TCP/IP – Estudo Geral

TCP/IP – Estudo 1

Introdução:

Para "hackear" um sistema ligado a Internet/Intranet ou até mesmo um uma simples rede que utiliza o tcp/ip, nada melhor do que saber lidar a fundo com o protocolo mais usado e mais famoso no mundo inteiro. TCP/IP TCP/IP e o nome que se da a toda a família de protocolos utilizados pela Internet. Esta família de protocolos foi desenvolvida pela DARPA (Defense Advanced Research Project Agency) no DoD (Departamento de Defesa dos Estados Unidos).
Este conjunto de protocolos foi desenvolvido p/permitir aos computadores compartilharem recursos numa rede. Toda a família de protocolos incluem um conjunto de padrões que especificam os detalhes de como comunicar computadores, assim como também convenções para interconectar redes e rotear o trafego.
Mas ao contrario do que acontece na imprensa, o nome completo raramente é usado. O TCP e o IP são protocolos individuais que podem ser discutidos de modo isolado, mas eles não são os únicos protocolos que compõem essa família. Pode acontecer de um usuário do TCP/IP não utilizar o protocolo TCP propriamente dito, mas sim alguns protocolos da família. A utilização do TCP/IP nessa situação deixa de ser apropriada porque o nome se aplica de modo genérico ao uso de qualquer protocolo da família TCP/IP.

Familia
ARP Address Resolution Protocol
ICMP Internet Control Message Protocol
UDP User Datagram Protocol
RIP Routing Information Protocol
HTTP Hypertext Transfer Protocol
NNTP Network News Transfer Protocol
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
FTP File Transfer Protocol
TFTP Trivial File Transfer Protocol
INET PHONE Telephone Services on Internet
IRC Internet Relay Chat
RPC Remote Procedure Call
NFS Network File System
DNS Domain Name System

Talvez seja difícil lembrar todos esses acrônimos, ate porque alguns também são utilizados por outros protocolos (por exemplo o protocolo RIP da família Novell, ou o IPX, é diferente do RIP da família TCP/IP). Alem do mais, saber exatamente quais

são os protocolos que compõem uma determinada família não é pré-requisito para compreender o funcionamento básico da rede.

Uma visão resumida do Protocolo

Alguma transferência se inicia com um pedido de leitura ou escrita de um arquivo, o qual também serve para pedir uma conexão. Se o servidor reconhece o pedido, a conexão é aberta e o arquivo é enviado num bloco de tamanho fixo de 512 bytes. Cada pacote de dados contem um bloco de dados e deve ser reconhecido por um pacote de acknowledgment antes que o próximo pacote possa ser enviado. Um pacote de dados menor que 512 bytes sinaliza a terminação de uma transferencia. Se um pacote consegue se perder na rede, o receptor indicara time-out e poderá retransmitir seu ultimo pacote (o qual pode ser dados ou um reconhecimento). Isto motiva ao transmissor do pacote perdido a retransmitir o pacote perdido. O transmissor tem que guardar apenas um pacote para retransmissao, desde cada passo de reconhecimento garante que todos os pacotes mais anteriores tenham sido recebidos.

Notar que as duas maquinas envolvidas na transferencia são consideradas transmissoras e receptoras. Uma envia dados e recebe reconhecimento, a outra envia reconhecimento e recebe dados.

Muitos erros são causados pela terminação da conexão. Um erro e sinalizado enviando um pacote de erro. Este pacote não e reconhecido nem retransmitido (i.e., um servidor TFTP ou usuário pode terminar depois enviando uma mensagem de erro) assim o outro terminal da conexão não deve recebe-lo. Portanto os time-out são usados para detectar tais terminais quando o pacote de erro foi perdido.

Protocolo IP O protocolo IP define mecanismos de expedição de pacotes sem conexão. IP define três pontos importantes:

1.- A unidade básica de dados a ser transferida na Internet.

2.- O software de IP executa a função de roteamento, escolhendo um caminho sobre o qual os dados serão enviados.

3.- Incluir um conjunto de regras que envolvem a idéia da expedição de pacotes não confiáveis. Estas regras indicam como os hosts ou gateways poderiam processar os pacotes; como e quando as mensagens de erros poderiam ser geradas; e as condições em que os pacotes podem ser descartados.

Dentro do protocolo IP tem os seguintes tópicos:

- Endereços IP
- Formato do datagrama IP
- Roteamento do datagrama IP
- ICMP (Internet Control Message Protocol)

Protocolo IP TCP (Transport Control Protocol) TCP e um protocolo da camada de transporte. Este e um protocolo orientado a conexão, o que indica que neste nível vão ser solucionados todos os problemas de erros que não forem solucionados no nível IP, dado que este ultimo e um protocolo sem conexão. Alguns dos problemas com os q TCP deve tratar são: pacotes perdidos ou destruídos por erros de transmissão. expedição de pacotes fora de ordem ou duplicados.

O TCP especifica o formato dos pacotes de dados e de reconhecimentos que dois computadores trocam para realizar uma transferência confiável, assim como os procedimentos que os computadores usam para assegurar que os dados cheguem corretamente. Entre estes procedimentos estão:

Distinguir entre múltiplos destinos numa maquina determinada. Fazer recuperação de erros, tais como pacotes perdidos ou duplicados. Para entender melhor o protocolo TCP a seguir veremos alguns conceitos, para depois passarmos ao formato TCP.

1-) Portas, Conexões e Endpoints
2-) Segmentos, fluxo e Numero de Seqüência
3-) Formato do Segmento TCP

DNS (Domain Name System)

O DNS (Domain Name System) e um esquema de gerenciamento de nomes, hierárquico e distribuído. O DNS define a sintaxe dos nome s usados na Internet, regras para delegação de autoridade na definição de nomes, um banco de dados distribuído que associa nomes a atributos (entre eles o endereço IP) e um algoritmo distribuído para mapear nomes em endereços. O DNS e especificado nas RFCs 882, 883 e 973.

As aplicações normalmente utilizam um endereço IP de 32 bits no sentido de abrir uma conexão ou enviar um datagrama IP. Entretanto, os usuários preferem identificar as maquinas através de nomes ao invés de números. Assim e necessário um banco de dados que permita a uma aplicação encontrar um endereço, dado que ela conhece o nome da maquina com a qual se deseja comunicar.

Um conjunto de servidores de nomes mantém o banco de dados com os nomes e endereços das maquinas conectadas a Internet. Na realidade este e apenas um tipo de informação armazenada no domain system (sistema de domínios).Note que e usado um conjunto de servidores interconectados, ao invés de um único servidor centralizado. Existem atualmente tantas instituições conectadas a Internet que seria impraticável exigir q elas notificassem uma autoridade central toda vez que uma maquina fosse instalada ou trocasse de lugar. Assim, a autoridade para atribuição de nomes e delegada a instituições individuais. Os servidores de nome formam uma arvore, correspondendo a estrutura institucional. Os nomes também adotam uma estrutura similar.

