**Outros componentes da arquitetura TCP/IP**

DHCP - Configuração e geração automática de endereços IP na rede

A geração e a administração de endereços IP são trabalhosas. Para automatizar parte desta tarefa foi criado o protocolo DHCP (Dynamic Host Configuration Protocol) que, por meio de um servidor DHCP, distribui os endereços, máscaras, gateway padrão e outras configurações automaticamente para os computadores da rede quando são ligados.

Os computadores da rede devem possuir um software cliente DHCP para se comunicar com o servidor DHCP. Normalmente esse software cliente vem no sistema operacional do computador, como o Windows. Solicita e obtém do servidor DHCP as configurações básicas do TCP/IP, como endereço IP, máscara e endereço IP do default gateway (roteador padrão), quando é ligado.

A partir de uma faixa de endereços IP predefinidos, o servidor DHCP atribui endereços aos computadores que estão na rede e que estejam configurados com o cliente DHCP.

O servidor DHCP normalmente atende a um segmento de rede. Para atender a outros, o roteador que interliga os outros segmentos deve ter o agente DHCP e fazer a ponte entre o computador cliente e o servidor DHCP.

A partir de uma faixa de endereços IP, o servidor DHCP faz a alocação dinâmica dos endereços IP e outras configurações para os computadores da rede.

NAT (Network Address Translation)

Quando a rede interna de uma empresa é ligada à Internet, é preciso que todos os computadores tenham endereços válidos para se comunicarem com ela. Como a quantidade de endereços IP da Internet é limitada e também para evitar conflitos de endereços entre as redes internas e a Internet, foram reservados três conjuntos de numeração para redes internas, conforme já vimos. Esses endereços são chamados de privados ou reservados.

Classe A privado: vai de 10.0,0.0 a 10.255.255.255

Classe B privado: de 172.16.0.0 a 172.31.255.255

Classe C privado: de 192.168.0.0 a 192.168.255.255

As empresas usam essas faixas de endereços IP em suas redes internas e para acesso à Internet utilizam endereços externos registrados.

Quando um computador das redes internas da empresa vai acessar a Internet, é preciso associar o endereço IP do computador na rede interna com o endereço IP externo de acesso à Internet.

O NAT tem a função de traduzir os endereços válidos e registrados de acesso à Internet para os endereços reservados da rede interna e vice-versa. Essa tradução também se chama address translation. O NAT pode ser implementado em um roteador ou em um computador no firewall. O roteador com NAT monta uma tabela com o endereço local interno do computador e o endereço externo que ele está acessando. Quando os dados vêm do endereço externo, o roteador consulta a tabela de tradução e encaminha-os para o endereço interno.

Os hosts de uma rede interna com endereços privados acessam os endereços IP públicos da Internet. Com essa facilidade obtemos aumento da segurança, pois os endereços internos privados não são válidos na Internet e não podem ser acessados diretamente a partir dela.

Com o NAT podemos também alterar a faixa de endereços IP da Internet sem alterar a numeração interna dos computadores da empresa, evitando assim muito trabalho de configurações.

A tradução dos endereços da rede interna para a externa pode ser de um para um, ou seja, um endereço interno para um externo, ou pode ser feita dinamicamente, em que só existe a associação quando um computador da rede interna quer fazer um acesso externo. A associação dinâmica é mais racional, pois otimiza a utilização dos endereços externos, permitindo que, para uma faixa reduzida de endereços externos válidos, haja uma quantidade relativamente maior de endereços internos. Por exemplo, para uma faixa de apenas 14 endereços externos IP válidos, podemos ter internamente na empresa 30 hosts ou mais acessando a Internet, utilizando compartilhadamente os 14 endereços disponíveis.

Em relação aos endereços IP privados, uma empresa poderia utilizar qualquer faixa para montar o endereçamento de suas redes internas, porém ao conectar-se à Internet, teria conflitos de endereços. Para evitar este problema devemos, preferencialmente, estruturar o plano de endereçamento IP das redes internas de uma empresa de forma a utilizar os endereços privados, os quais não têm permissão para se anunciarem como rotas na Internet.

DNS (Domain Name System)

Os endereços IP que trafegam nos equipamentos da rede Internet ou nas redes locais são difíceis de lembrar. Para superar a dificuldade de lembrar endereços IP para poder acessar sites na internet, foi desenvolvida uma equivalência de nomes aos endereços IP. A cada nome de site na Internet é associado o seu endereço IP correspondente. Esses nomes são chamados de domínios. Assim, os acessos passam a ser feitos por nomes, os quais conhecemos como [www.nome.yyy](http://www.nome.yyy), para facilitar. Um exemplo de domínio é www.empresaxyz.com.br.

