Unidade II

3 MODELO DE GERENCIAMENTO ISO

O gerenciamento está associado ao controle de atividades e ao monitoramento do uso dos recursos da rede. A tarefa básica que uma gerência de rede deve executar envolve a obtenção de informações desta, bem como o tratamento dessas informações, possibilitando um diagnóstico seguro e o encaminhamento das soluções dos problemas. Para cumprir estes objetivos, as funções de gerência devem ser embutidas nos diversos componentes da rede, possibilitando descobrir, prever e reagir a adversidades.

Para resolver os problemas associados à gerência em redes, a ISO desenvolveu o padrão denominado OSI, o qual contempla três modelos:

- Modelo organizacional: estabelece a hierarquia entre sistemas de gerência em um domínio de gerência, dividindo o ambiente a ser gerenciado em vários domínios.

- Modelo informacional: define os objetos de gerência, as relações e as operações sobre esses objetos. Uma base de informações de gerenciamento é necessária para armazenar os objetos gerenciados.

- Modelo funcional: descreve as funcionalidades de gerência: gerência de falhas, gerência de configuração, gerência de desempenho, gerência de contabilidade e gerência de segurança.

Visando suprir a necessidade de um desenvolvimento de gerenciamento que seja semelhante a todos os fabricantes, a ISO estabeleceu padrões de gerenciamento, a fim de promover a interoperabilidade de múltiplas e diferentes redes de comunicação e sistemas operacionais.

Nesses padrões, são especificados os serviços, os protocolos para intercâmbio das informações de gerenciamento, as funções, a sintaxe e a semântica das informações de gerenciamento. O objetivo é suportar o controle e a monitoração dos sistemas e recursos associados.

A ISO também dividiu as atividades em cinco área funcionais específicas (SMFA), assim como as redes TMN já tinham feito.

FCAPS: modelo OSI de gerenciamento

- Fault: gerenciamento de falhas.

- Configuration: gerenciamento de configuração.

- Account: gerenciamento de contabilidade.
- Performance: gerenciamento de desempenho.
- Security: gerenciamento de segurança.

Para cada área funcional foram desenvolvidos padrões de funções que incluem requisitos, serviços e modelos para o gerenciamento das redes. Existe uma certa sobreposição de requisitos e necessidades do usuário. Dessa forma, algumas funções desenvolvidas para uma área funcional também podem ser aproveitadas em outra.

O gerenciamento de falhas compreende a detecção de falhas, assim como o isolamento e a correção de operações anormais do ambiente OSI. Já o gerenciamento de configurações fornece insumos para a preparação, a iniciação, a operação contínua e a posterior interrupção dos serviços de interconexão de sistemas abertos. No gerenciamento de contabilidade são realizadas funções para informar os usuários sobre os recursos consumidos ou custos, a fim de associar o uso de recursos com escalas de tarifação e combinar recursos, visando atingir a comunicação. O gerenciamento de desempenho permite avaliar o comportamento de recursos no ambiente da rede, obtendo informações estatísticas de desempenho histórico. O gerenciamento de segurança, por fim, apoia a aplicação de políticas de segurança, incluindo funções como criação, controle e eliminação de mecanismos de segurança.

3.1 Componentes de gerência OSI

O ambiente de gerenciamento OSI é composto de elementos gerenciados, agentes e gerentes. Os elementos gerenciados são representados por objetos gerenciados, seguindo o paradigma da Abordagem de Orientação a Objetos. Os papéis assumidos por estas entidades não são fixos, isto é, um MIS-User pode executar o papel de gerente em um contexto, definido por uma associação, e o papel de agente em outro contexto, definido por outra associação.

Lembrete

Os agentes e gerentes são entidades usuárias do serviço de gerenciamento OSI e são denominados de MIS-Users (Management Information Service – Users).

No modelo de gerenciamento OSI, o número de associações estabelecidas entre os MIS-Users é considerado uma questão local, dependente de implementação. Conforme mostra a figura a seguir, pode-se ter um gerente associado a vários agentes e um agente associado a vários gerentes. Estas associações são estabelecidas com a finalidade de trocar informações de gerenciamento.

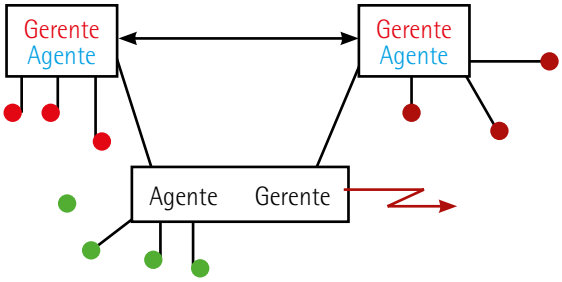

Figura 13 – Componentes do gerenciamento OSI

3.1.1 Funções e serviços CMISE

O CMISE (Common Management Information Service Element) consiste de uma definição de serviço (CMIS) e de uma especificação de protocolo (CMIP).

Os serviços e o protocolo são especificados pela definição de várias operações que podem ser invocadas pela aplicação de gerenciamento (no papel de gerente) sobre objetos gerenciados e pela definição de notificações que são emitidas pela aplicação de gerenciamento (no papel de agente) como resultado de algum evento ocorrido nos objetos gerenciados, para o gerente.

A definição do CMISE é especificada em termos do serviço que a máquina de protocolo proporciona a seus usuários e pela sintaxe e semântica das Unidades de Dados de Protocolo (PDUs) trocadas entre entidades pares.

O protocolo é baseado no paradigma *request/reply*, em que o invocador requisita a execução de uma operação sobre um ou mais objetos gerenciados. O sistema que invoca a operação atua no papel de gerente e o sistema que recebe a operação atua no papel de agente. O executor da operação possui o processo agente que proporciona a interface de comunicação externa e uma visão dos objetos gerenciados em uma estrutura de árvore.

As operações de gerenciamento consistem em troca de unidades de protocolo para criar, destruir, ler e modificar a informação de gerenciamento, bem como executar ações específicas do objeto gerenciado. O termo **informação de gerenciamento** é usado aqui para referenciar objetos gerenciados e suas propriedades.

Além das operações já mencionadas, o protocolo suporta a transferência de relatórios que descrevem eventos ocorridos nos objetos gerenciados.

3.2 Estrutura de Informação de Gerenciamento (SMI)

As informações de gerenciamento são organizadas em bases de dados. O conjunto das bases de dados de informações de gerenciamento é denominado MIB (Management Information Base). A implementação das MIBs não está sujeita à padronização, visto que as informações são definidas segundo uma Estrutura de Informação de Gerenciamento (Structure of Management Information – SMI).

No modelo de gerenciamento OSI, a SMI utiliza, como forma de representação das informações, o modelo orientado a objetos, com três hierarquias: hierarquia de herança, hierarquia de nomeação (ou de *containment*) e hierarquia de registro.

3.3 Serviços de gerenciamento

Os serviços definidos em ISO/IEC 9595 são:

- M-Get: para ler o valor de um conjunto de atributos de um objeto.
- M-Set: para substituir o valor de um conjunto de atributos de um objeto.
- M-Create: para criar uma instância de objeto de uma determinada classe.
- M-Delete: para destruir uma instância de objeto.
- M-Action: para solicitar que uma instância de objeto realize uma determinada ação.
- M-Event-Report: para avisar a ocorrência de um evento em um objeto.
- M-Cancel-Get: para cancelar uma operação de leitura realizada sobre múltiplos objetos.

Os serviços M-Set, M-Action, M-Delete e M-Event-Report podem ser requisitados tanto no modo confirmado quanto no modo não confirmado, enquanto os serviços M-Get, M-Create e M-Cancel-Get são sempre confirmados.

Alguns destes serviços podem ser requisitados de forma que a operação seja executada sobre um objeto individual ou sobre múltiplos objetos. O mecanismo para seleção de múltiplos objetos é descrito como uma combinação dos mecanismos de escopo (*scoping*) e filtro (*filtering*).

O mecanismo de *scoping* pode ser utilizado pelo usuário do serviço CMIS para identificar os objetos gerenciados que são candidatos à execução de uma operação particular, utilizando um dos métodos seguintes: selecionar todos os objetos em uma subárvore; selecionar objetos em um nível particular de uma subárvore.

A raiz da subárvore é indicada por um parâmetro cujo valor é o identificador de um objeto denominado **objeto gerenciado base**.

Filtering é um mecanismo de aplicação de critérios para selecionar objetos a fim de determinar se uma operação deve ou não ser executada sobre o objeto. O parâmetro *filter* é um conjunto de uma ou mais asserções sobre a presença ou o valor de um atributo em um objeto gerenciado.

As asserções sobre o valor de um atributo são avaliadas usando regras de comparação associadas com o tipo do atributo. São definidas as seguintes regras de comparação:

- *equality*: avaliado como *true* se e somente se existe um valor de atributo igual ao declarado;
- *greater or equal*: avaliado como *true* se e somente se o valor do atributo fornecido na asserção de valor do atributo é maior ou igual ao valor do atributo;
- *less or equal*: avaliado como *true* se e somente se o valor do atributo fornecido na asserção de valor do atributo é menor ou igual ao valor do atributo;
- *present*: avaliado como *true* se e somente se tal atributo está presente no objeto gerenciado;
- *substring*: avaliado como *true* se e somente se existe um valor de atributo no qual o *substring* especificado aparece em uma determinada ordem;
- *subset of*: avaliado como *true* se e somente se todos os membros declarados estão presentes no atributo;
- *superset of*: avaliado como *true* se e somente se todos os membros do atributo estão presentes na asserção de valor do atributo;
- *non-null set intersection*: avaliado como *true* se e somente se no mínimo um dos membros declarados está presente no atributo.

Além dos mecanismos de *scoping* e *filtering*, também é definido um mecanismo de sincronização (*synchronization*), que indica a forma que uma operação de gerenciamento deve ser sincronizada sobre instâncias de objetos gerenciados, quando múltiplos objetos gerenciados foram selecionados através dos mecanismos de escopo e filtro. Duas técnicas de sincronização foram definidas: melhor esforço (*best effort*) e atômica (*atomic*).

A sincronização de melhor esforço, quando escolhida para a execução de uma operação, indica que a operação deve ser executada sobre todos os objetos selecionados pelo mecanismo de escopo para os quais é possível a execução da operação. Para aqueles que a operação falha, deve ser retornada uma mensagem de erro. Para o caso em que a sincronização atômica é escolhida, se a operação falhar em pelo menos um dos objetos selecionados, ela não deverá ser executada em nenhum dos outros, mesmo que seja possível.

A sincronização atômica pode ser comparada ao mecanismo de operações atômicas oferecido pela camada de sessão do modelo de referência OSI. A ordem em que os objetos gerenciados são selecionados para a execução da operação é considerada uma questão local e, portanto, dependente da implementação. O CMIS não fornece um parâmetro para indicar sincronização de atributos de um objeto, isto é, não existe uma forma de executar uma operação com sincronização atômica sobre vários atributos de um mesmo objeto.

Os serviços de gerenciamento disponíveis para as entidades gerentes e agentes são definidos pelo CMIS, descrito em ISO/IEC 9595. Neste documento são definidos dois serviços de gerenciamento: o serviço de

operações de gerenciamento e o serviço de notificações de gerenciamento. As operações de gerenciamento são emitidas pelos MIS-Users, que são entidades de gerenciamento no papel de gerente; as notificações também são emitidas pelos MIS-Users que assumem o papel de agente neste caso. A figura a seguir mostra um cenário de comunicação em que são trocadas operações e notificações de gerenciamento.

