

Introdução

O gerenciamento de redes pode ser entendido como o processo de controlar uma rede de computadores de tal modo que seja possível maximizar sua eficiência e produtividade. Possui algumas metas como redução dos custos operacionais da rede, redução do congestionamento da rede, aumento da flexibilidade de operação e integração, maior eficiência com maior facilidade de uso.

A gerência de redes, não pode ser vista como uma atividade única, além da operação da rede, abrange outras tarefas como controle de acesso à rede, disponibilidade e desempenho, documentação de configuração, gerência de problemas, auxílio ao usuário entre outras. Algumas atividades podem ter mais relevância do que outras dependendo da complexidade da rede.

Recursos gerenciais são elementos de hardware e software que envolvem o gerenciamento de redes, alguns deles são:

- Componentes dos computadores, tais como dispositivos de armazenamentos, impressoras, etc.
- Componentes de interconexão e conectividade, tais como roteadores, hubs, switches, etc.
- Sistemas operacionais, tais como Windows NT, Netware, etc.
- Softwares de aplicação e ferramentas de desenvolvimento.

Modelos de Gerenciamento

Os modelos de gerenciamento diferenciam-se nos aspectos que se refere à disposição dos gerentes na rede. Existem dois modelos para gerência de redes:

Modelo Internet que adota uma abordagem gerente/agente onde os agentes mantêm informações sobre recursos e os gerentes requisitam essas informações aos agentes. O padrão Internet SMI (Structure of Management Information) especifica uma metodologia para definição da informação de gerenciamento contida na MIB. O SMI usa um subconjunto de tipos de dados ASN.1. A MIB define os elementos de gerenciamento de informação como variáveis e tabelas de variáveis.

Modelo OSI permite a representação das funções de monitoração aos agentes. Contudo, as funções de controle ainda ficam relegadas ao gerente. O gerenciamento no modelo OSI da ISO baseia-se na teoria da orientação a objetos. Com isso, o sistema representa os recursos gerenciados através de entidades lógicas, as quais recebem a denominação de objetos gerenciados.

Existem cinco áreas funcionais no gerenciamento num ambiente OSI:

- Gerência de configuração (**estado da rede**)
- Gerência de desempenho (**vazão e taxa de erros**)
- Gerência de falhas (**comportamento anormal**)
- Gerência de contabilidade (**consumo de recursos**)

- Gerência de segurança (**acesso**)

O gerenciamento OSI gera agentes mais complexos de serem desenvolvidos, consumindo mais recursos dos elementos de rede, enquanto economiza o uso da rede devido a minimização dos pedidos de informações necessários para obter dados sobre objetos gerenciados, livrando o gerente para tarefas mais inteligentes.

Protocolos e Padrões de Gerenciamento

Os protocolos de gerenciamento de rede têm sido tradicionalmente implementados como protocolos do nível de aplicação. E até recentemente, cada vendedor costumava ter um método proprietário pelo qual seus agentes podiam se comunicar, o que levava a existência de incompatibilidades entre os diversos "padrões".

Importantes Padrões e Protocolos

SNMP

A SNMP (Simple Network Management Protocol, em tradução livre: Protocolo Simples de Gerenciamento de Rede), foi projetado na década de 80, e veio na premissa de resolução de problemas na comunicação entre diversos tipos de rede, a ideia é oferecer uma maneira fácil e barata na implementação de uma rede, sua meta é que seja uma solução provisória até que surja um projeto de protocolo para gerenciamento com maior capacidade, entretanto na época nenhuma apareceu. É um protocolo do nível de aplicação da arquitetura TCP/IP, operando sobre o UDP, é considerado simples, pois, os agentes do processo requerem uma quantidade mínima de software. Muito poder de processamento de dados reside no sistema de gerenciamento, enquanto um subconjunto complementar dessas funções reside no sistema gerenciado.