Um exemplo típico e o nome chupeta.jxh.xyz.br. Para encontrar seu endereço Internet, pode ser necessário o acesso a ate quatro servidores de nomes. Inicialmente deve ser consultado um servidor central, denominado servidor raiz, para descobrir onde esta o servidor br. O servidor br e o responsável pela gerência dos nomes das instituições/empresas brasileiras ligadas a Internet. O servidor raiz informa como resultado da consulta o endereço IP de vários servidores de nome para o nível br (pode existir mais de um servidor de nomes em cada nível, para garantir a continuidade da operação quando um deles para de funcionar). Um servidor do nível br pode então ser consultado, devolvendo o endereço IP do servidor xyz.

De posse do endereço de um servidor xyz e possível solicitar que ele informe o endereço de um servidor jxh, quando, finalmente, pode-se consultar o servidor jxh sobre o endereço da maquina chupeta. O resultado final da busca e o endereço Internet correspondente ao nome chupeta.jxh.xyz.br

Cada um dos níveis percorridos e referenciado como sendo um domínio. O nome completo chupeta.jxh.xyz.br e um nome de domínio. Na maioria dos casos, não e necessário ter acesso a todos os domínios de um nome para encontrar o endereço correspondente, pois os servidores de nome muitas vezes possuem informações sobre mais de um nível de domínio o que elimina uma ou mais consultas. Além

disso, as aplicações normalmente tem acesso ao DNS através de um processo local (servidor para as aplicações e um cliente DNS),que pode ser implementado de modo a guardar os últimos acessos feitos, e assim resolver a consulta em nível local. Essa abordagem de acesso através de um processo local, simplifica e otimiza a tarefa das aplicações no que tange ao mapeamento de nomes em endereços, uma vez que elimina a necessidade de implementar, em todas as aplicações que fazem uso do DNS, o algoritmo de encaminhamento na arvore de domínios descrito anteriormente. O DNS não se limita a manter e gerenciar endereços na Internet. Cada nome de domínio é um nome em um banco de dados, que pode conter registros definindo varias propriedades. Por exemplo, o tipo da maquina e a lista de serviços fornecidos por ela. O DNS permite que seja definido um alias (nome alternativo) para o no. Também e possível utilizar o DNS para armazenar informações sobre usuários, listas de distribuição ou outros objetos.
O DNS e particularmente importante para o sistema de correio eletrônico. No DNS são definidos registros que identificam a maquina que manipula as correspondências relativas a um dado nome, identificado assim onde um determinado usuário recebe suas correspondências. O DNS pode ser usado também para definição de listas para distribuição de correspondências SMTP - Simple Mail Transfer Protocol O SMTP (Simple Mail Transfer Protocol) e o protocolo usado no sistema de correio eletrônico na arquitetura Internet TCP/IP. Um usuário, ao desejar enviar uma mensagem, utiliza o modulo interface com o usuário para compor a mensagem e solicita ao sistema de correio eletrônico que a entregue ao destinatário. Quando recebe a mensagem do usuário, o sistema de correio eletrônico armazena uma copia da mensagem em seu spool (área do dispositivo de armazenamento), junto com o horário do armazenamento e a identificação do remetente e do destinatário. A transferencia da mensagem e executada por um processo em background, permitindo que o usuário remetente, após entregar a mensagem ao sistema de correio eletrônico, possa executar outras aplicações.
O processo de transferencia de mensagens, executando em background, mapeia o nome da maquina de destino em seu endereço IP, e tenta estabelecer uma conexão TCP com o servidor de correio eletrônico da maquina de destino. Note que o processo de transferencia atua como cliente do servidor do correio eletrônico. Se a conexão for estabelecida, o cliente envia uma copia da mensagem para o servidor, que a armazena em seu spool. Caso a mensagem seja transferida com sucesso, o servidor avisa ao cliente que recebeu e armazenou uma copia da mensagem. Quando recebe a confirmação do recebimento e armazenamento, o cliente retira a copia da mensagem que mantinha em seu spool local. Se a mensagem, por algum motivo, não for transmitida com sucesso, o cliente anota o horário da tentativa e suspende sua execução. Periodicamente o cliente acorda e verifica se existem mensagens a serem enviadas na área de spool e tenta transmiti-las. Se uma mensagem não for enviada por um período, por exemplo de dois dias, o serviço de correio eletrônico devolve a mensagem ao remetente, informando que não conseguiu transmiti-la. Em geral, quando um usuário se conecta ao sistema, o sistema de correio eletrônico e ativado para verificar se existem mensagens na caixa postal do usuário. Se existirem, o sistema de correio eletrônico emite um aviso para o usuário que, quando achar conveniente, ativa o modulo de interface com o usuário para receber as correspondências.
Uma mensagem SMTP divide-se em duas partes: cabeçalho e corpo, separados por

uma linha em branco. No cabeçalho são especificadas as informações necessárias para a transferencia da mensagem. O cabeçalho e composto por linhas, que contem uma palavra-chave seguida de um valor. Por exemplo, identificação do remetente (palavra-chave "to:" seguida do seu endereço), identificação do destinatário, assunto da mensagem, etc... No corpo são transportadas as informações da mensagem propriamente dita. O formato do texto e livre e as mensagens são transferidas no formato texto.

Os usuários do sistema de correio eletrônico são localizados através de um par de identificadores. Um deles especifica o nome da maquina de destino e o outro identifica caixa postal do usuário. Um remetente pode enviar simultaneamente varias copias de uma mensagem, para diferentes destinatários utilizando o conceito de lista de distribuição(um nome que identifica um grupo de usuários). O formato dos endereços SMTP e o seguinte:

nome_local@nome_do_dominio onde o nome_do_dominio identifica o domínio ao qual a maquina de destino pertence (esse endereço deve identificar um grupo de maquinas gerenciado por um servidor de correio eletrônico). O nome local identifica a caixa postal do destinatário.

O SMTP especifica como o sistema de correio eletrônico transfere mensagens de uma maquina para outra. O modulo interface com usuário e a forma como as mensagens são armazenadas não são definidos pelo SMTP. O sistema de correio eletrônico pode também ser utilizado por processos de aplicação para transmitir mensagens contendo textos.

TCP/IP – Estudo 2

Protocolos e Topologias de Redes

LANs - Local Area Networks

1 - Redes Locais

Redes Locais são basicamente um grupo de PCs (desktops) interligados aos servidores. Os usuários de uma LAN executam suas tarefas a partir de seus PCs. Estas tarefas normalmente são edição de texto, planilhas eletrônicas ou aplicações gráficas e o acesso a aplicações disponíveis nos servidores de rede.
A característica mais importante é justamente seu recurso de aceitar aplicativos cooperativos, nos quais um aplicativo é executado em parte nas estações de trabalho e em parte num servidor de rede local ou um host de mainframe.
O IEEE (Institute of Electrical and Electronics Engineers) define uma rede local como como um sistema de comunicação de dados que permite que um número de dispositivos independentes se comunique diretamente um com o outro, dentro de uma área geográfica com tamanho moderado e através de um canal de comunicações de taxas de dados razoáveis.
Os módulos mais importantes de uma rede local são:
Servidores (Servers)
PCs desktop (Workstations)
Recursos de Comunicação