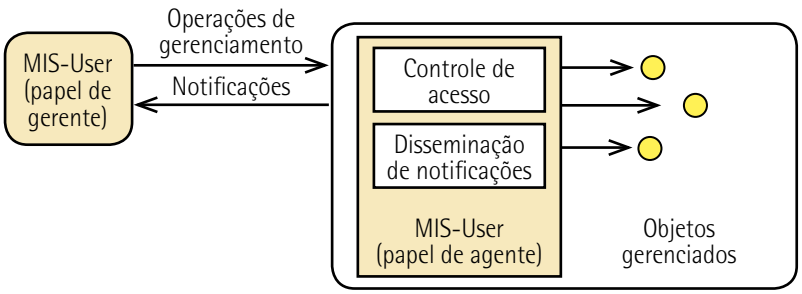

Figura 14 – Serviços de gerenciamento

As operações de gerenciamento podem sofrer um controle de acesso dependendo da especificação dos objetos gerenciados, isto é, dependendo da definição do objeto, a operação pode ter sucesso ou ser negada ao MIS-User solicitante. Na figura anterior, observa-se que existe uma função de controle de acesso associada ao MIS-User agente. Esta função tem como objetivo principal autenticar o gerente na solicitação de uma associação e verificar sua autoridade na execução de operações de gerenciamento.

As notificações representam informações sobre eventos ocorridos no sistema gerenciado e são enviadas ao destinatário através da utilização do serviço M-Event-Report, definido no CMIS. Também na figura anterior, pode-se observar a função de disseminação de notificações, que consiste em um suporte funcional ao MIS-User agente para a identificação dos destinatários para os quais devem ser repassadas as notificações geradas pelos objetos gerenciados

Embora uma notificação possa ser gerada como efeito colateral de uma operação de gerenciamento, ela não pode ser considerada como uma resposta a uma operação. As operações de gerenciamento são emitidas por iniciativa de um gerente. Se uma operação de gerenciamento for solicitada no modo confirmado, então ela será respondida através das primitivas *response* e *confirm*; caso contrário, nenhuma resposta será gerada. Uma notificação é emitida por iniciativa do MIS-User agente, que, por sua vez, pode solicitar este serviço no modo confirmado ou não confirmado, como vimos previamente.

3.4 Protocolos de gerenciamento CMIP

A comunicação entre as entidades de gerenciamento (gerente e agente) é realizada pelo protocolo CMIP (Common Management Information Protocol), definido em ISO/IEC 9596.

No caso especial de gerenciamento de redes de telecomunicações, também é permitida a utilização do protocolo FTAM (File Transfer Access and Management) para a transferência de informações de gerenciamento entre agentes e gerentes. Esta facilidade tornou-se essencial devido à necessidade de transferência de grandes quantidades de dados neste ambiente.

O CMIP especifica os elementos de protocolo que devem ser utilizados para fornecer os serviços de operação e notificação do CMIS. As operações podem ser:

- Classe 1: confirmada síncrona.
- Classe 2: confirmada assíncrona.
- Classe 5: não confirmada assíncrona.

O CMIP é especificado em termos das várias semânticas das operações, da sintaxe das informações trocadas e dos procedimentos que devem ser suportados pela máquina de protocolo.

A máquina de protocolo CMIPM (Commom Management Information Protocol Machine) recebe as primitivas de serviço *request* e *response* do usuário do serviço CMIS (MIS-User) e emite PDUs que serão transferidas através dos serviços oferecidos pelo elemento de serviço Remote Operation Service Element (Rose).

Por outro lado, a CMIPM remota recebe as PDUs do Rose e as encaminha através de primitivas *indication* e *confirm* apropriadas, para o MIS-User correspondente.

Os procedimentos de protocolo somente indicam como interpretar cada um dos campos existentes na PDU, mas não indicam como o usuário deve processar a informação recebida.

A sintaxe das unidades de dados do protocolo é especificada usando uma sintaxe denominada ASN.1 (Abstract Syntax Notation One).

A estrutura de gerenciamento refere-se aos três enfoques definidos pela ISO em seu *framework* (ISO 7498-4): gerenciamento de sistemas, gerenciamento de camada e operação de camada.

O **gerenciamento de sistemas** foi idealizado para monitorar e controlar o sistema como um todo. Para tanto, prevê funções de gerenciamento em todas as camadas da pilha de protocolos e seu escopo de abrangência é o mais completo.

O **gerenciamento de camada** consiste na monitoração e no controle dos recursos de uma camada de forma isolada e independente. Pode-se, por exemplo, enfocar aspectos da camada de transporte, analisando-se o número de conexões estabelecidas com sucesso e o número de tentativas sem sucesso, a fim de identificar situações de sobrecarga ou ociosidade nos sistemas. Esta abordagem, no entanto, não contempla um relacionamento com as atividades das outras camadas de protocolo; ela é útil para controlar recursos que, por sua natureza, não suportam uma arquitetura completa, isto é, todas as sete camadas do RM-OSI.

A estrutura de **operação de camada** restringe-se à monitoração e ao controle de uma única instância de comunicação. Neste caso, as informações de gerenciamento são concernentes a uma conexão. Por exemplo, na camada de transporte, pode haver várias conexões ativas; a operação de camada trata da gerência de cada uma destas conexões, de forma independente.

4 ARQUITETURA SNMP

Um dos protocolos desenvolvidos que foi padronizado no gerenciamento de redes foi o Protocolo Simples de Gerenciamento de Rede (SNMP). O SNMP foi criado em 1987 como um Simple Gateway Monitoring Protocol. Entretanto, foi logo estendido como protocolo de gerenciamento de rede, versão que foi definida no RFC 1157 de maio de 1990. Posteriormente, por existirem algumas funções relevantes e devido à simplicidade do SNMP, foram definidas novas versões do protocolo SNMP chamadas de SNMPv2 e SNMPv3, e o SNMP original ficou conhecido como SNMPv1.

O RFC 1157 define que a arquitetura SNMP consiste de uma solução para o problema de gerenciamento de redes, em termos da representação da informação de gerenciamento comunicada pelo protocolo, da forma e do significado das trocas entre entidades de gerenciamento, da definição dos relacionamentos administrativos entre entidades de gerenciamento, do escopo da informação de gerenciamento comunicada pelo protocolo e da forma e do significado das referências às informações de gerenciamento.

O RFC 1157 inclui ainda três objetivos a serem conseguidos pelo SNMP: ser independente da arquitetura e do mecanismo dos dispositivos gerenciados; minimizar o número e a complexidade das funções de gerenciamento; e ser flexível o suficiente para permitir expansões futuras.

O SNMP é uma estrutura de dispositivos em uma pilha de protocolos TCP/IP e utiliza o conceito de gerente e agente. O gerente, normalmente, é uma estação que controla um conjunto de agentes, que podem ser roteadores ou servidores. A figura a seguir ilustra o conceito do SMNP.

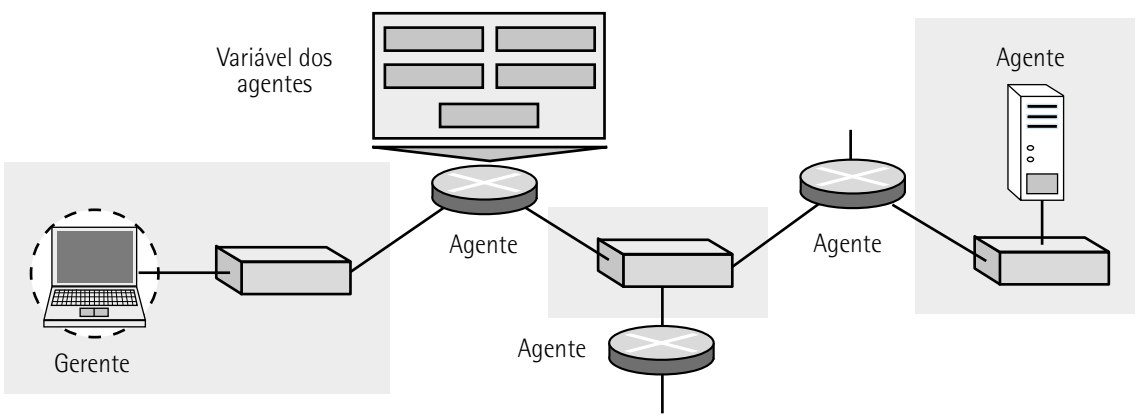

Figura 15 – Conceito do SNMP

O gerenciador central e os equipamentos de rede utilizam o protocolo SNMP para a comunicação das informações de gerenciamento de redes. Nos elementos que se busca gerenciar é instalado um *software* cliente, também conhecido como agente. Esse elemento manda dados ao gerenciador central da rede, o qual guarda esses dados e exibe alertas quando ocorre falha de algum equipamento ou do meio de comunicação utilizado.

O SNMP é um protocolo da camada de aplicação no qual poucas estações gerentes controlam um conjunto de agentes. O intuito de o protocolo ter sido desenvolvido nessa camada é possibilitar o monitoramento dos dispositivos produzidos por fornecedores variados e instalados em diferentes redes físicas. Assim, o protocolo SNMP permite que as atividades de gerenciamento ocorram independentemente das características físicas dos dispositivos ou da tecnologia da rede adotada.

Com o gerenciamento SNMP é possível implementar funções, como um gerente inspecionar um agente por meio de uma solicitação de informações que refletem no comportamento do agente. Outra função possível é um agente contribuir com o processo de gerenciamento por meio de alertas, avisando o gerente de uma situação incomum. Por fim, um gerente pode forçar um agente a executar uma tarefa por meio da reinicialização dos valores na base de dados desse agente. Essas interações podem ser verificadas na figura a seguir.

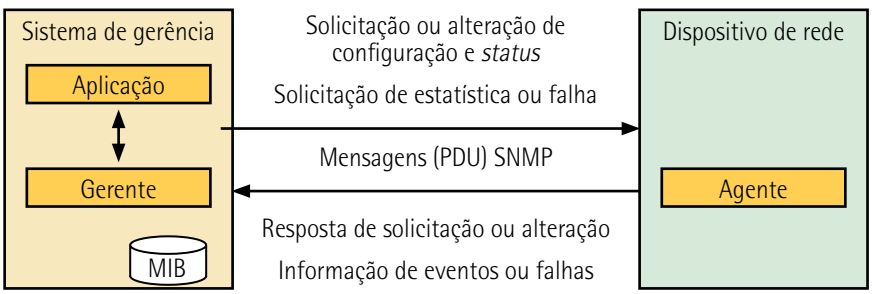

Figura 16 – Arquitetura do protocolo SNMP

Lembrete

O SNMP define o formato dos pacotes trocados entre um gerente e um agente; também lê e altera o estado de objetos nos pacotes.

Tanto os equipamentos de comunicação como o gerenciador central utilizam para a comunicação o protocolo SNMP. Com esse protocolo, é possível que gerentes de redes localizem e corrijam problemas de forma proativa. Os dados de gerenciamento pelos dispositivos são guardados em MIBs. Denomina-se SMI toda a estrutura de informações e a necessária especificação.

A SMI pode ser entendida como uma especificação de que define regras. As regras serão utilizadas para nomear objetos, bem como para atribuir seus tipos, incluindo o comprimento e a faixa de valores possíveis, e para mostrar como codificar objetos e valores.

A MIB cria uma coleção de objetos nomeados, seus tipos e os relacionamentos entre eles em uma entidade a ser gerenciada.

