Redes de Computadores II

Aula 13 - Gerenciamento de Redes – Parte I

Apresentação

Veja aqui uma introdução a esta aula.

Vídeo 01 - Apresentação

Nesta aula, vamos tratar de um assunto fundamental para quem administra qualquer rede de computadores que é a gerência de redes. Como veremos, e você já deve imaginar, precisamos acompanhar se a rede, incluindo os computadores e os programas, estão funcionando conforme o esperado. Você aprenderá que, além do monitoramento, a gerência de redes também compreende a tarefa de configuração dos equipamentos, e que isso é feito não apenas no momento inicial da implantação, mas ao longo de todo o tempo de operação da rede. Você estudará em detalhes o protocolo SNMP e verá como ele é utilizado para realizar a gerência de uma rede de computadores.

Objetivos

Ao final desta aula, você será capaz de:

- Identificar elementos que precisam ser monitorados em uma rede.
- Descrever a arquitetura do protocolo SNMP.
- Utilizar o SNMP para realizar a gerência de uma rede de computadores.
- Identificar ferramentas disponíveis para serem utilizadas na gerência de redes de computadores.

Gerência de Redes

Estamos chegando ao fim da disciplina de Redes de Computadores II e você já estudou uma série de protocolos e serviços que são utilizados nas redes de computadores. Portanto, você já sabe que quando for instalar uma rede na prática, vai ter que instalar e configurar vários desses protocolos e programas. Mas será que após a fase de instalação e configuração o trabalho termina? De modo algum! Depois que a rede está em funcionamento, podem acontecer diversos problemas, como, por exemplo:

- Equipamentos que deixam de funcionar completamente.Switchs, roteadores, ou mesmo computadores, podem apresentar problemas de hardware e pararem de funcionar.

- Equipamentos que apresentam erros esporádicos. Os problemas de hardware descritos no item anterior, podem se apresentar apenas de tempos em tempos, dificultando ainda mais a sua detecção. Pense, por exemplo, em uma placa de rede que de vez em quando apresenta problemas, fazendo com que os quadros sejam perdidos.

- Programas que param de funcionar. Os programas podem parar de funcionar ou passarem a executar de modo muito lento, devido a bugs, ataques, ou sobrecarga.

- Tráfego elevado que deixa a rede lenta. É muito comum os usuários de uma rede reclamarem que a ela está lenta. Isso pode acontecer por várias razões, incluindo: i) máquinas foram infectadas com vírus e estão gerando tráfego adicional; ii) os usuários estão utilizando aplicações que geram muito tráfego, mas que não fazem parte dos negócios da empresa, como Peer-to-Peer (P2P), por exemplo; iii) a própria rede da empresa cresceu e os links precisam ser redimensionados (ter suas velocidades aumentadas).

- O link de Internet, ou entre matriz e filiais, deixa de funcionar. Muitas dessas conexões atualmente são por links de rádio, que deixam de funcionar quando as antenas sofrem alguma mudança na sua posição (devido ao vento, por exemplo). Outras vezes, esses links são fornecidos por outras empresas e, portanto, manter esses links funcionando é de responsabilidade delas.

- Capacidade máxima atingida. Agrupamos aqui diversos outros problemas, como computadores trabalhando com 100% de utilização da CPU e/ou da memória, além de discos rígidos (ou partições) sem espaço livre disponível, entre outros.

Diante de tantos possíveis problemas que podem ocorrer, você não deve esperar que as pessoas reclamem que algo não está funcionando bem, para que só então você tome conhecimento desse fato e faça algo para corrigir o problema. Você deve se antecipar a respeito das reclamações e tentar resolver o problema o mais rápido possível, de preferência antes mesmo que as pessoas tomem conhecimento dele.