1.1 - Servidor

É um computador com elevada capacidade de processamento, cuja função é disponibilizar serviços à rede. Em geral esta máquina processa grandes volumes de dados (databases), exigindo CPUs rápidas e dispositivos de armazenamento (Hard Disks, Optical Disks) de alta capacidade e de acesso rápido. Os serviços que o "Server" oferece à rede são:
Servidor de Aplicação (Application Server)
Servidor de Arquivos (File Server)
Servidor de Impressoras (Print Server)
Servidor de Rede (Network Server)
Servidor de Banco de Dados Relacional (Relational Database Server)
Dentro da tecnologia atualmente disponível, o hardware servidor é composto de um PC Pentium/P6 mono ou multiprocessado, ou então máquinas RISC de fabricantes como HP, Sun, Digital (linha ALPHA PC) ou IBM.
O Sistema Operacional do servidor se enquadra na categoria "NOS" (Networking Operating Systems). Os "NOS" mais adotados no mercado são:
Netware - Novel Inc.
Windows NT Server - Microsoft Corp.
LAN Server - IBM
Unix - IBM, Sun, HP, SCO...
Banyan ENS - Banyan-Vines

1.2 - PCs Desktop

São as workstations individuais de trabalho. A partir delas os usuários acessam arquivos e aplicativos no servidor e executam tarefas locais. As aplicações Cliente-Servidor são compartilhadas: parte delas são executadas no servidor e parte no

cliente (PC). Um exemplo é uma consulta a um Banco de Dados SQL. O cliente envia uma solicitação de dados ao servidor (em linguagem SQL); o servidor faz o processamento de dados solicitados ,devolvendo-o ao cliente; neste os dados são formatados na forma desejada pelo usuário.

1.3 - Recursos de Comunicação

Significa a infraestrutura de hardware e sotware necessária para a comunicação entre os diversos componentes da LAN. Os recursos mais comuns são os hubs, placas de rede Ethernet, repeaters, bridges, roteadores, cabeamento, etc.

O padrão Ethernet, que define os diversos recursos de comunicação até parte do Nível 2 (lógico) segundo o modelo ISO/OSI, é o mais amplamente utilizado.

2 - O padrão Ethernet

Criada pela xerox, a Ethernet foi uma das primeiras redes locais a serem padronizadas e vendidas por multiplas empresas. Atualmente a maioria dos fabricantes de hardware usa a topologia Ethernet para LANs, além de ser considerada a melhor topologia (layout físico do cabo de conexão) em confiabilidade e produtividade operacional.

Com relação ao nível físico, a Ethernet é uma rede de topologia de barramento, com CSMA/CD (Carrier-sense multiple-access with colision detection), ou seja, cada estação que quiser acessar a linha verifica sua ocupação, se estiver livre, transmite; se não, espera o fim da transmissão atual para transmitir. Se duas estações transmitirem ao mesmo tempo, a colisão é detectada por ambas as estações, que abortam a transmissão, gerando uma retransmissão. Esta retransmissão segue um algoritmo que visa reduzir a chance de uma nova colisão.

3 - Novos padrões de LANs

Novas aplicações, principalmente as que incluem multimídia, necessitam maiores velocidades nas LANs que as oferecidas pelo padrão Ethernet.

FDDI

Padrão relativamente antigo, baseado em fibra óptica. É uma tecnologia ainda cara, porém confiável. Sua utilização maior era a interligação de redes locais (backbones) dada sua alta velocidade (100Mbits/sec).

Fast Ethernet (100Base-T)

É a opção mais simples para migrar a atual base Ethernet (baseada em 10Base-T) para uma taxa de 100Mbits/sec, uma vez que, ao contrário do padrão FDDI, o cabeamento (cabo coaxial) pode ser mantido.

ATM (Asynchronous Transfer Mode)

Surgiu como uma alternativa de melhor desempenho, permitindo 155 Mbits/sec de velocidade, viabilizando aplicações com vídeo e voz em tempo real.

TCP/IP – Estudo 3

1 - Identificadores Universais

Diz-se que um sistema provê um *serviço de comunicação universal* quando é possível a quaisquer dos elementos deste sistema se comunicarem arbitrariamente. Para tornar um sistema de comunicação universal, devemos estabelecer um método globalmente aceito para identificação dos componentes a ele conectados.
Nas redes TCP/IP, a entidade que atua como identificador universal é o endereço IP, um número de 32 dígitos binários. A idéia básica de seus mentores era a de tornar o roteamento simples e eficiente. É verdade que a manipulação deste tipo de número traz grande facilidade para o nível de software mas seu tratamento não é tão simples para um humano. Mais adiante (em Notação Decimal), veremos uma forma de representação de mais "alto nível".

2 - As três Classes Primárias de Endereço

Podemos pensar na Internet como uma gigantesca rede de computadores como qualquer outra rede física. A grande diferença, entretanto, está no fato de que a Internet é uma estrutura virtual, concebida por seus desenhistas e implementada inteiramente em software. Assim, os projetistas tiveram liberdade de arbitrar o tamanho e formato dos pacotes, endereços, técnicas de roteamento, etc. Nada é ditado pelo hardware. Na questão do endereçamento, optou-se por um esquema análogo ao das redes convencionais, onde a cada *host* é atribuído um número inteiro que será seu endereço - no caso o endereço IP. A grande vantagem no esquema de endereçamento da Internet é que ele foi cuidadosamente concebido para simplificar a tarefa de roteamento. Veremos adiante que um endereço IP identifica a rede a qual a máquina está conectada, além da máquina propriamente dita.
Numa primeira visão, cada máquina ligada à Internet possui um endereço de 32 bits, que se divide em duas partes: uma primeira que identifica a rede a qual esse computador está fisicamente conectado e uma segunda parte que identifica o computador propriamente dito. Observe que todas as máquinas conectadas a uma mesma rede irão compartilhar essa primeira parte, que se convencionou chamar *net id* (identificador da rede). Analogamente, à segunda porção do endereço IP chamamos *host id* (identificação da máquina).
Em termos práticos, cada endereço IP deverá estar contido em uma das cinco categorias representadas na **Figura 1**. A classe de um endereço pode ser identificada através do exame dos quatro bits de mais alta ordem, sendo que as três classes básicas (A, B e C) podem ser distinguidas apenas pelos dois primeiros. A classe A, usada para um pequeno número de redes que contêm mais de 65.535 *hosts*, reserva 7 bits para o *net id* e 24 bits para o *host id*. Os endereços da classe B se destinam a redes de tamanho intermediário (entre 256 e 65535 máquinas) e reservam 14 bits para o *net id* e 16 bits para o *host id*. Finalmente, a classe C, apropriada para pequenas redes, aloca 21 bits para o *net id* e apenas 8 bits para o *host id*. Observe que os endereços IP são estruturados de forma a permitir uma rápida extração da identificação da rede (*net id*) e da máquina a ela conectada (*host id*). Os *gateways* dependem da extração eficiente do *net id* para realizar o roteamento dos pacotes IP.