Para que os dados percorram a rede e os endereços sejam entendidos por ela, é preciso traduzir o nome de domínio (www) para o seu respectivo endereço IP numérico. Quem faz isso são servidores DNS que possuem tabelas de conversão e ficam nos provedores de acesso à Internet ou em outros pontos da rede, assim como também em servidores DNS de Intranets dentro da empresa.

O DNS é o sistema de tradução de domínios (www) para os seus respectivos endereços IP que trafegam na rede. Os nomes e endereços IP ficam em tabelas em banco de dados nos servidores DNS. O DNS gerencia e traduz nomes dos domínios .edu; .com; .net; .gov; .mil; versus os endereços IP correspondentes.

Na Internet existem vários servidores DNS interligados logicamente numa estrutura hierárquica a servidores DNS centrais (root). Toda rede deve ter um servidor DNS, que lê um nome de domínio (www) e descobre o seu endereço IP correspondente. Se um determinado servidor DNS não possuir o endereço IP correspondente, então vai procurar e consultar em outros servidores DNS espalhados pela rede.

Protocolo HTTP (Hypertext Transfer Protocol)

O HTTP faz a comunicação entre o browser (programa client responsável pelo recebimento de páginas web) do computador e o servidor web que ele vai acessar. Esse protocolo faz parte da camada de aplicação da arquitetura TCP/IP.

Protocolo TELNET (Terminal Emulator)

É uma aplicação que faz a conexão e a simulação do terminal de um servidor ou equipamento. É um protocolo utilizado para acessar equipamentos e servidores remotamente, por meio de uma conexão remota. O computador com o TELNET comporta-se como uma estação local do servidor, ou seja, o TELNET simula um terminal do servidor que se quer acessar. É utilizado tanto para efetuar consultas a um computador, como para configurar equipamentos remotamente.

O acesso pode ser por cabo direto, quando queremos configurar um equipamento utilizando um computador com TELNET, por exemplo, ou por uma rede como a Internet para acessar um sistema remoto. Ou seja, o TELNET simula o terminal de um computador servidor ou de um equipamento que tenham interface TCP/IP.

Protocolo FTP (File Transfer Protocol)

É uma aplicação da arquitetura TCP/IP utilizada para transferência de arquivos entre dois computadores. O FTP permite interatividade entre o cliente (computador que solicita o arquivo) e o servidor (computador que irá fornecer o arquivo), com segurança, por meio de logins e senhas.

Protocolo TFTP (Trivial File Transfer Protocol)

É uma aplicação da arquitetura TCP/ IP utilizada para transferência de arquivos entre dois computadores numa rede IP, utilizado com o protocolo UDP na camada de transporte. Ou seja, é uma transferência de arquivos sem os controles de fluxo e sem os controles de sequência de pacotes.

Protocolos SMTP (Simple Mail Transfer Protocol) e POP (Post Office Protocol)

Analogamente ao protocolo HTTP, os protocolos SMTP e POP são responsáveis pela comunicação entre um computador e um servidor, neste caso um servidor de correio eletrônico para recebimento e envio de mensagens de e-mail respectivamente.

Protocolo NFS (Network File System)

Análogo ao FTP, o NFS faz transferências de arquivos, porém adicionalmente faz acesso on-line aos arquivos da rede utilizando como protocolo de transporte o UDP e não 0 TCP.

Protocolo SMMP (Simple Network Management Protocol)

É um protocolo de comunicação utilizado em uma rede para transmitir informações de status dos equipamentos conectados à rede. Os computadores e demais equipamentos da rede possuem um software client também chamado de agente SNMP que recolhe informações do próprio equipamento e envia para um servidor de gerenciamento.

No servidor central da plataforma de gerenciamento existe um software chamado de gerente SNMP que recebe essas informações e as armazena numa base de dados chamada MIB (Management Information Base). Com esses dados são feitas estatística e análises da rede, como a avaliação do tráfego, visando obter subsídios para efetuar ações corretivas ou de expansão e adequação da rede.

Essas informações também podem ser utilizadas para compor um diagrama da rede que é programado para alarmar e sinalizar os componentes que estão com problemas, avisando os operadores de rede para tomarem as devidas ações corretivas ou preventivas.

Assim, todos os equipamentos de uma rede que tiverem um agente SNMP enviando informações de status para um gerenciador SNMP podem ser monitorados em tempo real e na sinalização de qualquer problema proporcionarem um imediato conhecimento do problema, agilizando a solução.