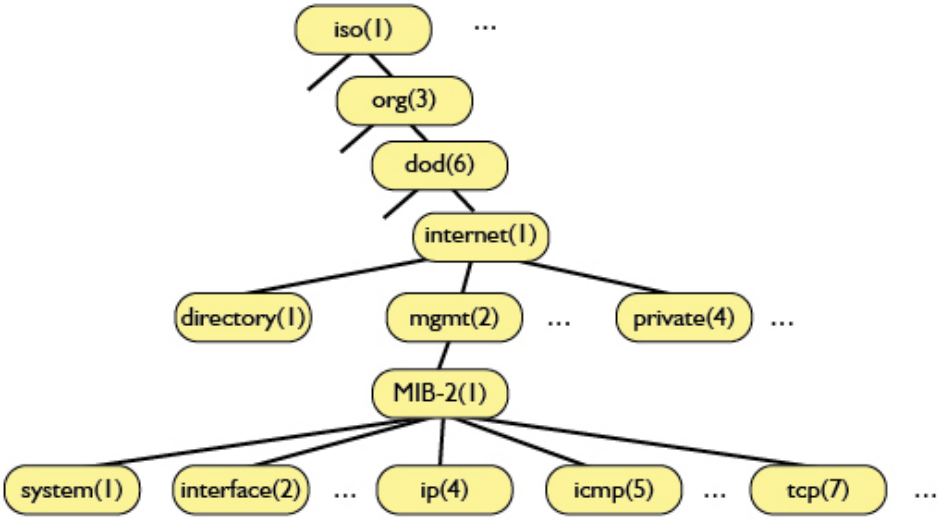
Como precisamos garantir que os nomes das MIB, e dos seus objetos sejam únicos, eles também são definidos usando uma estrutura em árvore. Portanto, o nome de uma MIB é formado pelos nomes de todos os nós desde a raiz da árvore até o nome do nó que representa a MIB, separados por um sinal de ponto (.), como no DNS.

A diferença do DNS é que lá o nome é escrito iniciando do nó representando a máquina, seguindo até a raiz da árvore, e nas MIB, o nome é escrito iniciando da raiz da árvore, e seguindo em direção ao nó que representa a MIB.

Os nomes dos objetos de uma MIB são definidos do mesmo modo, com a diferença que eles são nós-filhos do nó representando a MIB.

Outra diferença importante em relação ao DNS é que aqui cada nó da árvore tem um número, além de um nome. E pode-se usar a sequência de números para identificar cada nó da árvore (também separados pelo sinal de ponto). A Figura 1 ilustra esse esquema.

Figura 01 - Árvore com os identificadores de objetos



O nó ip, por exemplo, pode ser identificado por **iso.dod.org.internet.mgmt.mib-2.ip** ou por **1.3.6.1.2.1.4**.

Do mesmo modo, os objetos dentro do grupo *ip* da *mib-2* terão este prefixo (identificador do nó ip). Assim sendo, o objeto *ipForwarding*, por exemplo, é identificado por 1.3.6.1.2.1.4.1, enquanto *ipInHdrErrors* é identificado por 1.3.6.1.2.1.4.4. Concluímos portanto, que *ipForwarding* é um nó com identificador 1 (abaixo do nó ip) e *ipInHdrErrors* é um nó com identificador 4 (abaixo do nó ip).

A definição formal de uma MIB é feita em um arquivo texto seguindo uma notação bem definida, chamada de ASN.1. Essa notação determina, por exemplo, o tipo de dados (INTEGER, BOOLEAN,...) de cada objeto da MIB. Além disso, como as mensagens SNMP são transmitidas entre máquinas que podem ter arquiteturas de hardware diferentes, e, portanto, representar os tipos de dados de maneiras diferentes, existe ainda um mecanismo que define como os objetos devem ser representados para serem transmitidos pela rede.

Esse mecanismo se chama BER (*Basic Encoding Rules*) e garante que qualquer máquina seja capaz de entender as informações transmitidas.