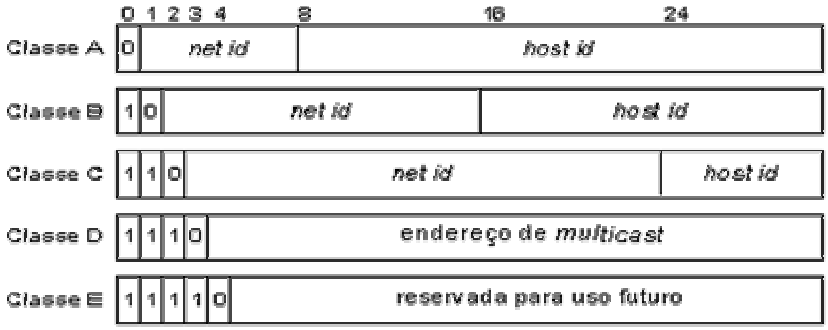

Figura 1

Ainda há pouco, dissemos que os endereços IP identificam um *host*. Essa afirmativa simplifica o tratamento do assunto mas não é estritamente correta. Considere um *gateway* que conecta duas redes. Como poderemos atribuir a essa máquina um único endereço IP, contendo uma identificação da rede e do *host*? Na verdade, não podemos. Máquinas como a deste exemplo, possuem não um, mas múltiplos endereços IP (dois, no caso). Cada um de seus endereços identifica uma conexão de rede. Numa definição mais precisa, portanto, endereços IP não definem *hosts*, mas conexões a uma rede. Máquinas conectadas a *n* redes, possuirão *n* endereços IP.

3 - Endereço de uma rede e Endereço de Difusão (*Broadcast*)

Já mencionamos a maior vantagem em codificar informação sobre a rede num endereço Internet: possibilitar um roteamento eficiente. Outra vantagem, é que os endereços IP podem se referir tanto a *hosts* quanto a redes. Por convenção, um *host id* 0 nunca é atribuído a uma máquina. Ao invés disso, esse endereço com os bits do *host id* todos zerados irá se referir à rede propriamente dita.

Outra vantagem do esquema de endereçamento da Internet é que ele permite que se faça referência a todos os *hosts* de uma determinada rede através do chamado endereço de difusão. Um endereço de *broadcast* é aquele em que os bits do *host id* são todos 1. Nem todas as redes suportam a difusão, algumas irão precisar de implementação de software e outras não permitirão esta facilidade nem mesmo a nível de software.

4 - Difusão local

O endereço de *broadcast* que acabamos de descrever é chamado de Endereço de Difusão Direcionada já que contém um *net id* válido (isto é, um endereço de uma rede existente) e um *host id* indicando *broadcast*. O endereço de difusão permite que um sistema remoto mande um pacote para todos os nós de uma determinada rede.

Do ponto de vista do endereçamento, a grande desvantagem deste esquema é que ele requer o conhecimento do endereço de rede. Outra forma de endereço de difusão de pacotes é chamada endereço de difusão limitada ou endereço de difusão local. Este endereço consiste de 32 bits iguais a 1. Esse mecanismo possibilita a referência a todas as máquinas de uma rede local sem que os endereços IP reais sejam conhecidos.

5 - Endereços de referência à própria rede e ao próprio *host*.
Já podemos perceber que campos de endereço preenchidos somente com 1's indicam "todos". Um endereço com 32 bits 1, indica **todas** as máquinas desta rede e um endereço com todos os bits do *host id* iguais a 1 indica **todas** as máquinas de uma determinada rede (especificada no *net id*). Analogamente, campos preenchidos com 0's são geralmente interpretados como significando "este". Assim, um endereço com 32 bits 0, indica o próprio *host* (**este** *host*) e um endereço com todos os bits do *net id* iguais a zero, se refere à rede local (**esta** rede).

6 - Endereço de *Multicast*
Muitas tecnologias de rede contêm mecanismos que permitem o envio simultâneo (ou quase simultâneo) de pacotes a múltiplos destinatários. Até agora, abordamos um destes mecanismos, conhecido com difusão. Na difusão é enviada uma cópia de um pacote para todos os nós de uma rede. Em redes de barramento (como a Ethernet) isso pode ser alcançado com o envio de um único pacote (capturado por todos os *hosts*). Em outras topologias, com conexões ponto-a-ponto, esse pacote deverá ser replicado para alcançar todos os *hosts*.
Algumas redes suportam um segundo tipo de comunicação ponto multi-ponto, conhecido com *multicast*. Ao contrário do *broadcast*, a técnica de *multicast* permite que cada *host* "escolha" se deseja ou não participar daquele "canal". Quando um grupo de máquinas decide se comunicar, elas selecionam um endereço de *multicast* que será, então, o seu canal de comunicação.
Na Internet, quando um determinado grupo de máquinas (que podem estar conectadas a redes distintas) deseja criar um grupo de *multicast*, elas devem todas "sintonizar", isto é, configurar suas interfaces para receber pacotes enviados para um mesmo endereço. Esse endereço deverá pertencer à Classe D. Assim, cada endereço entre 224.0.0.0 e 239.255.255.255 (mais de 268 milhões de alternativas!) pode ser usado por um determinado grupo de *multicast*.
A idéia é que *hosts* podem, a qualquer momento, conectar-se ou desconectar-se de um grupo de *multicast*. A técnica de *multicasting* traz, como vantagem sobre a difusão, uma melhor seletividade. Isto é, os dados só serão enviados aos *hosts* necessários. E mais, os *hosts* alcançados não precisam pertencer a uma mesma rede física. Entretanto, sua implementação é mais complexa pois necessita de *hardware* especializado.

7 - Fraquezas do Endereçamento IP
Um das desvantagens do esquema de endereçamento da Internet é que, como um endereço IP se refere a uma conexão de rede (e não a um *host*), quando uma máquina muda de uma rede para outra, ela deve mudar de endereço IP. Isso traz uma grande barreira à conexão de *hosts* móveis (como computadores portáteis) que precisem de IPs fixos à Internet.
Uma limitação menos importante está no fato de que redes classes C que crescam para além de 255 *hosts* devem ser realocadas para a classe B. O que implica uma mudança de todos os endereços.

A maior fraqueza, entretanto, surge quando analisamos cuidadosamente uma situação especial de roteamento de pacotes na Internet. Já dissemos que as decisões de roteamento (i.e. para que canal entre diversas possibilidades um pacote deve ser mandado) dependem da extração do *net id*. Considere uma máquina conectada a duas redes (Rede 1 e Rede 2). Como o roteamento de pacotes para este *host* será determinado pelo seu *net id* (e ele possui dois distintos), o caminho tomado por um pacote que se destina a essa máquina irá depender do endereço usado pelo remetente. Assim, parâmetros, como o tempo de resposta na comunicação, irão variar de acordo com a interface que seja endereçada. Essa multiplicidade de caminhos pode trazer consequências pouco óbvias. Um *host* pode deixar de ser acessível por um de seus endereços IP, caso haja algum impedimento físico em uma das redes a que ele está conectado. Uma outra máquina que conheça apenas esse endereço (desativado) e se comunique com este *host* através dele não poderá mais fazê-lo, embora o *host* ainda esteja ligado a Internet.

8 - Notação Decimal

Números de 32 bits não são facilmante manipuláveis por seres humanos, e mesmo os programas da camada de aplicação não tratam diretamente com este tipo de representação. Uma forma mais inteligível de representar endereços IP é a de particioná-lo em quatro octetos convertidos para a notação decimal e separados por pontos. Desta forma, o binário
11000000 11000110 00001011 10000001
passa a ser tratado como
192.198.11.129
Pode-se também atribuir nomes alfabéticos a *hosts*, facilitando ainda mais sua memorização. Esta tradução é apoiada por um protocolo específico que atua sobre uma imensa base de dados distribuída conhecida como *Domain Name System*. O DNS é um assunto de complexidade, que merece um curso exclusivamente dedicado a ele.