Suponha, por exemplo, que um switch parou de funcionar. Caso você detecte esse problema logo depois que ele ocorre, você pode trocar o switch com defeito por outro. Naturalmente, as pessoas que estavam usando a parte da rede afetada por esse switch vão notar o problema. Entretanto, a rede vai voltar a funcionar muito mais rapidamente do que se você tivesse que esperar alguém reclamar do problema. Além disso, muitas pessoas poderiam não estar usando a rede naquele momento, e essas pessoas nem mesmo iriam notar que o problema aconteceu.

Situação semelhante se aplica ao caso de um link que conecta uma matriz e uma filial, ou conecta a empresa à Internet. Você pode monitorar a utilização desse link constantemente. Quando notar que ele está frequentemente sendo usado na sua capacidade máxima, você pode tomar algumas medidas, como, por exemplo, solicitar que a capacidade do link seja aumentada, ou identificar e controlar quais aplicações estão gerando o tráfego em excesso.

Para várias situações você poderá mesmo impedir que o problema ocorra se estiver monitorando as coisas corretamente. Independentemente dos problemas que podem ocorrer, dificilmente uma rede vai permanecer sempre do mesmo modo

que foi instalada. Normalmente, a rede da empresa cresce de tamanho, ou então precisa ser reconfigurada para atender mudanças na própria empresa.

Nesses casos, você não vai querer ir fisicamente até o local onde está cada equipamento que precisa reconfigurar para poder fazer essa tarefa. Até porque estes equipamentos podem estar em outro prédio na mesma cidade, ou mesmo em uma cidade diferente!

Com certeza você vai preferir reconfigurar os equipamentos sem sair da sala onde trabalha, utilizando, para isso, a própria rede da empresa.

Veja que identificamos dois tipos de tarefa que precisam ser realizadas para manter as redes em bom funcionamento, que são: **monitoramento** e **configuração**. Essas duas tarefas juntas recebem o nome de **gerenciamento de redes**.

Mais formalmente, a ISO criou um modelo de gerenciamento de rede composto por cinco áreas:

- Gerenciamento de desempenho – Está relacionado a questões como taxa de utilização dos links, carga de CPU e memória etc.
- Gerenciamento de falhas – Está relacionado a problemas na rede, como, por exemplo, *queda* de links, equipamentos ou programas que param de funcionar etc.
- Gerenciamento de configuração – Está relacionado à análise das configurações dos equipamentos e programas, e a possibilidade de realizar alterações nessas configurações.
- Gerenciamento de contabilização – Está relacionado à contabilização da utilização dos recursos pelos usuários, por exemplo, para realizar cobranças. Por exemplo, a quantidade de bytes transmitidos, ou o número de e-mails enviados.
- Gerenciamento de segurança – Está relacionado à definição de uma política de controle de acesso aos recursos, e de mecanismos para garantir que essa política seja cumprida. Por exemplo, a utilização de firewalls para controlar quem acessa determinados serviços, como o servidor de banco de dados da empresa.

Nesta aula, você verá que a forma mais comum de fazer gerenciamento de redes é utilizar um protocolo que realize a comunicação com os equipamentos que precisam ser monitorados e/ou configurados. Como você vai começar a estudar na próxima seção, esse protocolo é o SNMP.

Veja aqui a explicação em vídeo sobre a necessidade do gerenciamento.

Vídeo 02 - Gerenciamento de Redes

Vídeo 03 - Gerencia Introdução

Atividade 01

1. Suponha que você pretende analisar a popularidade do seu site e pretende medir quantos acessos o servidor Web recebe por dia. Em qual das cinco áreas de gerenciamento estudadas, essa tarefa melhor se encaixa?

O Protocolo SNMP

O protocolo SNMP (***S**imple **N**etwork **M**anagement **P**rotocol - Protocolo Simples de Gerência de Rede*) é um protocolo de gerenciamento de redes amplamente utilizado nas redes de computadores há vários anos, permitindo tanto o monitoramento quanto a configuração dos equipamentos.

O SNMP é um protocolo da camada de aplicação que utiliza o UDP como protocolo de transporte para enviar suas mensagens. Pode ser utilizado para gerenciar qualquer tipo de equipamento, como computadores, switches, roteadores,

e até mesmo nobreaks e modems.