Veja aqui a explicação em vídeo sobre as MIBs

Vídeo 01 - Gerência Mibs

Atividade 01

1. Qual o OID do grupo “tcp” da MIB-2?

As mensagens do protocolo SNMP

Como você já sabe, as mensagens SNMP são transmitidas em pacotes UDP. Veremos a seguir as principais mensagens do SNMP.

- Mensagem **GetRequest** – É enviada pelo gerente aos agentes para solicitar o valor de um ou mais objetos. Em uma mesma mensagem são indicados todos os objetos desejados. Existem algumas variações dessa mensagem, como a mensagem GetNextRequest, utilizada para ler os próximos objetos, e GetBulkRequest, utilizada para obter um grande conjunto de informações.

- Mensagem **SetRequest** – É enviada pelo gerente aos agentes para definir o valor de um ou mais objetos. Em uma mesma mensagem são indicados todos os objetos para os quais se deseja alterar o valor.

- Mensagem **Response** – Enviada pelo agente para o gerente em resposta a uma mensagem GetRequest ou SetRequest. No primeiro caso, contém o valor de todos os objetos solicitados. No segundo caso, contém uma indicação se a alteração no valor do(s) objeto(s) foi realizada com sucesso.

- Mensagem de **Trap** – São enviadas pelos agentes ao gerente quando alguma condição definida previamente pelo gerente é atingida.

Evidentemente, os nomes de objetos utilizados nessas mensagens devem estar definidos em alguma MIB sendo utilizada pelos equipamentos.

As versões do protocolo SNMP

Existem três versões do protocolo SNMP, conhecidas como SNMPv1, SNMPv2 e SNMPv3. Apesar de existirem algumas diferenças entre elas, como o fato da versão 2 ter inserido o suporte à comunicação entre os gerentes, e permitido contadores de 64 bits, focaremos nossa discussão nas características de segurança.

Nas versões 1 e 2, a segurança é baseada no conceito de **comunidade**. Uma comunidade não passa de uma senha que garante acesso de **somente leitura**, ou **leitura e escrita** à MIB. Ou seja, são definidas as comunidades nos agentes e os gerentes devem informar o nome de uma comunidade quando tentar realizar alguma operação no agente.

O SNMPv3 incluiu o suporte a usuários, e um controle de acesso eficiente às MIBS. Pode-se definir, por exemplo, qual parte da MIB (subárvore) pode ser acessada por um determinado usuário.

Também foi incluído suporte à criptografia utilizando o algoritmo simétrico DES, que é baseado na utilização de uma chave compartilhada, de modo a proteger as mensagens transmitidas contra leitura indevida ou adulteração.

Todas as mensagens SNMP devem conter um campo indicando a versão do protocolo utilizado, bem como as informações de autenticação (nome da comunidade ou usuário e senha) necessárias.

Veja aqui a explicação em vídeo sobre as mensagens e as diferentes versões do protocolo SNMP.

Vídeo 02 - Mensagens Versões

Atividade 02

1. Existem diversas MIB. Marque a alternativa correta.

    a. Cada agente SNMP tem que suportar todas elas.

    b. Cada agente pode suportar apenas as MIB que desejar.

    c. Cada agente pode suportar apenas as MIB que desejar, mas existe uma MIB que todas devem suportar.

    d. Não são os agentes que precisam ter suporte as MIB. Quem precisa é apenas o gerente.

Instalando e configurando o SNMP em servidores Linux

Agora que já entendemos como o protocolo funciona, vamos ver como instalá-lo em uma máquina Linux (distribuição baseada no debian, como o Ubuntu). Para isso,deve-se instalar um pacote chamado “snmpd”, que é um programa que implementa um agente SNMP. Naturalmente, ele irá executar em *background*.

```
1 apt-get install snmpd
```

A configuração do agente é feita através do arquivo *snmpd.conf*. Por padrão, o arquivo já permite acesso de leitura a MIB-2 utilizando o nome de comunidade *public*. Caso deseje editar algo no arquivo, basta abri-lo em um editor de texto comum, conforme mostrado a seguir.

```
1 gedit /etc/snmp/snmpd.conf
```

Quando se faz alguma alteração no arquivo, é necessário reiniciar o snmpd, através do comando:

```
1 /etc/init.d/snmpd restart
```

A instalação dos programas para consultar o agente (ou seja, programas que fazem o papel do gerente), basta instalar o pacote a seguir.

```
1 apt-get install snmp
```

Esse pacote contém vários programas para enviar as diversas mensagens SNMP (um programa diferente para cada mensagem). Por exemplo: snmpget, snmpset, snmptrap, snmpgetnext, etc.