Como consequência da exigência de simplicidade adotada no seu desenvolvimento, o SNMP acabou deixando de tratar algumas características, o que fez com que ele tivesse algumas deficiências. Dentre essas características, destacam-se:

- Suporte para a transferência eficiente de grandes blocos de dados
- Estratégias de gerenciamento de rede centralizado
- Segurança

SNMPv2, nasceu para preencher lacunas deixadas por sua primeira versão como a segurança, e aumentar sua aplicabilidade, podendo ser usado em redes baseadas no modelo OSI, porém, apenas os primeiros defeitos levantados foram solucionados, aí então que surgiu a SNMPv3, que se focou em segurança e se tornou muito mais segura pois abordaram a Autenticação que verifica o usuário e o conteúdo, a Criptografia para evitar invasão e Controle de Acesso para configuração de níveis de acesso na rede.

RMON

O SMNP não é adequado para ambientes de redes grandes, com várias redes locais conectadas a distância, ela é muito simples para essa aplicação, os enlaces longos operam a taxas de transmissão inferiores as locais que a interconectam, pois passam a

ter parte da banda de transmissão ocupada por informações de gerenciamento, a solução para isso é o RMON (Remote Monitoring, em tradução livre: Monitoramento Remoto).

O Objetivo da RMON é definir padrões de monitoramento e interfaces para a comunicação entre agentes e gerentes SNMP, o RMON dá ao gerente da rede a habilidade de monitorar sub redes como um todo e não somente individualmente.

O RMON oferece suporte à implementação de gerenciamento distribuído e cada elemento do mesmo tem sua tarefa como coletar, analisar, tratar e filtrar as informações de gerenciamento de rede e apenas notificar à gerente os eventos significativos e situações de erro.

Objetivos do protocolo RMON são:

- Reduzir a quantidade de informações trocadas entre a rede local gerenciada e a estação gerente conectada a uma rede local remota.
- Possibilitar o gerenciamento contínuo de segmentos de redes locais, mesmo quando a comunicação entre o elemento RMON e a estação gerente estiver, temporariamente, interrompida.
- Permitir o gerenciamento pró-ativo da rede, diagnosticando e registrando eventos que possibilitem detectar o mau funcionamento e prever falhas que interrompam sua operação.
- Detectar, registrar e informar à estação gerente condições de erro e eventos significativos da rede.
- Enviar informações de gerenciamento para múltiplas estações gerentes, permitindo, no caso de situações críticas de operação da rede gerenciada, que a causa da falha ou mau funcionamento da rede possa ser diagnosticada a partir de mais de uma estação gerente.

RMON1 e RMON2 são complementares ao protocolo específico RMON, o RMON1 opera somente na camada MAD (Media Access Control), oferecendo recurso ao administrador da rede para monitorar o tráfego e coletar informações da operação de um segmento de rede local, além de diagnóstico remoto de falhas e erros, RMON só trabalha na MAC, portanto possui os defeitos de não gerar estatísticas de outros protocolos como o IP e não distingue o tráfego originado de um roteador.

O RMON2, por sua vez, opera no nível da camada de rede e camadas superiores, complementando portanto o RMON1, possibilitando coletar informações estatísticas e monitorar a comunicação fim-a-fim e o tráfego gerado por diferentes tipos de aplicação. A figura a seguir ilustra esta diferença.

Proxies

O uso de SNMP requer que todos os agentes, bem como as estações de gerência, suportem UDP e IP, o que limita o gerenciamento direto de dispositivos e exclui outros, tais como bridges e modems, que não suportam nenhuma parte da pilha de protocolos do TCP/IP. Além disso, existem inúmeros pequenos sistemas (PCs, workstations, controladores programáveis) que implementam TCP/IP para suportar suas aplicações, mas para os quais não é desejável adicionar o peso do SNMP.

Para acomodar dispositivos que não implementam SNMP, foi desenvolvido um conceito de proxy. Neste esquema, um agente SNMP atua como um proxy para um ou mais dispositivos, isto é o agente SNMP atua a favor dos dispositivos sob o proxy.