É possível estabelecer uma analogia entre o protocolo SNMP, a base MIB e a estrutura SMI e os elementos necessários para escrever um programa em uma linguagem de computador para resolver um determinado problema.

Antes de começar a escrever o programa, deve-se conhecer a sintaxe da linguagem sobre a qual irá se desenvolver o programa, a qual pode ser, por exemplo, uma linguagem C ou Java. Cada linguagem tem regras quanto a que tipos de variável podem ser utilizados e como as variáveis podem ser nomeadas. No gerenciamento de redes, essas regras são definidas pela SMI.

A declaração e a definição de escopos criam objetos usando tipos predefinidos e alocam memória para eles. No gerenciamento de redes, é a MIB que atua nessa tarefa.

Após a declaração de variáveis, constantes e funções, o programa apresenta as instruções que armazenam valores nas variáveis e modificam esses valores conforme a necessidade. No gerenciamento de rede, o SNMP armazena, modifica e interpreta os valores dos objetos já declarados pela MIB.

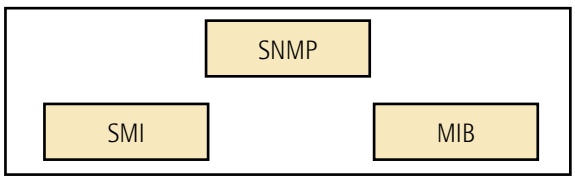

Figura 17 – Componentes do gerenciamento de redes na internet

O SNMP utiliza o protocolo UDP (User Datagram Protocol) para o envio de dados em uma rede TCP/IP na comunicação entre cliente e servidor. Para o cliente da rede, o SNMP executa as operações sobre os objetos de forma transparente, o que permite à interface do *software* de gerenciamento da rede criar comandos imperativos para executar operações sobre os objetos gerenciados. Esta é a grande diferença entre gerenciar uma rede usando o protocolo SNMP e gerenciar a mesma rede usando outros protocolos.

No protocolo SNMP são definidos tanto a sintaxe (a forma e a representação dos nomes e dos valores) como o significado das mensagens trocadas entre os clientes e os servidores. O formato das mensagens e dos objetos gerenciados de uma MIB é especificado com a linguagem ASN.1 e, ao contrário de outros protocolos usados nas redes TCP/IP, suas mensagens não apresentam campos fixos, e, portanto, não se podem representar as mensagens simplesmente com o uso de estruturas fixas. O SNMP também define as relações administrativas entre os vários *gateways* que estão sendo gerenciados, determinando a autenticação necessária para os clientes acessarem os objetos gerenciados.

Ao contrário dos outros protocolos de gerenciamento, que apresentam muitos comandos (operações), o SNMP apresenta um conjunto limitado de comandos, baseado num simples mecanismo de busca/alteração. Portanto, é muito mais fácil de ser implementado do que um protocolo com muitas operações, em que cada operação sobre um objeto necessita de um comando diferente para implementá-la.

O mecanismo de busca/alteração conceitualmente só apresenta duas operações: uma para o cliente alterar atributos de um objeto de uma MIB (SET), e outra para obter os valores dos atributos de um objeto (GET). Somente estão disponíveis estas operações (e suas variações) para

o gerenciamento da rede, as quais serão aplicadas sobre os objetos de uma MIB. A principal vantagem de um mecanismo como este é a simplicidade e a flexibilidade que ele dá ao protocolo, o que permite ao SNMP ser um protocolo bem estável – a sua estrutura básica continuará fixa, mesmo que novos objetos sejam adicionados na MIB ou que novas operações sejam definidas sobre estes objetos (elas serão constituídas pelas operações básicas).

A MIB define o conjunto e a semântica dos objetos que os servidores SNMP devem controlar, ou seja, define o conjunto conceitual de objetos que um servidor SNMP controla. A MIB é usada para armazenar em seus objetos os estados internos das entidades de uma rede. Na maioria dos casos, usamos as variáveis convencionais para o armazenamento dos objetos de uma MIB, mas em alguns casos, em que a estrutura interna do TCP/IP não é exatamente compatível com a estrutura de um objeto de uma MIB, é necessário que o SNMP seja capaz de computar os objetos de uma MIB a partir das estruturas de dados disponíveis (simulação deste conjunto conceitual de objetos).

Ao receber e enviar mensagens no protocolo SNMP, os nomes dos objetos não devem ser armazenados na forma textual, e sim na forma numérica, definida pela sintaxe ASN.1, que representa o objeto univocamente, com o objetivo de tornar o pacote SNMP mais compacto. Quando a forma numérica que representa um objeto termina com um zero (como em 1.3.6.1.2.1.4.3.0), representa que o objeto é a única instância existente. Por exemplo, o objeto gerenciável iso.org.dod.internet.mgmt.mib.ip.ipInReceives será representado na mensagem SNMP como 1.3.6.1.2.1.4.3. A figura a seguir ilustra o identificador de objeto na SMI.

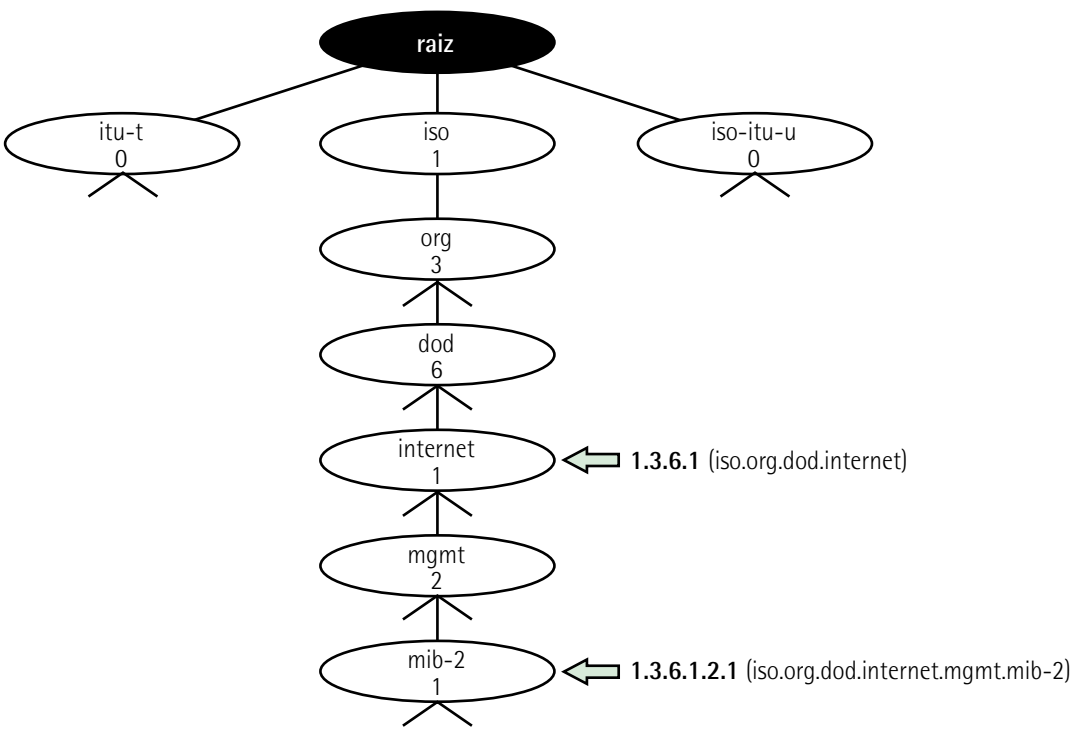

Figura 18 – Identificador de objeto na SMI

Para minimizar o espaço interno necessário para representar um objeto, e considerando que todos os objetos em uma MIB apresentam o mesmo prefixo no seu nome, podemos retirar o prefixo após a mensagem chegar à máquina e recolocá-lo imediatamente antes de enviar a mensagem para outra máquina.

A Base de Informações de Gerenciamento versão 2 (MIB2) é o segundo componente utilizado no gerenciamento de redes. Cada agente tem sua própria MIB2, que é uma coleção de todos os objetos que o gerente pode gerenciar.

A Estrutura de Gerenciamento de Informação versão 2 (SMIv2) é outro componente do gerenciamento de redes. A SMI é uma diretriz usada pelo SNMP. Ela define três atributos para tratar um objeto: nome, tipo de dados, que pode ser simples ou estruturado, e método de codificação.

De forma sintetizada, os principais objetivos do protocolo SNMP são:

- Construir uma arquitetura que seja independente de detalhes relevantes somente a algumas implementações particulares.
- Reduzir o tráfego de mensagens de gerenciamento necessário para gerenciar os recursos da rede.
- Reduzir o número de restrições impostas às ferramentas de gerenciamento da rede, devido ao uso de operações complexas e pouco flexíveis.
- Reduzir o custo da construção de um agente que suporte o protocolo.
- Apresentar operações simples de serem entendidas, sendo facilmente usadas pelos desenvolvedores de ferramentas de gerenciamento.
- Permitir facilmente a introdução de novas características e novos objetos não previstos ao definir o protocolo.

Um gerente interage com um agente de acordo com as regras estabelecidas pelo *framework* de gerenciamento. Em geral, o gerenciamento da rede impõe *overheads* significativos, pois cada nó apenas produz algumas variáveis, que serão lidas e usadas para sua monitoração.

A figura a seguir representa a estrutura de uma rede com diversos agentes, como servidores, impressoras, computadores, roteadores e estações de trabalho com gerenciamento utilizando protocolo SNMP.