Qualquer que seja o fabricante e modelo do seu computador, ele deve suportar SNMP, porque como o SNMP é implementado por um programa, basta que o sistema operacional suporte SNMP – e não o hardware. Para os sistemas operacionais que utilizamos nos computadores, como Linux, Windows, Mac OS (Apple), isso não é problema, pois todos eles possuem o SNMP.

Para outros equipamentos, como switches e roteadores, por exemplo, nos quais não temos a liberdade de instalar programas, como nos computadores, é importante observar se o equipamento já vem com suporte ao SNMP.

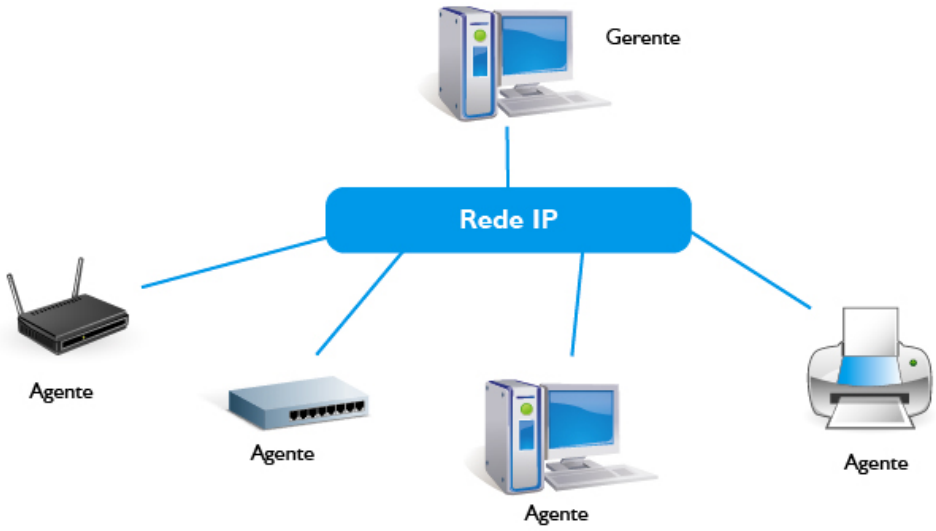
> Idealmente todos os equipamentos de rede deveriam suportar gerenciamento. Entretanto, para reduzir os custos, existem modelos de equipamentos que não o fazem. Isso acontece, por exemplo, com vários modelos de switchs. Na sua rede, procure usar sempre equipamentos gerenciáveis.

Comunicação entre o Gerente e os Agentes

Quando se pensa em como seria de fato o gerenciamento de uma rede, em termos dos papéis que cada máquina desempenha, é natural imaginar que temos uma máquina principal de onde o administrador da rede realiza a gerência da rede, ou seja, solicita informações às máquinas monitoradas, ou envia comandos de configuração para elas.

No SNMP, essa máquina principal é chamada de **Gerente** e as máquinas gerenciadas são chamadas de **Agentes**. Do mesmo modo, dizemos que o software que é executado na máquina principal é chamado de gerente e o software executado nos demais equipamentos é chamado de agente. Ou seja, usamos os termos gerente e agente tanto para o equipamento como um todo quanto para o software SNMP sendo executado nele. Tal fato é mostrado na Figura 1.

Figura 01 - Agentes e Gerente no SNMP.