CMIP

O CMIP é o protocolo para gerenciamento de redes definido pelo modelo OSI. O CMIP especifica os elementos de protocolo que são usados para prover os serviços de operação e notificação definidos pelo CMIS. É implementado num modelo orientado a objetos e baseado em eventos. Destina-se ao gerenciamento de diferentes níveis do modelo OSI, inclusive o de aplicações. Devido à sua complexidade, tem uso restrito.

CMIS

Define os serviços providos para o sistema de gerenciamento OSI. Estes serviços são invocados pelos processos de gerenciamento para comunicação remota. É uma interface de serviços de gerenciamento de redes OSI que monitora e controla redes heterogêneas.

CMOT

Criado com objetivo de viabilizar a convivência da arquitetura Internet e do protocolo de gerenciamento OSI, o CMOT se baseia na estrutura de gerenciamento OSI e nos modelos, serviços e protocolos desenvolvidos pela ISO para gerenciamento de redes. O CMOT permite que a estrutura de gerenciamento OSI possa ser aplicada sobre os objetos gerenciados de uma rede TCP/IP.

CORBA

CORBA (Common Object Request Broker Architecture) é um padrão atualmente em desenvolvimento pelo OMG (Object Management Group) para fornecer mecanismos pelos quais objetos podem, de forma transparente, fazer solicitações e receber respostas. O CORBA ORB é uma estrutura que fornece interoperabilidade entre objetos, construída em (possivelmente) linguagens diferentes, executando em (possivelmente) máquinas diferentes em ambientes heterogêneos distribuídos.

Comparação: SNMP versus CMIP

No gerenciamento OSI, objetos gerenciados são vistos como entidades sofisticadas com atributos, procedimentos associados e capacidades de notificação, e outras características complexas associadas com a tecnologia orientada a objetos. Para manter o SNMP simples, ele não foi projetado para trabalhar com tais conceitos sofisticados. Na verdade, os objetos no SNMP não são objetos propriamente ditos do ponto de vista da orientação a objetos; ao invés disso, objetos no SNMP são simplesmente variáveis com poucas características, tais como tipo de dados e permissões de leitura e/ou escrita.

Em relação à MIB, as duas arquiteturas adotaram a abordagem orientada a objetos para descrever e especificar as informações nela armazenadas. No caso Internet, são definidos os objetos a serem armazenados na MIB. A ISO, por sua vez, especifica

algumas classes de objetos a serem empregadas pelos sistemas de gerenciamento e fornece um guia de definição dos objetos gerenciados.

A partir dos diversos aspectos apresentados sobre as arquiteturas de gerenciamento OSI e Internet, pode-se concluir que:

- As duas arquiteturas apresentam modelos de gerenciamento similares envolvendo elementos agentes e gerentes da rede, uma MIB e um protocolo de aplicação responsável pelo transporte de operações e informações de gerenciamento entre tais elementos agentes e gerente.
- No caso da arquitetura Internet, o elemento agente é muito mais simples. A sua função básica é responder às operações de gerenciamento emitidas pelo gerente. No caso OSI, o agente tanto responde às operações como também emite notificações quaisquer de gerenciamento. Tais operações são mais complexas do que as definidas para sistemas Internet. Vale salientar também que, tanto no OSI como no SNMPv2 um elemento de rede pode exercer os papéis de agente e de gerente simultaneamente, o que não acontece no SNMP.
- No que diz respeito aos protocolos de gerenciamento, o SNMP é um protocolo não orientado à conexão que normalmente utiliza os serviços prestados pelo UDP. O CMIP é um protocolo orientado à conexão executado sobre toda pilha de protocolos OSI de gerenciamento. Dentro deste contexto, pode-se afirmar que o sistema de gerenciamento OSI apresenta um nível de confiabilidade maior em relação ao da Internet. Contudo, em determinadas situações de falhas, a simplicidade do SNMP pode representar uma eficiência maior na solução do problema ocorrido.

Referências

MENEZES, E. S; SILVA, P. L. L. Gerenciamento de Redes: Estudos de Protocolos, Workshop de Administração e Integração de Sistemas, UFP, Pernambuco, Setembro 1998; Disponível em: <<http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html>>. Acesso em: Agosto de 2016.