9 - Endereço de *Loopback*

O endereço 127.0.0.0 é reservado à aplicação de *loopback*. Isto é, qualquer pacote enviado a este endereço não deve trafegar na rede, mas retornar ao próprio remetente (isto equivale a dizer que o pacote retornará da própria interface de rede do *host*). O endereço de *loopback* se presta a testes e comunicação entre processos que rodam numa mesma máquina.

10 - Sumário dos Endereços Especiais

Já abordamos diversos endereços IP especiais, isto é, combinações que têm significados específicos. A **Figura 2** esquematiza essas diversas possibilidades.

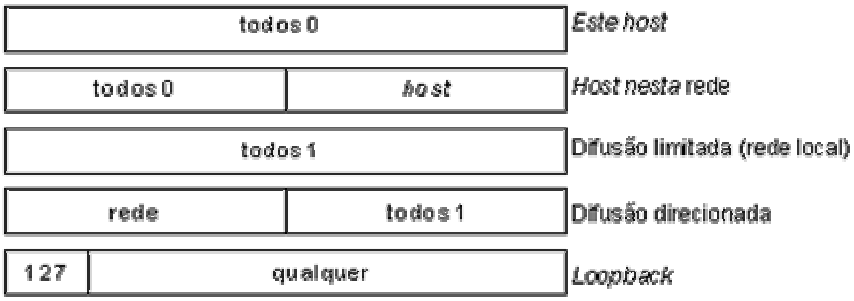

Figura 2

11 - Endereçamento de Sub-Rede

Uma técnica que permite que se partilhe um mesmo endereço de rede entre diversas redes é o endereçamento de sub-rede. Vamos imaginar uma instituição a qual foi atribuído um endereço classe C mas que possui diversas redes interconectadas em suas instalações. Como partilhar este endereço entre estas diversas redes?

A adição de sub-redes implica uma nova subdivisão do endereço IP. O sufixo designador do *host* (*host* id) é dividido em duas partes: a primeira designará uma sub-rede, e a segunda um *host* a ela conectado.

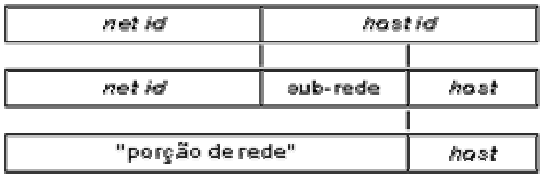

Figura 3

O problema básico que surge quando realizamos esta nova divisão é que o esquema convencional de roteamento, que procura extrair a porção que designa a rede, deixa de funcionar. Para suplantar esta dificuldade, introduz-se no sistema de roteamento uma nova entidade: a máscara de sub-rede.

A máscara de sub-rede é um número de 32 bits que, aplicado (através de um "e" lógico) a um determinado endereço, permite a extração de sua "porção de rede". Isto é, ele possui bits 1 nas posições correspondentes a esta "porção de rede". Para uma rede classe C sem sub-redes a máscara seria:

11111111 11111111 11111111 00000000

que em notação decimal corresponde a:

255.255.255.0

Qual seria a máscara de sub-rede usada para extrair a "porção de rede" num classe C partilhado entre quatro redes? Observe que, para podermos realizar a partilha, os dois bits mais significativos do último octeto irão ser usados para determinar a sub-rede. A máscara deverá então extrair os três primeiros octetos e estes dois bits adicionais. A máscara seria:

11111111 11111111 11111111 11000000

correspondente a:

255.255.255.192
Esse é o número que aplicado a um determinado endereço IP irá resultar na extração da porção deste endereço sobre a qual iremos "resolver" o roteamento.
A utilização de máscaras é tão importante na Internet, que qualquer administrador de redes, independente de utilizar ou não sub-redes, irá lidar com esse parâmetro quando configurar seus *gateways*

12 - Resumo

As redes TCP/IP utilizam números de 32 bits como seus identificadores universais.
Esses números são conhecidos como endereços IP ou endereços Internet.
Para facilitar sua memorização, os endereços IP são usualmente representados em notação decimal.
Os endereços IP, incluem uma identificação da rede e do *host* conectado a esta rede (net id e host id) - o que facilita a tarefa de roteamento.
Endereços IP são agrupados em cinco classes, que podem ser distinguidas pelos quatro bits de mais alta ordem.
O esquema de endereçamento da Internet permite três tipos de comunicação ponto multi-ponto: Difusão Direcionada, Difusão Local e Multcast
Através da técnica de aplicação de máscaras, um endereço de rede pode ser partilhado entre diversas sub-redes.
A principal fonte deste texto é o livro *Internetworking with TCP/IP* - COMER, Douglas - Prentice Hall International Editions

TCP/IP – Estudo 4

1- Introdução

TCP/IP (Transmission Control Protocol/Internet Protocol, ou Protocolo de Controle de Transmissão / Protocolo da Internet) se refere ao conjunto de protocolos utilizados na Internet. Ele inclui uma série de padrões que especificam como os computadores vão se comunicar e cria convenções para interconectar redes e para o routeamento através dessas conexões.

Os protocolos da Internet (IP) são o resultado de um projeto da DARPA (Defense Advanced Research Projects Agency, ou Agência de Projetos de Pesquisa Avançada de Defesa) sobre conectividade entre redes no final dos anos 70. Ele foi utilizado em todas as redes de longa distância do sistema de Defesa dos EUA em 1983, mas não foi amplamente aceito até ser incorporado ao BSD (Berkeley Software Distribution) Unix 4.2. A popularidade do TCP/IP é baseada em:

Estrutura cliente-servidor robusta. O TCP/IP é uma excelente plataforma cliente-servidor, especialmente em ambientes WAN (wide-area network, ou redes de grande alcance).

Compartilhamento de informações. Milhares de organizações miltiares, educacionais, científicas e comerciais compartilham dados, correio eletrônico (e-mail), e outros serviços na Internet usando o TCP/IP.

Ampla disponibilidade. Implementações do TCP/IP estão disponívies em praticamente todos os sistemas operacionais populares. Seu código fonte é amplamente disponível em várias implementações. Fabricantes de bridges, routers e analizadores de redes oferecem suporte para o TCP/IP em seus produtos.

Existem alguns conceitos básicos que são imprencindíveis ao entendimento do TCP/IP e de redes que o utilizam.

2 - Número de IP.

Existem algumas analogias entre computadores e telefones e o número de IP é uma delas. Você pode imaginar o número IP como um número de telefone com todos os códigos de discagem internacional. Isto significa que qualquer máquina pode contactar outra máquina usando o número de IP, bastando apenas que exista um caminho entre as 2 máquinas. Além disso toda máquina na rede tem de ter um nº de IP.

Isto também significa que 2 máquinas na mesma rede NÃO podem ter o mesmo número de IP. Essa restrição só ocorre para máquinas na mesma rede, pois máquinas numa rede não conectada usualmente tem número de IP iguais, por algumas razões técnicas. No caso da analogia com os telefones, imagine 2 pessoas morando em países diferentes que possuam o mesmo número de telefone (apenas os números locais). Nesse caso não há conflito (exceto talvez na sua mente! :-)).