Um programa interessante é o **snmpwalk** que utiliza mensagens GetNextRequest para obter todos os objetos de uma determinada subárvore da MIB.

Segue um exemplo da utilização desse comando para mostrar todos os objetos do grupo **system** da MIB-II, utilizando o nome de comunidade **public** e assumindo que o IP do agente é 10.1.1.5.

```
1 snmpwalk -Os -c public -v 1 10.1.1.5 system
```

Ao invés da palavra **system** poderia ter sido utilizado a representação com números desse grupo da MIB-2, que é 1.3.6.1.2.1.1.

Vídeo 03 - SNMP

Atividade 03

1. Pesquise por algum programa que tenha uma interface gráfica e permita ver a MIB. Normalmente esses programas são chamados **MIB Browsers**. Instale o programa e tente acessar o seu agente.

Veja aqui a explicação em vídeo sobre a configuração de um agente SNMP no Linux.

Vídeo 04 - SNMP Linux

O Protocolo de gerenciamento RMON

O RMON é um padrão IETF (***I**nternet **E**ngineering **T**ask **F**orce*) de gerenciamento de redes cuja sigla representa ***R**emote **M**onitoring **N**etwork*. Basicamente, ele é uma MIB padrão do protocolo SNMP (no qual ele foi baseado) que visa facilitar a gerência de redes remotas, ou seja, redes distantes do gerente.

Para entender a necessidade do RMON pense na seguinte situação. Imagine que você tem uma rede em uma filial que pretende monitorar remotamente, mas a estação gerente se encontra na matriz. Existe um link ligando a matriz e a filial, que possui uma capacidade relativamente baixa.

Imagine que a rede da filial está muito lenta e você pretende descobrir as máquinas que mais geram tráfego naquela rede. Como você já estudou, a estação gerente iria interrogar continuamente cada máquina da filial e calcular o tráfego gerado por cada uma, de modo a gerar uma lista com todas as máquinas. Isso, entretanto, iria gerar muito tráfego no link entre a matriz e a filial!

É aí que entra o RMON. Com ele, um agente na filial (com a MIB RMON) se encarregaria de ficar capturando o tráfego na filial e gerando a lista com todas as máquinas. O gerente apenas solicitaria essa lista já pronta!

> Existe a versão 1 e a versão 2 do RMON. Enquanto a versão 1 se encarrega de analisar informações das camadas 1 e 2 (física e enlace), a versão 2 consegue monitorar as camadas superiores, como rede e transporte.

Veja aqui a explicação em vídeo sobre o RMON

Vídeo 05 - RMON

Ferramentas que utilizam o SNMP

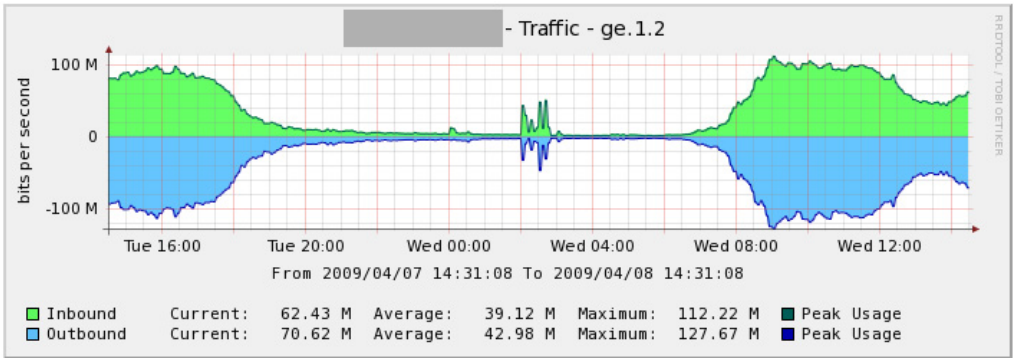
Anteriormente, nesta aula, utilizamos o programa snmpwalk, que faz parte do pacote snmp, para obter informações de um agente snmp.