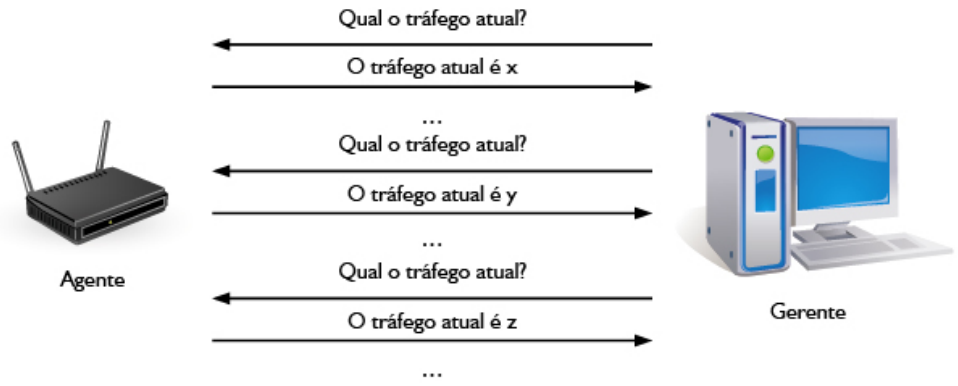
Naturalmente, o administrador da rede não precisa ficar sentado na frente da máquina de gerência para que o processo ocorra. O software SNMP de gerência pode realizar as tarefas de modo automático, conforme determinado previamente pelo administrador, gerando alertas para ele (através de e-mail, mensagem para celular etc.) quando for necessário.

Embora tenhamos citado que o modelo utiliza **uma** estação de gerência, o SNMP permite que sejam utilizadas **várias** estações de gerência.

Na forma mais comum de trabalhar, é o gerente SNMP que fica enviando requisições periodicamente para obter informações do agente. Pense por exemplo, que o gerente pretende gerar um gráfico com o tráfego de rede no link com a Internet a cada instante. Nesse caso, o gerente fica enviando solicitações repetidamente (a cada 30 segundos, por exemplo) ao roteador conectado ao link de Internet, pedindo que ele informe o valor do tráfego sendo utilizado naquele instante.

Esse modelo é chamado de *Pooling* e, como dissemos, é o mais utilizado para realizar o monitoramento. A Figura 2 ilustra esse esquema.

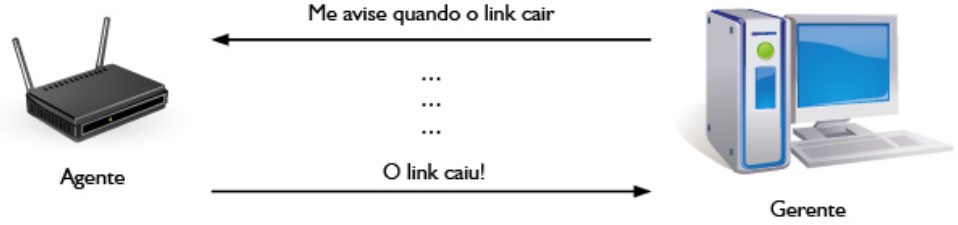
Figura 02 - Utilização de *Pooling*.



Existem situações, entretanto, em que ele não é muito indicado. Suponha, por exemplo, que queremos monitorar apenas se o link ao qual um roteador está conectado está funcionando ou não. Por exemplo, o link para uma filial. Nesse caso, não faz sentido ficar perguntando ao roteador a todo instante se o link está funcionando, pois a resposta vai ser sempre que sim (enquanto o link estiver funcionando)! Uma forma mais eficiente, é pedir ao roteador que nos avise (a estação de gerência) quando o link parar de funcionar.

Esse método é conhecido como *Trap* e consiste em definir uma condição que o agente deve ficar verificando. Quando ela acontece, o agente envia uma mensagem informando esse fato ao gerente. A Figura 3 ilustra esse esquema.

Figura 03 - Utilização de Traps.



Outros exemplos de condições que são adequadas para a utilização com o método de Traps são: o número de conexões TCP abertas na máquina excederem um certo valor, o espaço livre em disco está abaixo de um certo valor, o número de quadros com erro recebidos por uma placa de rede excederem um certo valor etc.

Além de o gerente solicitar informações ao agente (monitoramento), naturalmente, ele pode realizar alguma configuração no agente. Por exemplo, o gerente pode solicitar ao agente executando em um switch que desative uma determinada porta. Isso teria o mesmo efeito que desconectar o cabo de rede daquela porta do switch.