O número de IP tem 4 bytes de tamanho e tem um formato específico, xxx.xxx.xxx.xxx (exemplo : 200.241.216.20). Isso significa que cada grupamento xxx só pode ir de 0 à 255 (pois essa é a capacidade de 1 byte).

3 - Máscara de Sub-Rede

Existem 3 classes de endereços IP : classes A, B, C. A diferença entre as classes é a forma de como o nº de IP é interpretado. O nº de IP é divido em duas partes : o

endereço da rede e o enderço da sub-rede. Considere o nº IP da seguinte forma : w.x.y.z (ex: 200.241.216.20)

Classe	Nº de IP	Indicador da rede	Indicador da Sub-rede	Nº de redes disponíveis	Nº de sub-redes disponíveis
A	1.126	w	x.y.z	126	16,777,214
B	128.191	w.x	y.z	16,384	65,534
C	192.223	w.x.y	z	2,097,151	254

Obs: O endereço 192.168 é reservado para uso em redes internas, o endereço 127 é utilizado para testes de loopback e os acima de 224 (inclusive) são reservados para protocolos especiais.
Uma sub-rede é uma rede ligada diretamente a Internet através de uma rede pertencente a Internet. A rede pertencente recebe um nº de IP, e distribui nº de IP dentro de sua sub-rede. As classes apenas definem quantas sub-redes um nº de IP tem. De acordo com a tabela, existem 126 nº de IP da classe A e cada um deles pode ter 16.777.214 sub-redes. Você logo pode imaginar que não existem endereços classe A para todo mundo, e tem razão, atualmente não existem endereços classe A e B disponíveis na Internet, e os de classe C estão acabando, o IETF (Internet Engenniering Task Force, ou Força Tarefa de Engenharia da Internet) está estudando a expansão desses números.
As máscaras de sub-rede identificam a classe do nº de IP. A primeira vista isso parece desnecessário, pois basta olhar o primeiro número do nº do IP para determinar sua classe. Mas acontece que um nº de IP classe A pode funcionar como um classe B ou classe C, dependendo da estrutura interna de sua sub-rede. Um exemplo : Imagine uma empresa com 200 filiais no Brasil conectadas por uma rede própria. A matriz tem um nº de IP classe A, digamos 100 e distribui suas sub-redes da seguinte forma :

100.1.0.0	Matriz
100.2.0.0	Filial 1
100.3.0.0	Filial 2
.....	
100.201.0.0	Filial 200

Para as filiais, o nº de IP (ex: 100.201.0.0) é de classe B, pois só tem 16.384 sub-redes disponíveis, embora comece com 100. Dentro das filiais ainda é possível se distribuir sub-redes, as quais teriam nº de IP classe C.
Para que o roteamento funcione corretamente, os computadores precisam saber qual a classe do nº de IP, e elas são as seguintes:

Classe	Máscara de Sub-rede
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

4 - Gateway padrão (default gateway)
O gateway padrão é a máquina para quem pedimos ajuda quando não conseguimos achar uma outra máquina na rede. Funciona assim: Quando uma máquina na rede precisa se comunicar com uma outra, ela emite um pedido de conexão (esse pedido é feito através de broadcasting, ou seja, a máquina envia um pedido a toda a rede, e apenas a máquina destino responde) e aguarda uma resposta. Se a resposta não vier, ela entra em contato com o gateway padrão e solicita que o mesmo conecte com a máquina destino. Se o gateway conseguir se conectar à máquina destino, ele fica como "intermediador" dessa conexão, caso contrário ele avisa a máquina solicitante que não foi possível encontrar a máquina destino.
Essa estrutura de procura visa diminuir o tráfego desnecessário na rede. Imagine só se toda a solicitação de conexão realizada na Internet (e em todas as redes conectadas à Intenet) fosse enviada para todos os computadores ligados à ela! Seria um tráfego muito grande. Ao invés disso, o broadcasting é feito em níveis, primeiro na LAN (local area network, ou rede local), depois na WAN de sua cidade ou estado, depois na WAN nacional até chegar na WAN internacional. Reduz-se desse modo todo o tráfego interno às WANs e LANs, aliviando as linhas de conexão.

5 - DNS
Essas 3 letras não significam muita coisa para a maior parte das pessoas, mas elas significam Domain Name System (ou Sistema de Nomes de Domínio). Essas 3 palavras também não significam muita coisa para a maior parte das pessoas também, por isso vamos à analogia com o telefone. Quando deseja telefonar para a loja da esquina, você consulta o catálogo, descobre o telefone de lá e liga. Você não consegue telefonar para lugar algum se não souber o número do telefone. Na rede TCP/IP acontece a mesma coisa. Os usuários não decoram o número IP das máquinas, e sim seus nomes. Mas para se alcançar uma máquina na rede, precisamos do seu número de IP. Para resolver isso, foi criado o DNS, um serviço diponível na rede que, dado um nome de máquina, ele retorna o número de IP da mesma.
Existe uma particularidade aqui. No caso da rede local estar conectada a alguma outra, é recomendável que o servidor DNS (o programa que oferece o serviço DNS) seja executado na máquina de ligação entre as 2 redes (o gateway), para que no caso do nome requisitado não existir na rede local, o DNS possa pedir ao servidor DNS da outra rede para pesquisar tal nome.
O Windows NT oferece um serviço semelhante, o WINS (Windows Internet Name System, ou Sistema de nomes da Internet do Windows). A principal diferença entre os dois é que o DNS usa uma tabela estática, e o WINS usa uma tabela dinâmica. No caso do servidor DNS rodar numa máquina Windows NT é recomendável que ele seja substituído pelo WINS.

6 - DHCP
Mais um caso de 4 letras que não significam nada para a maioria das pessoas. Mas infelizmente não existe uma boa analogia para o DHCP, portanto vamos direto ao assunto: DHCP significa Dynamic Host Configuration Protocol ou seja : Protocolo de Configuração de Host Dinâmico. Numa rede TCP/IP, todo computador tem de ter um

número de IP distinto. Isto significa que antes de colocar uma nova máquina na rede, o administrador teria de checar quais números estão sendo utilizados para poder escolher um nº adequado para a nova máquina. Em pequenas redes isso é possível de ser feito, mas em grandes redes isso se torna uma tarefa muito tediosa e sujeita a falhas. Para evitar isso, foi criado o DHCP. Quando uma máquina entra na rede, ela procura o servidor DHCP (cujo nº de IP foi previamente fornecido) e solicita um nº de IP para si própria. O servidor verifica qual o nº disponível, informa ao solicitante esse nº e o torna indisponível para futuras solicitações. Dessa maneira, a administração dos nº de IP é feita automaticamente e não existem problemas de conflito. Quando a máquina solicitante sai da rede, o servidor DHCP torna seu nº de IP disponível novamente.