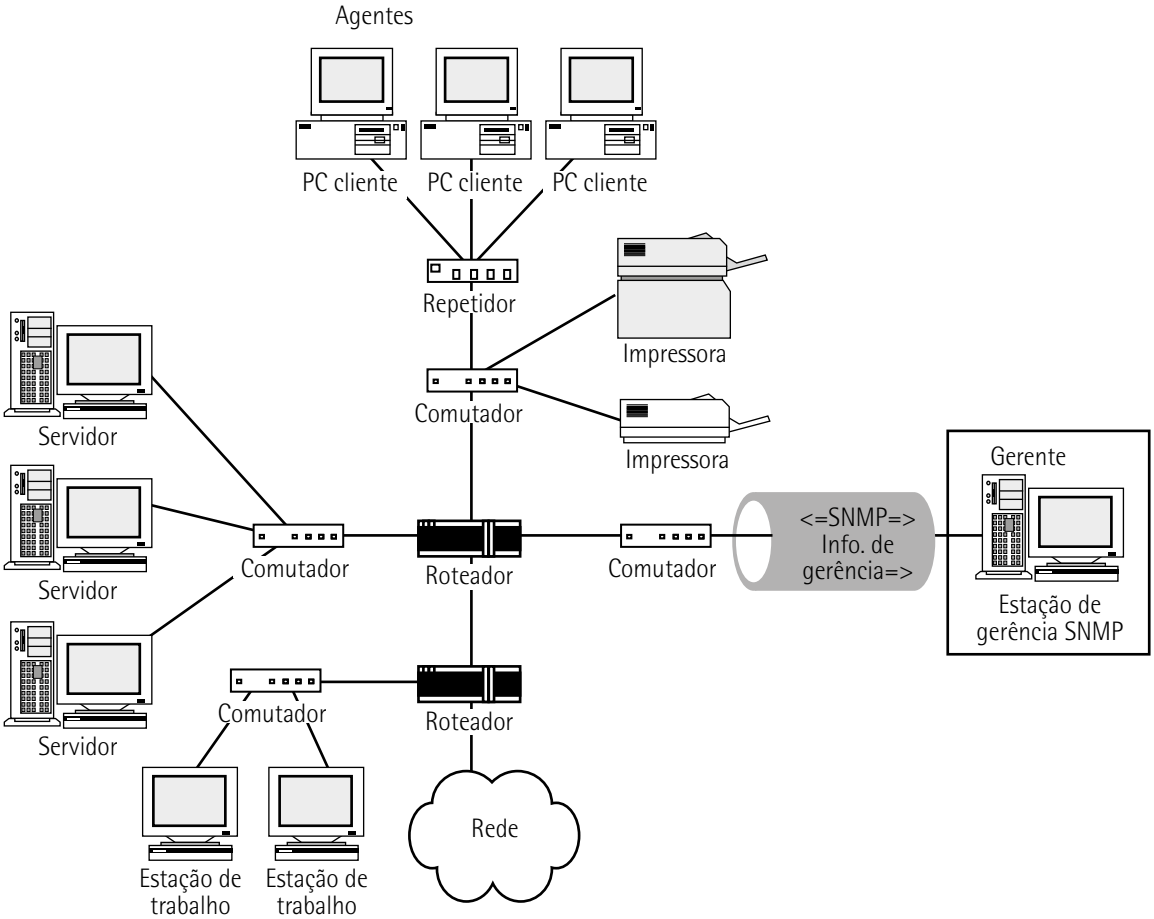

Figura 19 – Elementos de uma arquitetura geral de solução de gerência

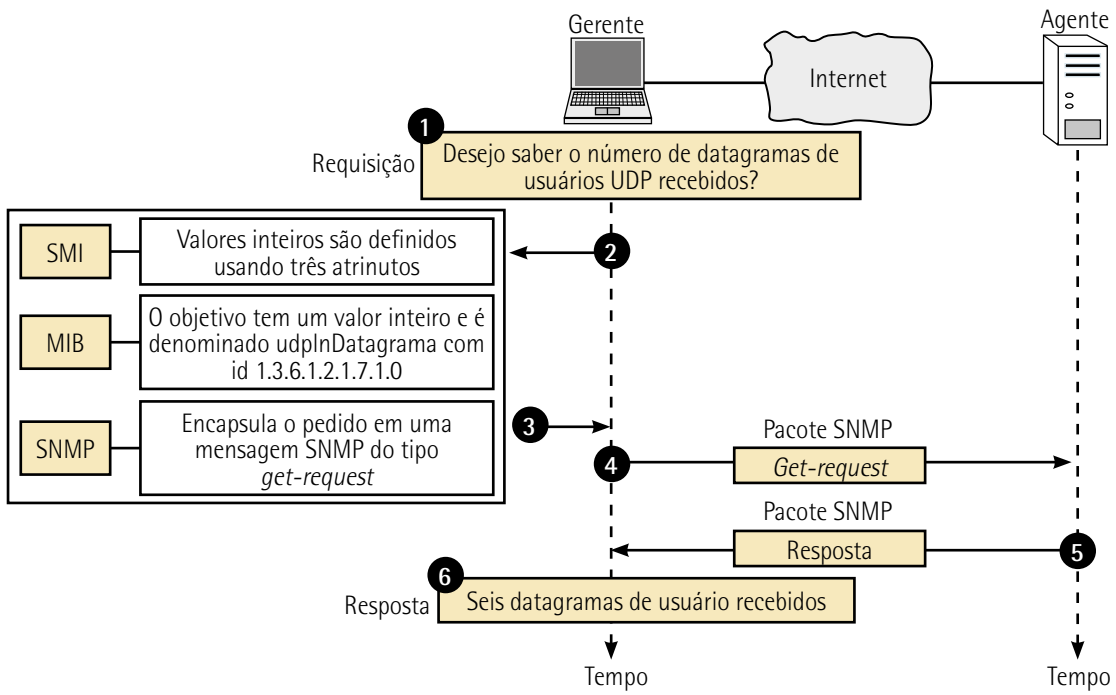

Figura 20 – Visão geral do monitoramento SNMP

4.1 SNMPv1

O SNMP tem como base a técnica *fetch-store*, ou seja, todas as suas operações previstas são derivadas de operações básicas de busca e armazenamento.

Na versão 1 do SNMP, foram definidas cinco operações, que estão descritas no quadro a seguir:

Quadro 2 – Operações suportadas no SNMPv1

Operação	Função
Get-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis informados na solicitação.
Get-next-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis que sucedem lexicograficamente àquelas informadas na solicitação.
Set-request	Solicitação para atribuição de valor a uma ou um conjunto de variáveis.
Get-response	resposta às operações *get-request*, *get-next-request* e *set-request*.
Trap	Envio de um evento não solicitado para uma ou várias estações de gerenciamento. Tipos de *trap* definidos no RFC 1215: *cold start*, *warm start*, *link down*, *link up*, *authentication failure*, *egp neighbor loss* e *enterprise specific*.

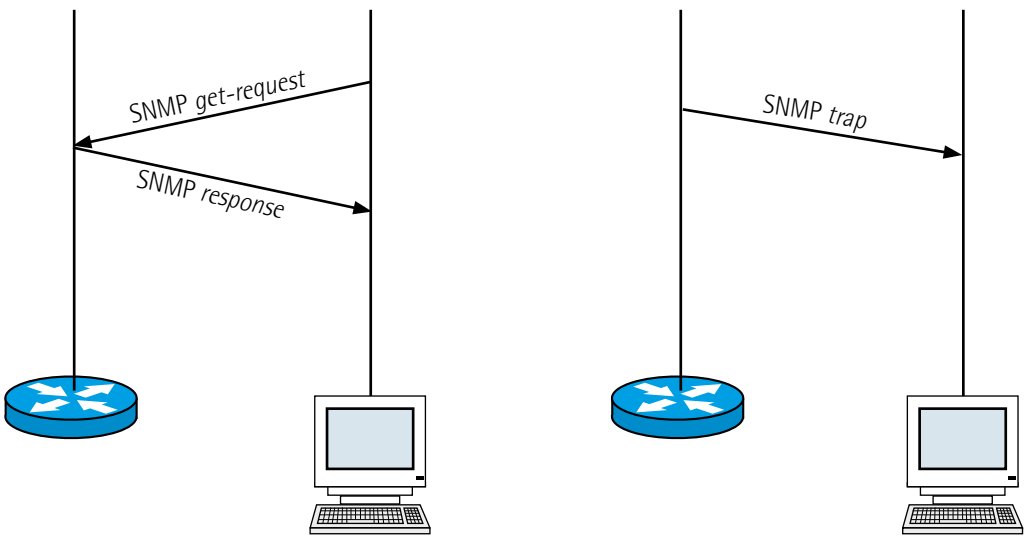

Figura 21 – Exemplos de mensagem SNMP *request/response* e *trap*

O SNMPv1 tem um processo de autenticação fraca, que é baseado em uma cadeia de caracteres chamada *community*, contida no cabeçalho do pacote SNMP e que trafega em modo legível pela rede. São definidas duas *communities*: uma para acesso somente de leitura e outra para acesso de leitura e gravação.

O SNMP não provê mecanismos específicos para que um gerente dê comandos para que um agente execute uma ação. Entretanto, é possível utilizar a operação *set* para contornar esta deficiência. Um objeto pode ser utilizado para representar um comando. Então, uma ação específica é executada se o valor do objeto é alterado para um valor específico. Um exemplo dessa funcionalidade é o objeto *reboot*.

O protocolo SNMPv1 é muito utilizado no gerenciamento de rede, apesar de possuir diversas limitações que podem comprometer o processo, como:

- O padrão SNMPv1, como já comentado, possibilita somente uma autenticação trivial.
- Não suporta a comunicação gerente-gerente.
- Não é apropriado para o gerenciamento de redes com muitos elementos, devido à limitação de *performance* da coleta de dados (*polling*).
- Não permite determinar o tráfego existente nas redes em que os recursos gerenciados estão instalados, pois estas informações se referem ao próprio recurso em que o agente está executando.
- Não é capaz de analisar os dados próprios e enviar notificações quando alguns limiares são alcançados.
- O modelo da MIB é limitado e não são admitidas aplicações em que o gerenciamento seja baseado em valores ou tipos de objeto.
- As *traps* SNMP não são reconhecidas, pois são implementadas sobre protocolos sem reconhecimento ou sem conexão.

Saiba mais

Sobre as especificações do protocolo SNMP, leia o seguinte estudo dedicado a ele:

<http://penta.ufrgs.br/gr952/trab1/snmp_especificacao.html>.

4.2 SNMPv2

O SNMP foi desenvolvido como uma solução temporária para o fornecimento de um mínimo de gerenciamento da rede. A expectativa era de que a solução definitiva viria com o gerenciamento baseado no modelo OSI.

Entretanto, algumas razões não permitiram que esta transição acontecesse da forma planejada, pelo menos inicialmente. Uma das razões é a abordagem orientada a objeto utilizada pelo modelo OSI, muito mais complexa que a MIB escalar implementada no SNMP. Adicionalmente, o desenvolvimento

de padrões OSI de gerenciamento e sua posterior implementação levou muito mais tempo do que o esperado, possibilitando que novas versões do SNMP fossem lançadas.

Desse modo, foi desenvolvida a versão 2 do SNMP (SNMPv2) quando ficou nítido que o gerenciamento OSI não seria adotado tão rapidamente. Tanto esse fato é verdade que os fabricantes de dispositivos de rede já o haviam incorporado quando se tornou óbvio que o padrão de gerenciamento OSI não seria implementado em um futuro próximo. Os maiores fabricantes de dispositivos de rede já haviam adotado módulos SNMP em seus equipamentos e era evidente para todos os elos da cadeia que o SNMP necessitava de muitas melhorias.

O primeiro projeto do SNMPv2 não foi amplamente aceito pelo mercado. Alguns dos motivos para esta falta de aceitação são a complexidade das melhorias de segurança e administração do *framework*. Foram realizadas várias tentativas de simplificar o protocolo de gerenciamento, mas não se chegou a nenhum consenso. Como resultado, ocorreram ações em três frentes distintas. Os documentos que tinham atingido consenso foram publicados em janeiro de 1996 como RFCs 1902-1908. Já as modificações menores no modelo de administração e segurança do SNMPv2 (denominadas *community-based* SNMPv2 [SNMPv2c]) foram publicadas em janeiro de 1996 como RFC 1901. Por fim, o trabalho continuou em outras áreas: segurança, *framework* administrativo, MIB de configuração remota e comunicação gerente-gerente.

Várias mudanças significativas deveriam ser introduzidas no SNMPv2. Uma delas seria a de prover funções de segurança, que inexistiam no SNMPv1.

Infelizmente, mesmo depois de muito esforço de diversas partes do processo, não houve consenso: os atributos de segurança foram retirados da especificação final.