Veja aqui a explicação em vídeo sobre o modelo de agentes e gerentes do SNMP

Vídeo 04 - Agentes e Gerentes

Atividade 02

1. Suponha que você está suspeitando que o ventilador (cooler) de um determinado computador está com problemas e pretende monitorar a temperatura do processador para que ela não passe de um determinado valor. Qual modelo (pooling ou trap) é mais adequado para esta situação?

Informações Compreendidas pelo SNMP

Já citamos vários exemplos de informações que podem ser monitoradas/configuradas pelo SNMP. Qual é a relação completa das informações especificadas pelo protocolo SNMP?

A resposta é **nenhuma**! Ou seja, o protocolo SNMP não define quais informações podem ser monitoradas/configuradas. Ele define apenas um mecanismo para transmitir informações. Quem precisa entendê-las são os programas agentes e os gerentes. Talvez você fique surpreso com a resposta. Mas esse modelo é que permite ao SNMP gerenciar qualquer tipo de equipamento.

Suponha que você criou um ventilador inteligente que pode ser ligado à Internet. Se seu ventilador possui três velocidades, você poderia ser capaz de verificar a velocidade em que ele se encontra (ou mudar a velocidade) usando SNMP. Isso seria possível porque o SNMP não precisaria entender o tipo de informação gerenciada (a velocidade do ventilador). Quem precisaria fazer isso era o agente dentro do ventilador. O protocolo SNMP se encarregaria apenas de transmitir as informações entre o gerente e o agente.

As informações que podem ser manipuladas nos diversos equipamentos, e que chamamos de informação gerenciada no parágrafo anterior, são divididas em grupos chamados ***M****anagement* ***I****nformation* ***B****ase* (***MIB***, Base de Informações de Gerenciamento).

Cada MIB contém um conjunto de informações que de certo modo estão relacionadas de alguma forma. Entenda uma MIB como um conjunto de variáveis que podem ser lidas ou alteradas. Cada variável representa uma informação, como por exemplo, o número de conexões TCP abertas, o número de quadros transmitidos etc.

Na verdade, o termo correto para identificar cada informação em uma MIB não é **variável**, mas sim **objeto**.

Alterar o valor de um objeto, altera o comportamento do equipamento. Por exemplo, alterar o valor de um objeto que controla se o roteamento está ativo ou não, de fato irá ativar ou desativar o roteamento. Portanto, a configuração de equipamentos utilizando SNMP, é feita, de fato, alterando-se o valor dos objetos.

Existem diversas MIB que são padronizadas e diversas outras que são criadas por diferentes empresas, como os fabricantes de equipamentos, por exemplo.

Cada agente deve ser capaz de entender as informações da MIB que ele resolver suportar.

Voltando ao exemplo do ventilador. Você poderia criar uma MIB que contivesse apenas dois objetos. Um para representar se o ventilador está ligado ou desligado, e outro para controlar a velocidade (também poderia ser feito com apenas um objeto).

O seu agente precisaria entender essa MIB, e quando alguém mudasse o valor do objeto que representa se o ventilador está ligado, ele deveria ligar (ou desligar) o ventilador.

Vídeo 05 - SNMP

Atividade 03

1. Qual é o protocolo de transporte utilizado para transmitir mensagens SNMP?
2. O que é uma MIB?

Resumo

Nesta aula, você aprendeu que toda rede precisa ser monitorada constantemente para identificação de falhas e problemas de desempenho. Além disso, reconfigurações também precisam ser realizadas com frequência. Essas tarefas de monitoramento e configuração formam o que é chamado de gerência de redes. Iniciamos nossos estudos conhecendo o protocolo SNMP, que utiliza o conceito de agentes e gerentes.

Autoavaliação

1. Quais são as áreas de gerenciamento de redes estabelecidas pela ISO?
2. Qual o protocolo de transporte utilizado pelo protocolo 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, K.**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.