7 - Portas

Uma porta pode ser vista como um canal de comunicações para uma máquina. Pacotes de informações chegando a uma máquina não são apenas endereçadas à maquina, e sim à máquina numa determinada porta. Você pode imaginar uma porta como sendo um canal de rádio, com a diferença fundamental de que um computador pode "ouvir" a todos os 65000 canais possíveis ao mesmo tempo!
Entretanto, um computador geralmente não está escutando a todas as portas, ele escuta umas poucas portas específicas. E ele não vai responder a um pedido que chegue numa porta a qual ele não esteja escutando.
Existem uma série de portas pré-definidas para certos serviços que são aceitos universalmente. As principais são :

Serviço	Porta	Descrição
FTP	21	File Transfer Protocol (Protocolo de Transferência de Arquivos)
Telnet	23	Para se conectar remotamente a um servidor
SMTP	25	Para enviar um e-mail
Gopher	70	Browser baseado em modo texto
HTTP	80	Protocolo WWW - Netscape, Mosaic
POP3	110	Para receber e-mail
NNTP	119	Newsgroups
IRC	6667	Internet Relay Chat - Bate papo on-line
Compuserve	4144	Compuserve WinCIM
AOL	5190	America Online
MSN	569	Microsoft Network

8 - Outros termos

8.1Roteador : É um computador especial que é utilizado para conectar 2 ou mais redes distintas. Ele tem esse nome porque tem de "rotear" (ou redirecionar) os pacotes de uma rede para outra, atuando como um "guarda de trânsito" para os pacotes entre as redes.

8.2 Gateway : O gateway é um computador que também é utilizado para conectar 2 ou mais redes distintas. A principal diferença para o roteador é que o gateway não

tem hardware especial para efetuar o roteamento. Usualmente os gateways conectam LANs e os roteadores, WANs. Em vários casos se utiliza um roteador em conjunto com um gateway.

9 - Visão geral de uma rede TCP/IP

Uma rede utilizando o TCP/IP tem uma estrutura básica composta por um (ou mais) servidor rodando um servidor DNS (ou WINS), DHCP, SMTP, POP3 e os servidores dos serviços desejados (HTTP, Gopher, Telnet e etc.) e as máquinas clientes solicitando esses serviços. Para se interligar essa rede a uma outra rede TCP/IP, se faz necessário o uso de um roteador ou gateway e da correta configuração da rede.
Existem 2 maneiras de se ligar a LAN à Internet :
Atribuindo-se um n.º de IP válido para cada máquina na rede, o que pode ser impossível para redes com muitas máquinas.
Atribuindo-se um n.º de IP válido para o gateway e utilizando-se o n.º de IP 192.168.x.x internamente.
Como o segundo caso é o mais factível, vamos observá-lo melhor. Nele, se utiliza internamente à LAN o IP 192.168.x.x, que quando da determinação do padrão dos n.º de IP foi reservado para uso em redes internas, ou seja, nenhuma máquina ligada diretamente à Internet tem um IP 192.168.x.x. Isso é necessário pois como já vimos nenhuma máquina pode ter um n.º de IP que já esteja sendo utilizado por uma outra máquina.
O gateway tem 2 interfaces de rede, uma para se conectar à Internet e outra para se conectar à LAN. À interface da Internet é atribuído o n.º de IP válido na Internet e na da LAN o n.º de IP do tipo 192.168.x.x (usualmente 192.168.0.1). Nas máquinas da LAN o n.º de IP é do tipo 192.168.x.x (aonde o 1º "x" é o mesmo do gateway) e o gateway default é o IP do gateway voltado para a LAN (192.168.x.x). Dessa forma podemos ter até 16.384 máquinas na internet por n.º de IP válido. Essa estrutura também facilita a adoção de medidas de segurança contra intrusos da Internet, pois como todo o tráfego Internet passa pelo gateway, basta protegê-lo para proteger toda a LAN.

TCP/IP – Estudo 5

Protocolos do TCP/IP

1 - TCP e IP

O TCP e o IP são apenas 2 membros da família TCP/IP. IP é um protocolo que providência a entrega de pacotes para todos os outros protocolos da família TCP/IP. O IP oferece um sistema de entrega de dados sem conexão. Isto é, os pacotes IP não são garantidos de chegarem ao seu destino, nem de serem recebidos na ordem em que foram enviados. O checksum do IP confirma apenas a integridade do cabeçalho do pacote. Desta maneira, a responsabilidade pelos dados contidos no pacote do IP (e sua seqüência) é tarefa de protocolos de mais alto-nível.
Talvez o protocolo de alto nível do IP mais comum seja o TCP. O TCP oferece um confiável protocolo baseado em conexão encapsulado no IP. O TCP garante a entrega dos pacotes, assegura o sequenciamento dos pacotes, e providencia um checksum que valida tanto o cabeçalho quanto os dados do pacote. No caso da rede perder ou corromper um pacote TCP/IP durante a transmissão, é tarefa do TCP retransmitir o pacote faltoso ou incorreto. Essa confiabilidade torna o TCP/IP o protocolo escolhido para transmissões baseadas em sessão, aplicativos cliente-servidor e serviços críticos como correio eletrônico.
Porém essa confiabilidade tem um preço. Os cabeçalhos dos pacotes TCP requerem o uso de bits adicionais para assegurar o correto sequenciamento da informação, bem como um checksum obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantir a entrega dos pacotes, o protocolo também requer que o destinatário informe o recebimento do pacote.
Tal "informação de recebimento" (ou ACKs, de acknowledgments) geram tráfego adicional na rede, diminuindo a taxa de transferência de dados em favor da confiabilidade. Para reduzir o impacto na performance, a maioria dos servidores enviam um ACK para todo segmento de dados (ao invés de todo pacote) ou quando um ACK expira.

2 - UDP

Se a confiabilidade não é essencial, o UDP (User Datagram Protocol), um complemento do TCP, oferece um serviço de transmissão de dados sem conexão que não garante nem a entrega nem a correta seqüência dos pacotes enviados (bem parecido com o IP). Checksums no UDP são opcionais, oferecendo assim uma maneira de se trocar dados em uma rede altamente confiável sem consumir desnecessariamente recursos da rede.

3 - ARP e ICMP

Dois outros protocolos na família TCP/IP tem importantes funções, embora essas funções não estejam diretamente relacionadas com a transmissão de dados: ARP (Address Resolution Protocol, ou Protocolo de Resolução de endereços) e ICMP (Internet Control Message Protocol, ou Protocolo de Controle de Mensagens da Internet). O ARP e o ICMP são protocolos de manutenção que mantêm a estrutura do IP e usualmente são invisíveis aos usuários e às aplicações.
Os cabeçalhos do IP contém tanto o endereço IP da origem quanto do destino, mas o endereço do hardware também tem de ser conhecido. O IP obtém um endereço de

hardware de um determinado sistema difundindo pela rede um pacote especial de requisição (um pacote ARP de requisição) contendo o endereço IP do sistema com o qual está tentando se comunicar. Todos os nós da rede local que tiverem o ARP habilitado detectam essa difusão, e o sistema que tem o número de IP em questão envia um pacote (do tipo ARP reply, ou resposta ARP) contendo seu endereço de hardware para o computador que o solicitou. O endereço de hardware e o endereço IP do computador estão é armazenado no cache do ARP para uso futuro. Como a resposta ARP também é feita na forma de difusão, é normal que outros nós usem essa informação para atualizar seus caches ARP.
O ICMP permite que 2 nós em uma rede IP compartilhem o status do IP (protocolo) e informação de erros. Esta informação pode ser usada por protocolos de alto nível para tratar problemas de transmissão ou para administradores de rede para detectar problemas na rede. Embora estejam encapsulados em pacotes IP, o ICMP não é considerado um protocolo de alto nível (ele é necessário em toda implementação do TCP/IP). O utilitário ping faz uso do ICMP para determinar se um certo endereço IP na rede está operacional. Isto é útil para diagnosticar problemas em redes IP ou falhas em gateways.