Apesar de o modelo organizacional permanecer praticamente inalterado, e a despeito da falta de melhorias na parte de segurança, várias melhorias foram feitas na arquitetura SNMPv2: novos tipos de dado, novas macros, convenções textuais, operações que facilitam a transferência de grandes quantidades de dados (*bulk*), transferência de blocos de dados (*bulk*), códigos de erro mais detalhados, suporte a multiprotocolos na camada de transporte, inclusão de mensagem de gerente para gerente, definição de uma nova estrutura de informações de gerenciamento (SMIv2, estabelecida nas RFCs 1902 a 1904), comandos de conformidade, melhorias em tabelas e inclusão de dois novos grupos na MIB, *security* e SNMPv2

O SNMPv2 proporciona três categorias de acesso às informações de gerenciamento de redes. A primeira categoria de interação, chamada *request/response*, é quando o gerente SNMP envia uma solicitação a um agente SNMPv2, que responde. A segunda categoria de interação é um *request/response* em que ambas as entidades são gerentes SNMP. A terceira categoria é uma interação não confirmada, em que um agente SNMPv2 envia uma mensagem não solicitada, ou *trap*, para o gerente e nenhuma resposta retorna. Somente a segunda categoria é nova no SNMPv2 – as outras duas já existiam no SNMPv1. A figura a seguir ilustra a arquitetura de gerenciamento utilizada no SNMPv2.

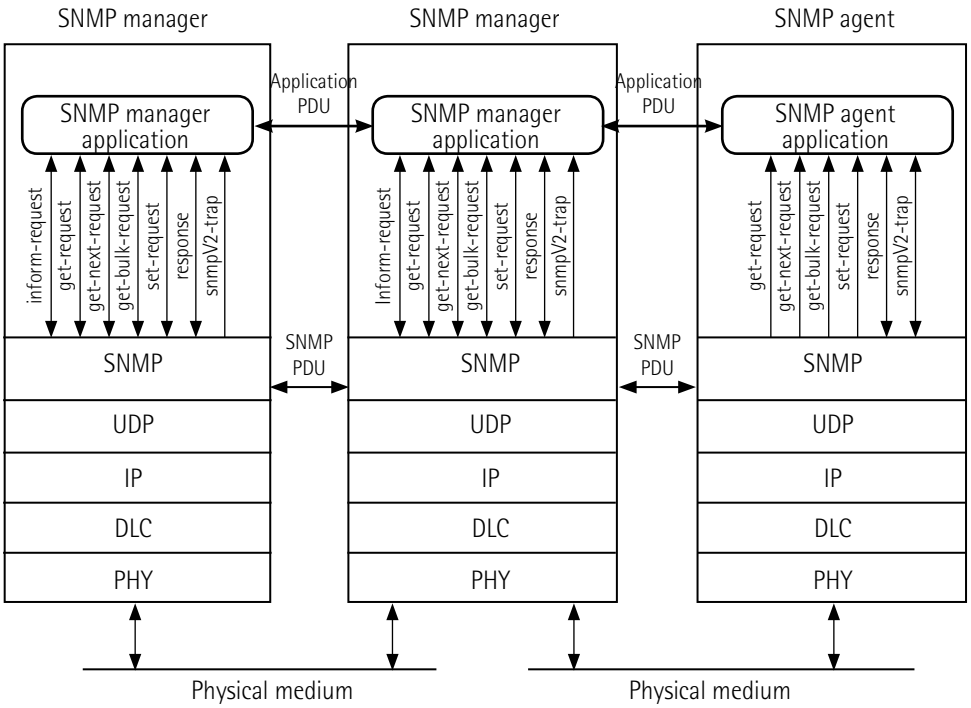

Figura 22 – Arquitetura de gerenciamento de rede SNMPv2

A alteração mais relevante nas operações do SNMPv2 foi a inclusão de duas novas PDUs. A PDU *get-bulk-request* possibilita ao gerente recuperar grandes blocos de dados eficientemente, em particular várias linhas de tabelas, permitindo uma maior eficiência ao gerenciamento. Já a PDU *information-request* é gerada por um gerente para comunicar a outro gerente a informação contida em sua visão da MIB. Uma resposta é gerada pelo gerente que recebeu a mensagem para o gerente que a enviou.

4.3 SNMPv3

Depois de muita controvérsia, o SNMv2 foi liberado como um *framework* SNMP, SNMPv2c, sem nenhuma implementação adicional de segurança em relação ao SNMPv1. Esta deficiência somente foi solucionada no SNMPv3. Os documentos do grupo de trabalho do SNMPv3 não são de fato especificações completas de um protocolo de gerenciamento de redes. Na verdade, estes documentos definem um conjunto de características de segurança e um *framework* que poderia ser utilizado com as capacidades funcionais do SNMPv2 ou SNMPv1.

Uma das características principal do SNMPv3 é a modularidade da documentação e da arquitetura. O projeto da arquitetura integra as especificações SNMPv1 e SNMPv2 com as do SNMPv3. Esta integração permite a continuação de uso do legado do SNMP por agentes e gerentes SNMPv3.

O RFC 2571, documento que estabeleceu a arquitetura do SNMPv3, define os seguintes objetivos que guiaram seu desenvolvimento:

- Utilizar o trabalho existente. Os conceitos de segurança do SNMPv3 se baseiam fortemente no SNMPv2u e no SNMPv2*.

- Resolver o problema de segurança, principalmente para a operação *set-request*, considerada a deficiência mais importante no SNMPv1 e no SNMPv2c.

- Ser modular para possibilitar o desenvolvimento de parte da arquitetura, mesmo que o consenso não tenha sido atingido no todo.

- Definir uma arquitetura que permita longevidade ao *framework* SNMP que já tenha sido definido e que venha a ser definido no futuro.

- Manter o SNMP o mais simples possível.

- Projetar uma arquitetura modular que permita a implementação sobre diversos ambientes operacionais.

- Acomodar modelos de segurança alternativos.

Um dos principais objetivos do SNMPv3 foi a área de segurança. Autenticação, privacidade bem como autorização e controle de acesso também foram incorporados na especificação SNMPv3. O SNMPv3 é projetado para prover segurança contra as seguintes ameaças:

- modificação da informação: uma entidade poderia alterar uma mensagem em trânsito gerada por uma entidade autorizada;

- *masquerade*: uma entidade não autorizada poderia assumir a identidade de uma entidade autorizada;

- modificação de *stream* de mensagem: como o SNMP é projetado para operar sobre um protocolo não orientado à conexão, existe a ameaça de que as mensagens SNMP possam ser reordenadas, atrasadas ou duplicadas;

- descoberta: uma entidade poderia observar trocas de mensagens entre gerentes e agentes e aprender o valor de objetos gerenciados e eventos notificados.

O SNMPv3 não contém mecanismos de segurança contra duas ameaças:

- *denial of service*: uma pessoa poderia impossibilitar trocas de mensagens entre gerente e agente;

- análise de tráfego: uma pessoa poderia observar o padrão de tráfego entre gerentes e agentes.

A arquitetura SNMP, conforme definida no RFC 2571, consiste de uma coleção de entidades SNMP distribuídas e interagindo. Cada entidade implementa uma parte das características do SNMP e pode atuar como um nó agente, um nó gerente ou uma combinação dos dois. Cada entidade SNMP consiste de uma coleção de módulos que interagem entre si para prover serviços. A entidade SNMP tem os seguintes componentes:

- *dispatcher*: permite o suporte concorrente a múltiplas versões de mensagens SNMP no *engine* SNMP;

- *message processing subsystem*: responsável por preparar mensagens para envio e extrair dados de mensagens recebidas;

- *security subsystem*: provê serviços de segurança como autenticação e privacidade de mensagens. Este subsistema pode conter múltiplos modelos de segurança;

- *access control subsystem*: provê um conjunto de serviços que uma aplicação pode usar para checagem de direitos de acesso;

- *command generator*: inicializa as PDUs SNMP (*get, get-next; get-bulk, set-request*) e processa a resposta gerada para uma requisição;

- *command responder*: recebe as PDUs SNMP destinadas para o sistema local; a aplicação *command responder* executará a operação apropriada do protocolo, usando o controle de acesso, e gerará a mensagem de resposta a ser enviada;

- *notification originator*: monitora o sistema por eventos e condições particulares e gera mensagens (*trap/inform*) baseado nos eventos e condições; devem existir mecanismos que determinem para onde enviar as mensagens, qual versão do SNMP utilizar e quais parâmetros de segurança acionar;

- *notification receiver*: ouve as mensagens de notificação e gera mensagens de resposta quando uma mensagem contendo uma PDU *inform* é recebida;

- *proxy forwarder*: repassa mensagens SNMP; sua implementação é opcional.

O modelo de segurança do SNMPv3 é baseado em usuários (User-based Security Model – USM) e reflete o conceito tradicional de nome de usuários e senhas. A base de segurança, no uso de esquemas de autenticação e privacidade, são as chaves secretas. A chave secreta para autenticação é derivada de uma senha escolhida pelo usuário.

O controle de acesso trata de quem pode acessar os componentes de gerenciamento das redes e o que pode ser acessado. Nas versões anteriores do SNMP, este tópico era coberto pela política de acesso baseada em nomes de comunidade. No SNMPv3, o controle de acesso tornou-se muito mais seguro e flexível pela introdução do Modelo de Controle de Acesso Baseado em Visão (View-based Access Control Model – VACM). O VACM define um conjunto de serviços que uma aplicação em um agente pode usar para validar comandos de requisição e notificação.

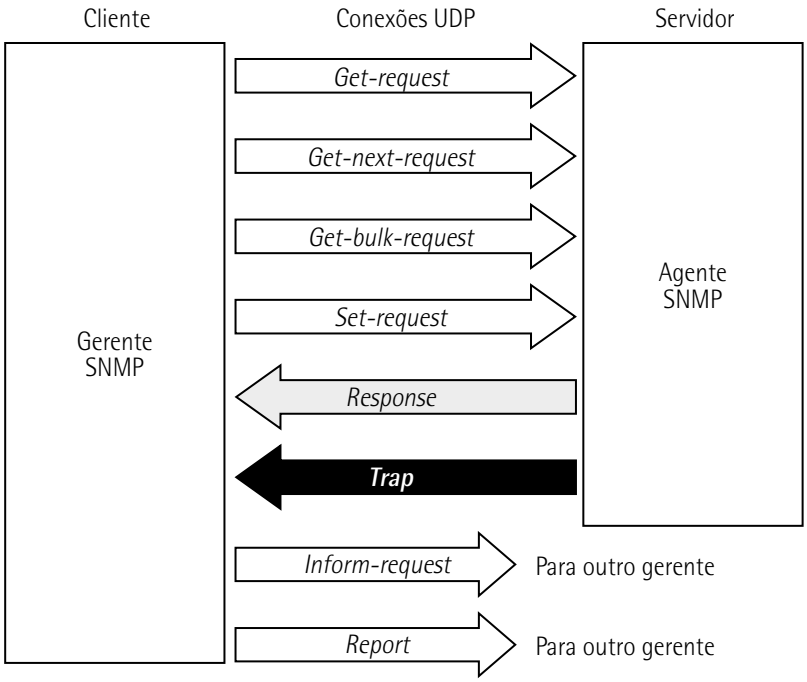

Figura 23 – PDU do SNMPv3

Observação

No protocolo SNMPv1 existia apenas uma forma de autenticação muito trivial. Com isso, a questão da segurança era muito prejudicada. Tal aspecto foi ajustado no SNMPv3, que provê autenticação, privacidade, autorização e controle de acesso.

4.4 Comparação OSI x SNMP

Tanto as arquiteturas CMIP quanto as SNMP adotaram a abordagem orientada a objetos para descrever e especificar as informações presentes e armazenadas na MIB.

O SNMP é o padrão de protocolo de gerenciamento utilizado na internet e em redes que usam a arquitetura TCP/IP. O CMIP só foi aplicado em redes com arquitetura OSI.