É muito comum, entretanto, utilizar programas mais completos que apresentam as informações coletadas dos agentes de uma forma muito mais amigável para o usuário.

Uma forma comum de mostrar as informações é representar em um gráfico o valor da informação ao longo do tempo. Pode-se, por exemplo, gerar gráficos diários, semanais, mensais e anuais.

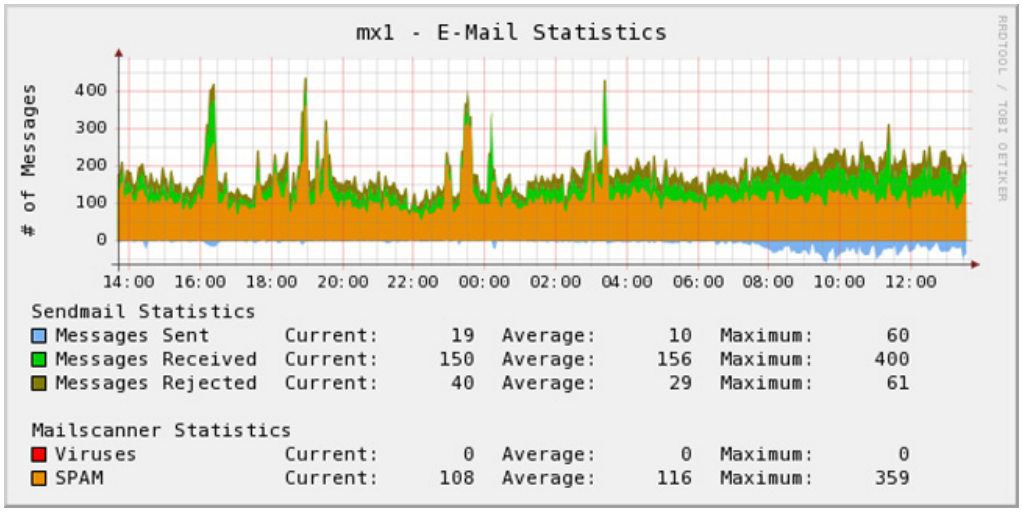
Um dos programas bastante utilizados para essa tarefa é o CACTI (http://www.cacti.net). A Figura 2 mostra um exemplo de saída do CACTI, no qual é mostrado o consumo de banda do link Internet. Isso possibilita vermos se o link está sobrecarregado, e em que horários do dia isso acontece.

Figura 02 - Gráfico do tráfego diário em um link



A Figura 3 mostra uma visão detalhada do funcionamento do servidor de e-mail, indicando a quantidade de mensagens enviadas, recebidas e descartadas. Além disso, também é mostrado o total de spams e vírus recebidos. Esse gráfico também foi gerado pelo CACTI.