O elemento SNMP agente é muito mais simples do que o CMIP. As operações definidas para o SNMPv1 restringem-se às operações simples do tipo *get-and-set*, com melhoras na definição do SNMPv2. Por sua vez, o CMIP especifica um conjunto mais completo de operações, com a possibilidade de sincronizar operações realizadas sobre vários objetos.

Outro fator é que o SNMP é um protocolo não orientado à conexão, enquanto o CMIP é um protocolo orientado à conexão executado sobre toda a pilha de protocolos OSI de gerenciamento.

Uma desvantagem, que veio a ser o grande problema do CMIP, é que ele se tornou um sistema muito grande e complexo. Por conseguinte, poucas redes conseguem suportá-lo.

O quadro a seguir consolida essa comparação entre o protocolo SNMP e o protocolo CMIP.

Quadro 3 – Comparativo protocolo SNMP x CMIP

Característica	Protocolo SNMP	Protocolo CMIP
Complexidade	Simples	Complexo
Tipo de rede em que é aplicado	Redes mais simples	Redes mais complexas
Padrão de gerenciamento de redes	Internet	Base do modelo TMN
Utilização	Amplamente utilizado	Pouco utilizado
Protocolo de transporte	Não orientado à conexão (utiliza o protocolo UDP)	Orientado à conexão
Arquitetura	Modelo agente-gerente	Modelo agente-gerente
Operação	Comando/resposta e *trap*	Comando/resposta e *trap*

Observação

Como o padrão TCP/IP surgiu antes do modelo OSI, já existiam soluções de gerenciamento SNMP quando surgiram as soluções CMIP, que precisam de redes operando no modelo OSI. Como já tinham sido investidos muitos recursos na arquitetura TCP/IP, não houve a troca pelo modelo OSI para a maior parte dos casos. Assim, o protocolo de gerenciamento SNMP é o mais utilizado.

As redes de computadores permitem, por exemplo, através da arquitetura TCP/IP, transportar facilmente os protocolos SNMP e CMIP, que atuam na camada de aplicação do modelo OSI em paralelo com o transporte de outras aplicações.

Além de SNMP, TMN e OSI, também existem outros modelos de gerenciamento de redes. O quadro a seguir compara as características de cada um deles.

Quadro 4 – Comparativo entre os modelos de gerenciamento de redes

Modelo de gerência	Órgão responsável	Tipo de gerenciamento	Utilização
FCAPS	ISO	Falhas, configurações, desempenho, contabilidade, segurança	Estrutura conceitual popular para gerência de redes
TMN	ITU-T	Negócios, serviços, redes e elementos	Estrutura conceitual popular para gerência de redes, voltada para provedores de serviços de telecomunicações
OAM&P	Provedores de serviço	Operação, manutenção, administração, provisionamento	Utilizado em redes de grandes provedores de serviço
TOM	TeleManagement Forum	Redes e sistemas, desenvolvimento de serviços e operações, atendimento ao usuário	Ainda em estágio conceitual
CMIP/CMIS	ISO	Desempenhos, falhas, configurações	Desenvolvimento limitado, baseado em redes do modelo OSI
SNMP	IETF	Desempenho, falhas	Amplamente utilizado em redes de dados, especialmente em redes baseadas no TCP/IP

Saiba mais

Uma outra comparação entre os protocolos CMIP e SNMP pode ser encontrada no *site* indicado a seguir:

<http://penta2.ufrgs.br/gere96/cmipXsnmp/cmip_stra.htm>.

4.5 Monitoração remota – RMON MIB

Como houve um crescimento exponencial das redes com operações distribuídas tanto de forma geográfica quanto de forma lógica, com as estruturas de MIB do SNMP não era possível calcular o tráfego nas redes em que o recurso está instalado, mas somente as informações referentes ao próprio recurso em que o agente está executando.

Para resolver esse problema, foram instalados dispositivos remotos de gerenciamento, os monitores Remote Monitoring (RMON), também chamados de *probes*. O RMON foi proposto como modelo pelo IETF em 1991 (RFC 1271), sendo padronizado em 1995 (RFC 1757), oferecendo uma arquitetura de gerência distribuída e permitindo análise de tráfego, resolução de problemas, demonstração de tendências e gerenciamento proativo de redes. O maior incremento aos padrões SNMP foi a Remote Network Monitoring MIB (MIB RMON).

Outra deficiência dos agentes SNMP tradicionais é que eles não são capazes de analisar as informações coletadas, não sendo possível programar o envio de notificações no momento em que valores-limites

forem alcançados. Tal fato implica a inspeção contínua, ou *polling*, das variáveis de cada elemento de gerenciamento, causando um aumento de tráfego por conta da função de gerenciamento.

No RMON, o processo de captação de dados é dividido em duas partes. Inicialmente, os dados são coletados pelo agente RMON, implementado no dispositivo ou em um segmento próximo. Uma ou mais estações de gerenciamento se comunicam com o agente RMON pelo protocolo SNMP, em lugar de se comunicar diretamente com o dispositivo gerenciado.

Visando diminuir a quantidade de informações necessárias para o gerenciamento, foi implementada a capacidade de gerenciamento remoto do SNMP, o RMON, o qual consiste na presença de um monitor instalado na rede de interesse coletando informações e, eventualmente, enviando notificações sobre a ocorrência de determinados eventos. O monitor tanto pode ser um dispositivo dedicado exclusivamente à captura de dados e à sua análise, como também pode estar implementado em estações de trabalho, em servidores, em roteadores ou em *hubs*.

A grande vantagem do RMON é permitir uma drástica redução da quantidade de informações de gerenciamento transmitidas entre a rede local gerenciada e a estação gerente conectada a uma rede local remota.

Os agentes que implementam o RMON MIB têm diversos objetivos. Um deles é realizar operações *off-line*, pois o monitor coleta e armazena estatísticas que podem ser recuperadas pela estação gerente a qualquer momento, mesmo quando a comunicação com a estação de gerenciamento não estiver disponível. Outro objetivo é que a realização da monitoração proativa permita executar continuamente diagnósticos e armazenamento de dados. Além de manter históricos dos dados observados, é possível detectar e enviar alertas de problemas, caso determinadas condições ocorram na rede.

Um outro objetivo é a valorização dos dados coletados, visto que o monitor RMON realiza diversos tipos de análise sobre os dados coletados – por exemplo, descobrir os dez *hosts* mais ativos na rede.

Por fim, é possível estabelecer múltiplos gerentes, o que facilita o diagnóstico e aumenta a disponibilidade do gerente.

A figura a seguir mostra o cenário de gerenciamento de uma rede utilizando RMON. Ela ilustra o gerenciamento proativo da rede, em que são diagnosticados e registrados eventos que possibilitem detectar o mau funcionamento e em que se realiza a análise e o levantamento de informações estatísticas sobre os dados coletados em uma sub-rede, liberando a estação gerente desta tarefa.

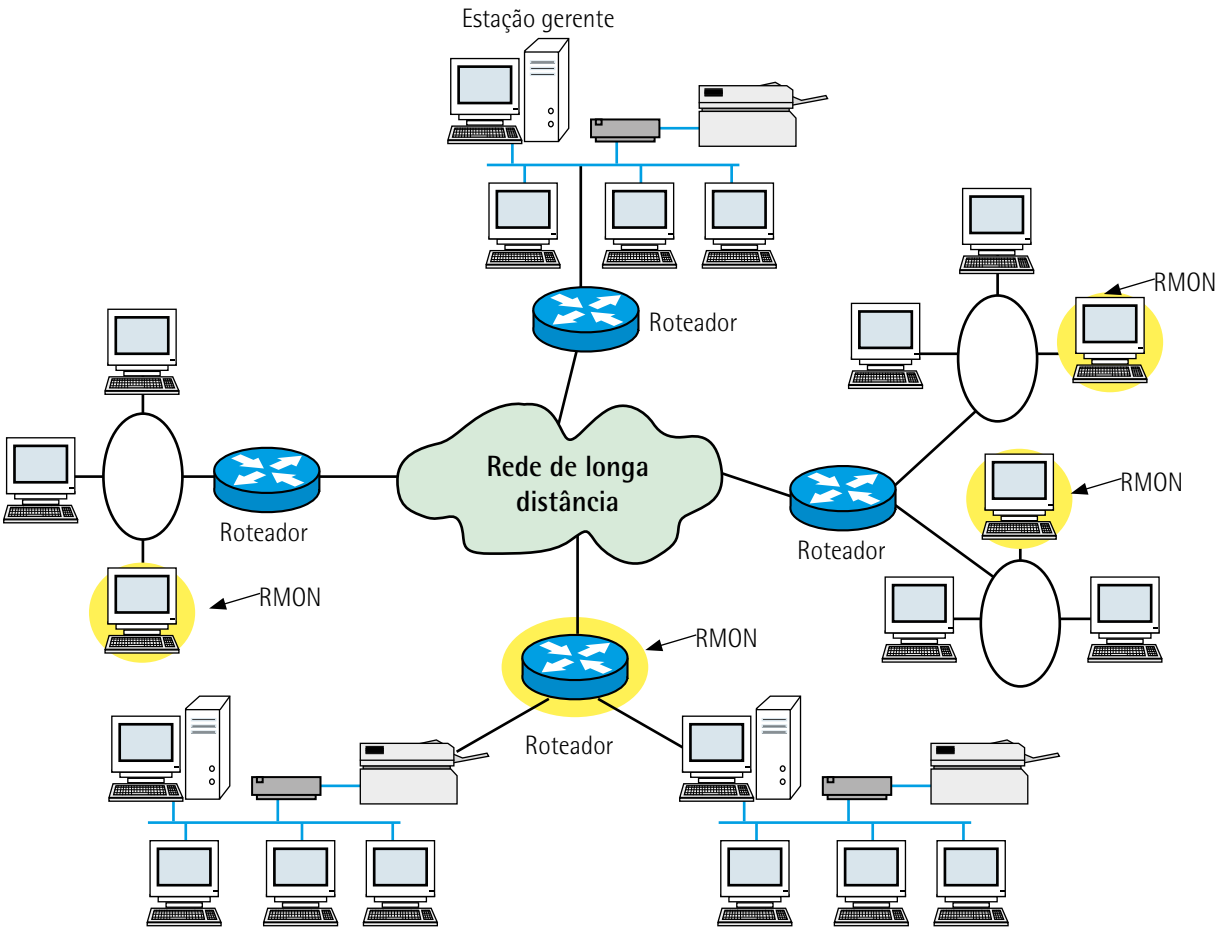

Figura 24 – Utilização de RMON na gerência de rede

Foram implementados dois padrões do protocolo RMON: RMON1 e RMON2.

RMON1

Nessa versão, a monitoração ocorre em nível de camada MAC (Media Access Control), assim como o controle do tráfego e a coleta de informações e estatísticas do segmento de rede local. Também é possível realizar um diagnóstico remoto de erros e falhas contidos no segmento com o auxílio de um analisador de protocolos.

RMON2

A MIB RMON1 se concentrava basicamente em operação e gerenciamento das camadas física e de enlace de uma rede remota. Um monitor RMON pode monitorar o tráfego de rede ao qual está conectado, mas não pode saber a origem desse tráfego, tampouco seu destino final.

Para tentar solucionar esta deficiência, foi criado um grupo de trabalho para desenvolver o padrão RMON2, gerando dois *internet drafts*: Remote Network Monitoring MIB Version 2 e Remote Network Monitoring MIB Protocol Identifiers. O RMON2, definido no RFC 2021, estende as capacidades do RMON às camadas superiores, adicionando dez novos grupos.