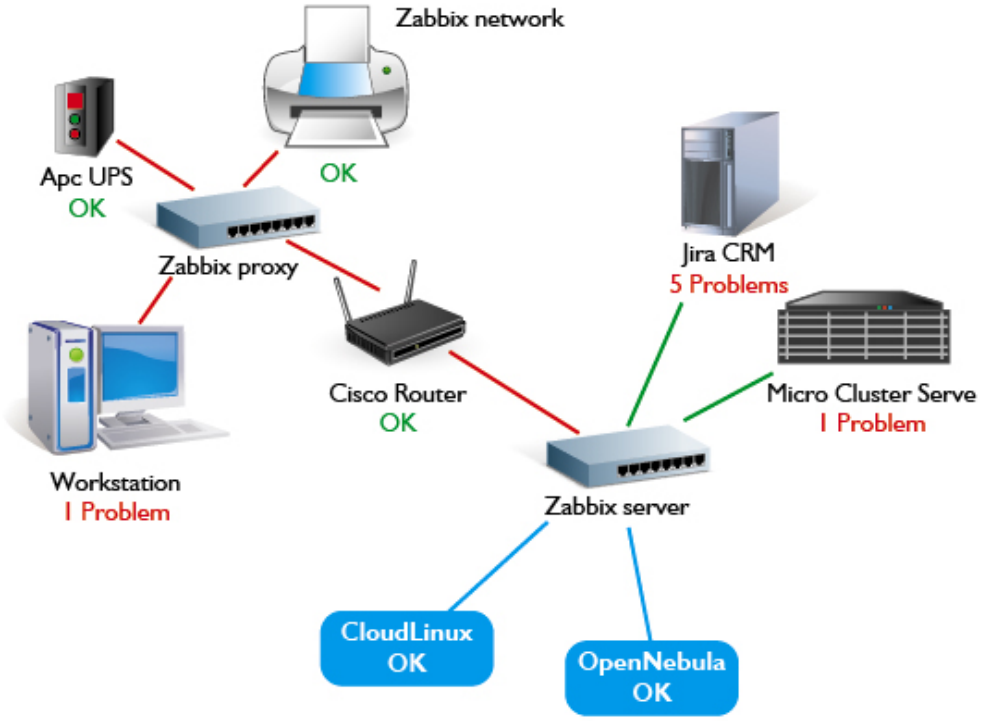
Figura 03 - Gráfico com estatísticas de e-mails



Existem vários outros programas que fazem o papel do gerente, e oferecem tanto opções de monitoramento quanto de configuração dos agentes. Dois exemplos são o Nagios <http://www.nagios.com/products/nagiosxi/screenshots> e o Zabbix <http://www.zabbix.com/screenshots.php>. Naturalmente, esses programas vão muito além da geração de gráficos.

A Figura 4 mostra uma tela do Zabbix, na qual aparece uma rede com a indicação dos locais (equipamentos e links) que apresentam problemas.

Figura 04 - Tela do Zabbix



Fonte: <http://www.zabbix.com/screenshots.php> Acesso em: 13 nov. 2012.

Veja aqui a explicação sobre ferramentas de gerenciamento.

Vídeo 04 - SNMP Linux

Resumo

Nesta aula você aprendeu que a forma mais comum de realizar a gerência de uma rede é através do protocolo SNMP, que utiliza agentes e gerentes, e possui um conjunto reduzido de mensagens para ler e definir valores de variáveis (objetos) suportadas pelos agentes. Viu também que essas variáveis são definidas através de MIB que precisam estar instaladas nos equipamentos. Você também conheceu exemplos de ferramentas existentes para atuarem como um gerente SNMP. Finalmente, você conheceu um pouco sobre o protocolo RMON, assim como teve contato com ferramentas de gerenciamento de redes, como o CACTI.

Autoavaliação

1. Quais as mensagens do protocolo SNMP que estudamos nesta aula?
2. O que é uma mensagem Trap?
3. Cite quatro grupos, e dois objetos de cada grupo, para a MIB-II.
4. Qual é a relação entre o RMON e SNMP?

Referências

INTRODUÇÃO a Gerenciamento de Redes TCP/IP. Boletim bimestral sobre tecnologia de redes, RNP, v. 1, n. 3, 15 jan. 1997.Disponívelem: <https://memoria.rnp.br/newsgen/9708/n3-2.html>. Acesso em: 10 out. 2012.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5.ed. São Paulo:Addison Wesley, 2010.

LESSA, Demiam. O Protocolo de Gerenciamento RMON. Boletim bimestral sobre tecnologia de redes, RNP, v. 3, n. 1, 15 jan. 1999. Disponível em: <https://memoria.rnp.br/newsgen/9901/rmon.html>. Acesso em: 10out. 2012.

Maura, D.; Schmidt, **SNMP Essencial.O'Reilly**, 2005.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.3rd ed**.New York: Addison-Wesley, 1999.

WALSH, L. **SNMP MIB**: Essential Guide to MIB Development, Use, and Diagnosis Handbook. London: Wyndham Press, 2008.