Um monitor RMON2 não está limitado somente a monitorar e decodificar o tráfego da camada de rede. Ele também pode ver os protocolos de alto nível rodando acima da camada de rede, determinando, assim, quais protocolos da camada de aplicação estão gerando este tráfego.

Um gerente necessita consultar, periodicamente, os monitores para obter informações. Visando ao aumento de eficiência, podem-se apenas enviar os dados que foram alterados desde a última consulta. Para possibilitar tal facilidade, o RMON2 criou o conceito de filtragem de tempo *(time filtering)*, introduzindo um *time stamp* em cada linha, que armazena a última vez em que esta foi alterada.

O RMON2 opera no nível da camada de rede e camadas superiores, complementando o RMON1, possibilitando coletar informações estatísticas e monitorar a comunicação fim a fim e o tráfego gerado por diferentes tipos de aplicação.

A configuração do gerenciamento RMON2 é composta de uma *probe* que gerencia o tráfego da rede incluindo suas sub-redes. Em cada sub-rede existe uma máquina que gerencia localmente o tráfego desta, funcionando do mesmo modo que a *probe* e independentemente de sua arquitetura.

4.6 WMI: instrumentação e gerenciamento em ambientes distribuídos

Dependendo da complexidade e da quantidade de nós da rede, o custo total de manutenção de uma rede distribuída de computadores pode ser muito elevado e o custo dos treinamentos necessários para a manutenção também pode ser. Por causa disso, várias empresas tomaram iniciativas de redução desses custos nas companhias. Uma dessas iniciativas é o Web-Based Enterprise Management (WBEM), o qual estabelece padrões de gerenciamento de infraestrutura e fornece uma forma de agregar informações de vários sistemas de gerenciamento de *hardware* e *software*.

O início dos trabalhos do WBEM ocorreu em 1996, por meio de um grupo de empresas: Microsoft, Compaq Computer, BMC Software, Cisco Systems e Intel. O objetivo inicial era definir um ambiente aberto de gerenciamento, em que todos os sistemas de gerenciamento e aplicações poderiam acessar, controlar e compartilhar informações de gerenciamento entre si.

De 1996 a 1998, a Microsoft trabalhou para desenvolver uma implementação do WBEM para a plataforma Windows, a qual originou a Windows Management Instrumentation (WMI). A WMI é a principal ferramenta para monitoração e gerenciamento de aplicações construídas sobre o sistema operacional Windows, da Microsoft.

A WMI é baseada em conceitos como monitoração e instrumentação. Em relação à monitoração, verifica o estado de todos os componentes do sistema que são gerenciáveis, sejam eles de *hardware* ou *software*. Já a instrumentação se refere aos métodos de medida e controle e aos instrumentos que facilitam esse trabalho. No caso da WMI, instrumentação se refere aos métodos e medidas disponíveis para o gerenciamento de *hardware* e *software*.

A WMI utiliza o Common Information Model (CIM), base do WBEM, que define um modelo independente de linguagem, usado para representar os recursos gerenciados através de programação

orientada a objetos. Assim, os recursos do sistema são representados como objetos gerenciáveis com propriedades que caracterizam seus dados e métodos que descrevem seu comportamento

Baseada no Modelo de Informação Comum, a iniciativa WBEM é uma tecnologia da DMTF que estabelece padrões de infraestrutura de gerenciamento e oferece uma maneira padronizada de acesso a informações de diversos sistemas de gerenciamento de *hardware* e *software* em um ambiente empresarial. Usando padrões da iniciativa WBEM, os desenvolvedores podem criar ferramentas e tecnologias que reduzam a complexidade e os custos do gerenciamento empresarial, pois, com essa padronização, existe uma redução de custo considerável.

Fornecendo tais padrões, a iniciativa WBEM contribui com os esforços de toda a indústria de reduzir o Custo Total de Propriedade (Total Cost of Ownership – TCO). O TCO refere-se aos custos administrativos associados à compra, implementação e configuração de *hardware* e *software*, atualizações de *hardware* e *software*, treinamento, manutenção e suporte técnico.

A iniciativa WBEM ainda proporciona um ponto de integração pelo qual os dados das fontes de gerenciamento podem ser acessados, bem como complementa e estende os protocolos e a instrumentação de gerenciamento existentes, como os protocolos SNMP e CMIP e a Interface de Gerenciamento da Área de Trabalho (Desktop Management Interface – DMI).

4.6.1 Tecnologia de Instrumentação de Gerenciamento do Windows (WMI)

A tecnologia de Instrumentação de Gerenciamento do Windows (WMI) é uma infraestrutura de gerenciamento que proporciona suporte a uma interface de programação comum, à sintaxe CIM e à sintaxe MOF (Managed Object Format). Esta última define a estrutura e o conteúdo do esquema CIM em uma forma que pode ser entendida tanto pelo homem quanto pela máquina. A Instrumentação de Gerenciamento do Windows disponibiliza uma série eficiente de serviços, que inclui a recuperação de informações com base em consulta e aviso de evento. Esses serviços e as informações de gerenciamento estão acessíveis por meio de uma interface de programação COM (Modelo de Objeto Componente). A interface de *script* WMI também oferece suporte a *scripts*.

Ainda é possível observar as seguintes características da tecnologia WMI:

- Um modelo sólido de operação, configuração e *status* do sistema operacional Windows.
- Interoperabilidade com outros serviços de gerenciamento do Windows. Essa funcionalidade simplifica o processo de criação de soluções de gerenciamento integradas e bem desenhadas.
- Acesso para monitorar, comandar e controlar qualquer objeto gerenciado por meio de um conjunto comum e unificado de interfaces, independentemente do mecanismo de instrumentação suportado.
- Uma API (Interface de Programação de Aplicativo) COM que oferece um único ponto de acesso a todas as informações de gerenciamento.

- Uma arquitetura flexível e extensível. Os desenvolvedores podem estender o modelo de informação para abranger novos dispositivos e aplicativos, escrevendo módulos de códigos denominados provedores de WMI.
- Extensões para o WDM (Windows Driver Model) para capturar dados de instrumentação e eventos de *drivers* de dispositivo e componentes do *kernel*.
- Uma arquitetura de evento potente. Isso possibilita que as alterações nas informações de gerenciamento sejam identificadas, agregadas, comparadas e associadas a outras informações de gerenciamento. Essas alterações também podem ser encaminhadas a aplicativos de gerenciamento local ou remoto.
- Uma linguagem de consulta eficiente que possibilita consultas detalhadas do modelo de informação.
- Uma API programável, que os desenvolvedores podem usar para criar aplicativos de gerenciamento. A API de *script* oferece suporte a diversas linguagens, incluindo Microsoft Visual Basic; Visual Basic for Applications (VBA); Visual Basic, Scripting Edition (VBScript); *software* de desenvolvimento Microsoft JScript. Além de VBScript e JScript, os desenvolvedores podem usar qualquer implementação de linguagem de *script* que ofereça suporte às tecnologias de *script* do ActiveX da Microsoft com essa API (por exemplo, um mecanismo de *script* Perl).

4.6.2 Visão geral da arquitetura de WMI

A arquitetura da tecnologia WMI, ilustrada na figura a seguir, é composta de objetos gerenciados, provedores, infraestrutura WMI e consumidores, que são aplicações acima das APIs.

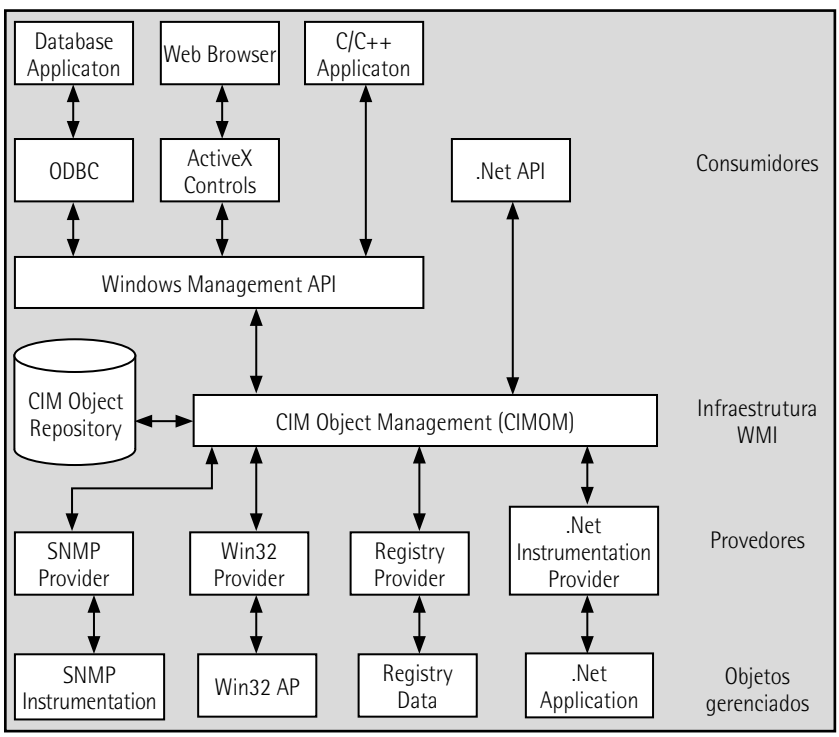

Figura 25 – Estrutura da arquitetura WMI

Uma infraestrutura de gerenciamento inclui o Gerenciador de Objetos CIM, que oferece aos aplicativos acesso padronizado aos dados de gerenciamento e uma área de armazenamento central dos dados de gerenciamento denominada repositório Gerenciador de Objetos CIM.

Os Provedores WMI funcionam como intermediários entre o Gerenciador de Objetos CIM e os objetos gerenciados. Usando as APIs WMI, os provedores fornecem ao Gerenciador de Objetos CIM dados dos objetos gerenciados, gerenciam solicitações em nome dos aplicativos de gerenciamento e geram notificações de eventos.

A infraestrutura de gerenciamento consiste no Gerenciador de Objetos CIM e no repositório Gerenciador de Objetos CIM. Os aplicativos dependem do Gerenciador de Objetos para lidar com a interface entre os aplicativos de gerenciamento e os provedores de dados. A WMI facilita essas comunicações fornecendo uma interface de programação comum com os serviços de gerenciamento do Windows usando COM. Essa API COM oferece serviços de notificação de evento e processamento de consultas e pode ser usada em diversos ambientes de linguagem de programação como C e C++.

O repositório Gerenciador de Objetos CIM armazena o CIM e os esquemas de extensão e as informações de dados ou detalhes da fonte de dados. O Gerenciador de Objetos CIM usa os dados do esquema desse repositório ao atender às solicitações dos aplicativos de gerenciamento para os objetos gerenciados.

Já os objetos gerenciados são componentes empresariais físicos ou lógicos que são modelados usando CIM. Por exemplo, um objeto gerenciado pode ser um item de *hardware*, como um cabo, ou um item de *software*, como um aplicativo de banco de dados. Os aplicativos de gerenciamento podem acessar os objetos gerenciados por meio do Gerenciador de Objetos CIM.

Aplicativos de gerenciamento são aplicativos ou serviços do Windows que usam ou processam informações provenientes de objetos gerenciados. Os aplicativos de gerenciamento podem acessar informações dos objetos gerenciados fazendo uma solicitação ao Gerenciador de Objetos CIM por meio de um dos métodos na API WMI.

Por fim, os provedores WMI são servidores COM e DCOM padrão que funcionam como mediadores entre os objetos gerenciados e o Gerenciador de Objetos CIM. Se o Gerenciador de Objetos CIM receber uma solicitação de um aplicativo de gerenciamento referente a dados que não estejam mais disponíveis no repositório Gerenciador de Objetos CIM ou notificações de evento que não sejam suportadas pelo Gerenciador de Objetos CIM, ele encaminhará a solicitação a um provedor WMI. Os provedores fornecem dados e notificações de eventos para os objetos gerenciados que são específicos aos seus domínios.

A tecnologia WMI possui provedores internos, ou seja, provedores padrão, os quais possuem a função de fornecimento de dados de fontes como o registro do sistema. Esses provedores internos incluem:

- Provedor do Active Directory: funciona como um *gateway* para todas as informações armazenadas no serviço do Active Directory. Permite que informações tanto da WMI quanto do Active Directory sejam acessadas usando uma única API.

- Provedor do Windows Installer: possibilita o controle total do Windows Installer e a instalação do *software* por meio da WMI. Também fornece informações sobre qualquer aplicativo instalado com o Windows Installer.

- Provedor do contador de desempenho: expõe as informações brutas do contador de desempenho usadas para computar os valores de desempenho mostrados na ferramenta Monitor do Sistema. Todos os contadores de desempenho instalados em um sistema poderão ser automaticamente visualizados por meio desse provedor.

- Provedor do registro: possibilita criação, leitura e gravação de chaves do registro. É possível gerar eventos WMI quando chaves do registro especificadas forem modificadas

- Provedor do SNMP: funciona como um *gateway* para os sistemas e dispositivos que usam o SNMP para gerenciamento. As variáveis do objeto MIB SNMP podem ser lidas e gravadas. É possível mapear automaticamente as interceptações SNMP aos eventos WMI.

- Provedor de *log* de eventos: oferece acesso a dados e notificações de eventos do *log* de eventos do Windows Server 2008.

- Provedor Win32: oferece informações sobre sistema operacional, sistema do computador, dispositivos periféricos, sistemas de arquivos e informações de segurança.

- Provedor WDM: oferece informações de nível inferior do WDM (Windows Driver Model) para dispositivos de entrada do usuário, dispositivos de armazenamento, interfaces de rede e portas de comunicação.

- Provedor de visualização: possibilita que novas classes agregadas sejam criadas a partir de classes existentes. As classes de origem podem ser filtradas para exibir apenas as informações pretendidas, as informações de várias classes podem ser combinadas em uma única classe e os dados de várias máquinas podem ser agregados em uma única visualização.

A tecnologia WMI também oferece suporte a provedores personalizados de terceiros. É possível usar provedores personalizados para atender às solicitações de serviço relacionadas a objetos gerenciados específicos de um ambiente. Os provedores costumam usar a linguagem MOF para definir e criar classes. Os provedores usam a API WMI para acessar o repositório Gerenciador de Objetos CIM e para atender a solicitações do Gerenciador de Objetos CIM feitas inicialmente por aplicativos.

Resumo

Nesta unidade vimos que a ISO desenvolveu padrões de gerenciamento e dividiu as atividades em cinco área funcionais específicas, ou Specific Management Functional Area (SMFA), assim como as redes TMN já tinham feito. Nesse sentido, desenvolveu-se um

modelo OSI de gerenciamento denominado FCAPS (Fault, Configuration, Account, Performance e Security).

Vimos também que o ambiente de gerenciamento OSI é composto de elementos gerenciados, agentes e gerentes. O CMISE (Common Management Information Service Element) consiste de uma definição de serviço (CMIS) e de uma especificação de protocolo (CMIP).

Os serviços definidos pelo CMIP são: M-Get, M-Set, M-Create, M-Delete, M-Action, M-Event-Report e M-Cancel-Get. Alguns desses serviços podem ser executados no modo não confirmado e outros somente no modo confirmado.

As notificações representam informações sobre eventos ocorridos no sistema gerenciado e são enviadas ao destinatário através da utilização do serviço M-Event-Report, definido no CMIS.

As informações de gerenciamento são organizadas em bases de dados. O conjunto das bases de dados de informações de gerenciamento é denominado MIB (Management Information Base). A implementação das MIBs não está sujeita à padronização, visto que as informações são definidas segundo uma estrutura de informação de gerenciamento SMI (Structure Management Information).

Analisamos que o SNMP foi desenvolvido como uma solução simples de gerenciamento temporária para fornecimento de um mínimo de gerenciamento da rede, pois existia a expectativa de que a solução definitiva viria com o gerenciamento baseado no modelo OSI. Os objetivos do SNMP são: redução do tráfego de mensagens de gerenciamento necessárias para gerenciar os recursos da rede, redução das restrições inseridas para ferramentas de gerenciamento, permitindo maior flexibilidade, e utilização de operações mais simples para entendimento dos desenvolvedores.

O SNMP é uma estrutura para gerenciar dispositivos em uma rede usando a pilha de protocolos TCP/IP. Um gerente, normalmente uma estação, controla e monitora um conjunto de agentes, geralmente roteadores. O SNMP utiliza os serviços da SMI e da MIB. A SMI nomeia objetos, define os tipos de dado que podem ser armazenados em um objeto e codifica os dados. A MIB é uma coleção de grupos de objetos que podem ser gerenciados pelo SNMP. A MIB usa ordenação lexicográfica para gerenciar suas variáveis.

Estudamos igualmente que a Notação Sintática Abstrata Um (Abstract Syntax Notation Number One – ASN.1) é uma linguagem que define a sintaxe e a semântica de dados. Ela usa alguns símbolos, palavras-chave e tipos de dado simples e estruturados. Parte da ASN.1 é usada pela SMI para definir o formato de objetos e os valores utilizados no gerenciamento da rede.

Na versão 1, SNMPv1, existiam cinco PDUs diferentes, e quatro delas eram do tipo *request/response* e uma do tipo notificação (*trap*). Essa versão possuía uma série de limitações – por exemplo, somente eram permitidas as comunicações entre gerente e agente e entre agente e gerente; não eram possíveis as comunicações entre gerentes. Também não era apropriada para o gerenciamento de redes com muitos elementos, devido à limitação de *performance* da coleta de dados (*polling*), além de não ter implementado nenhum elemento de segurança.

Já na versão 2 do protocolo SNMP (SNMPv2), a principal diferença é a existência de um mecanismo de comunidade melhorado, que apresenta uma identificação não ambígua tanto da origem como do formato da mensagem SNMPv2, permitindo utilizar métodos de acesso mais convencionais aos objetos gerenciados, além de possibilitar o uso futuro de protocolos assimétricos de segurança, com a utilização de chaves públicas.

A versão 2 do SNMP melhorou alguns aspectos, como novos tipos de dado, novas macros, convenções textuais, operações que facilitam a transferência de grandes quantidades de dados (*bulk*), transferência de blocos de dados (*bulk*), códigos de erro mais detalhados, suporte a multiprotocolos na camada de transporte, inclusão de mensagem de gerente para gerente, definição de uma nova estrutura de informações de gerenciamento, comandos de conformidade, melhorias em tabelas e inclusão de dois novos grupos na MIB, *security* e SNMPv2. Entretanto, não agregou nenhuma solução na parte de segurança.

Somente no SNMPv3 é que as soluções na área de segurança foram incorporadas. Autenticação, privacidade bem como autorização e controle de acesso foram incorporados na especificação SNMPv3.

Também no SNMPv3 surgiram PDUs para comunicação entre gerente e gerente, o que inexistia nas versões anteriores.

Comparando-se os protocolos CMIP e SNMP, verifica-se que o protocolo SNMP é mais simples e mais amplamente utilizado em redes

baseadas no padrão TCP/IP e na internet. Somente redes mais complexas usam o CMIP, que, por sua vez, aplica como protocolo de camada de transporte o TCP, sendo, portanto, orientado à conexão, e tem sua utilização bastante mais restrita.

O monitoramento remoto RMON pode ser entendido como um padrão de monitoramento que permite que vários monitores de rede, ou *probes*, e sistemas de gerenciamento troquem informações de monitoramento na rede.

Finalmente, vimos que a tecnologia de Instrumentação de Gerenciamento do Windows (WMI) é uma forma encontrada de padronizar o monitoramento e a instrumentação de dispositivos de forma distribuída para diminuir os custos de manutenção e de treinamento para essa manutenção. Consiste em monitoração dos estados dos dispositivos e medição das informações desses estados.

Exercícios

Questão 1. (TRE-RS 2015) Assinale a opção correta a respeito do protocolo de gerenciamento SNMP.

A) O SNMPv2 opera como protocolo de aplicação orientado a conexão TCP, mantendo os padrões de autenticação, senhas e criptografia forte do SNMPv1.

B) O SNMPv1 disponibiliza recursos avançados de autenticação e criptografia forte, o que permite alta efetividade e segurança no gerenciamento, mesmo em redes IP complexas como a internet.

C) O SNMPv1 opera no modo requisição e resposta, ou seja, para cada mensagem de requisição enviada pelo gerenciador, é esperada uma resposta antes do envio de outra requisição ao agente. Por questões relacionadas a desempenho, o SNMPv1 foi concebido como não orientado a conexão, usando protocolo de transporte UDP.

D) O SNMPv1 é um protocolo relativamente simples: possui apenas quatro tipos de mensagens definidas previamente, duas para solicitar valores de objetos aos agentes e duas para retornar valores de objetos para os gerenciadores.

E) Embora contenha novos tipos de mensagens, o SNMPv2 é compatível com o SNMPv1. Assim, um gerenciador SNMPv2 pode enviar requisições e tratar nativamente as respostas de agentes em dispositivos capazes de executar somente o SNMPv1

Resposta correta: alternativa C.

Análise das alternativas

A) Alternativa incorreta.

Justtificativa: o SNMP utiliza o protocolo UDP da camada de transporte. Além disso, o SNMPv1 utiliza autenticação em texto aberto, não implementando recursos de criptografia.

B) Alternativa incorreta.

Justificativa: reforçando o comentário da questão anterior.

C) Alternativa correta.

Justificativa: essa alternativa corresponde exatamente ao protocolo de gerenciamento SNMP.

D) Alternativa incorreta.

Justificativa: o SNMPv1 previa 5 tipos de mensagens:

GET REQUEST – do gerente para o agente.

GETNEXT REQUEST – do gerente para o agente.

GET RESPONSE – do agente para o gerente.

SET RESPONSE – do gerente para o agente.

TRAP – do agente para o gerente.

E) Alternativa incorreta.

Justificativa: não há compatibilidade entre as duas versões justamente pelos novos tipos de mensagens e formatos. Portanto, não podemos afirmar que há compatibilidade nativa. Nesse sentido, surgiu o SNMPv2c, que permitiu o ajuste de campos nas mensagens para conceder a compatibilidade.

Questão 2. (DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO 2015) O administrador de redes de computadores deseja implantar o serviço de VoIP utilizando os seguintes protocolos:

1. UDP

2. SIP

3. IPv4

Considerando a arquitetura TCP/IP, o relacionamento entre os protocolos e as respectivas camadas da arquitetura é:

Parte superior do formulário

A) 1 – Transporte

2 – Redes

3 – Redes

B) 1 – Redes

2 – Transporte

3 – Redes

C) 1 – Redes

2 – Aplicação

3 – Enlace

D) 1 – Transporte

2 – Aplicação

3 – Redes

E) 1 – Transporte

2 – Enlace

3 – Redes

Resolução desta questão na plataforma.