4 - Outros Protocolos
Além desses protocolos citados, existem os protocolos de alto-nível, como o Telnet, FTP, HTTP e etc. Vamos a uma breve descrição deles :

4.1 - Telnet : É um protocolo que permite o logon em máquinas remotas. Você passa a utilizar a máquina remota para realizar o processamento. No Windows NT existe o RAS (Remote Access Service, Serviço de Acesso Remoto) que tem os mesmos objetivos do Telnet.

4.2 - FTP : File Transfer Protocol (protocolo de transferência de arquivos), como o nome já diz é utilizado para a transferência de arquivos.

4.3 -HTTP: Hyper Text Transfer Protocol : É o protocolo utilizado pela Web, ele transmite textos, gráficos e qualquer outro tipo de arquivo (substituindo o FTP) além de permitir a navegação através de hiper texto.

TCP/IP – Estudo 6

Arquitetura TCP/IP: Overview.

1 - Introdução
TCP/IP é um conjunto de protocolos de comunicação que define como computadores de diferentes tipos devem *"falar"* entre si. O principal objetivo da arquitetura TCP/IP é fazer a interconecção de Redes Locais e *"Wide Area Networks".* Cada rede física tem sua própria tecnologia e o TCP/IP faz o papel da "cola" entre as redes. Assim, podemos ter um *host* numa rede Token-Ring e, através de *Gateways* fazê-lo comunicar-se com um servidor numa rede Ethernet, por exemplo.
Mas quais são as vantagens de ter um computador numa Rede TCP/IP? Inúmeras!
2 - Transmissões e trocas de Dados: Permite que grandes quantidades de Dados/Informações sejam facilmente trocados com uma boa margem de segurança e confiabilidade.
3 - Telnet(Network Terminal Protocol): Aplicação que permite o *Login* remoto a um servidor através da Rede.
4 - e-mail: Permite uma comunicação simples, eficiente e instantânea através de correio eletrônico.
Porém atualmente existem alguns riscos quanto a conectar-se à uma Rede TCP/IP. Por isso deve-se tomar alguns cuidados(Permissões, FireWall, Criptografia,etc) quanto a segurança dos dados do usuário para que não seja possível que um *"visitante"* se logue em sua máquina(ou rede) e ocasione prejuízos para você!

5 - Características.
Esta arquitetura se refere a um conjunto de protocolos de comunicação de dados onde os mais importantes são o TCP e o IP.A necessidade de uma Comunicação de Dados *"World Wide"* e muitas características importantes auxiliaram o grande avanço do TCP/IP onde podemos destacar:
**Open Protocol Standard:* Protocolos facilmente avaliáveis e desenvolvidos independentemente. Isto torna o TCP/IP ideal para unir diferentes Hardwares e Softwares, mesmo que você não esteja conectado à Internet(como por exemplo a *Intranet Bamerindus*).
**Independência de um Hardware de Rede específico:* Isto permite o TCP/IP integrar diversos tipos de redes; ou seja, TCP/IP pode ser rodado sob Ethernet, Token-Ring, linha dial-up, X25,etc..
**Um esquema comum de endereçamento* que permite que qualquer dispositivo TCP/IP um único endereço IP em toda a Internet ou Rede TCP/IP.
**Protocolos padronizados* de alto nível, serviços de usuários amplamente avaliáveis para usuários.

6 - Modelo de Comunicação de Dados:
Um modelo arquitetural desenvolvido pela *International Standards Organization(ISO)* é frequentemente usado para descrever as estruturas e as funções dos protocolos de comunicação. Este modelo é chamado de *Open Systems Interconnect(OSI) Reference Model*. O modelo *OSI* contém 7 camadas. Cada camada representa uma função executada quando os dados são transmitidos entre as aplicações.

Uma camada não define um protocolo e sim a função de comunicação que devem ser executados por um ou mais protocolos. Assim, cada camada contém vários protocolos. Analogamente, nós podemos considerar a arquitetura TCP/IP como um modelo baseado em camadas.

Principais Protocolos de cada Camada.

6.1 - Application Layer:

Protocolo SMTP(Simple Mail Transfer Protocol) RFC 821
FTP(Network Terminal Protocol) RFC 959
RIP(Routing Information Protocol) RFC 1058
DNS(Domain Name service) RFC 1035

6.2 - Transport Layer:

Protocolo TCP(Transmission Control Protocol) RFC 793
Protocolo UDP(User Datagram Protocol) RFC 768

6.3 - Internet Layer:

Protocolo IP(Internet Protocol) RFC791
Protocolo ICMP (Internet Control Message Protocol) RFC 792

6.4 - Network Access Layer:

ARP(Address Resolution Protocol) RFC826

7 - Endereçamento,Subnet e Roteamento.

7.1 - Endereçamento: O Protocolo *IP* transporta dados em forma de datagramas. No "cabeçalho" (header) do Datagrama contém o *Endereço de Destino* que é um endereço padrão de 32 bits capaz de identificar uma única Rede e um Host específico naquela Rede TCP/IP. A partir do endereço IP podemos identificar a *Classe de Endereçamento* onde as principais são: *Classe A, Classe B e Classe C.*

7.2 - Classe A: O 1º byte é menor que 128. Os outros 3 bytes são o endereço do Host.
Ex.: No caso do endereço IP ***26.104.0.15*** temos:
Endereço de Rede ***26***
Endereço de Host ***104.0.15***

7.3 - Classe B:de 128 até 191:
Os dois primeiros bytes identificam a Rede e os dois últimos identificam o Host.
Ex.: O Endereço IP ***128.66.12.32***
Endereço de Rede ***128.66***
Endereço de Host ***12.32***

7.4 - Classe C:de 192 até 223:
Os três primeiros bytes identificam a Rede e último identifica o Host.
Ex.: O Endereço IP ***192.178.16.12***
Endereço de Rede ***192.178.16***
Endereço de Host ***12***

7.5 - Subnets e Máscaras

A *Máscara (Subnet Mask)* é um recurso afim de organizar topologica e organizacionalmente uma rede. A partir de um único endereço IP podemos obter várias "sub-redes" cada uma com vários Hosts. Para isso é necessário "aplicarmos" uma máscara apropriada.*Em breve colocarei o método para aplicar a mascara. Se você tem dúvidas de como aplicá-la, mande me um e-mail*
Exemplo:

Endereço IP	Máscara Subnet	Interpretação
40.0.90.23	255.255.255.0	Host 23 na Subnet 40.0.90
40.0.98.4	255.255.0.0	Host 98.4 na Subnet 40.0
40.0.132.70	255.255.255.192	Host 6 na Subnet 40.0.132.64
40.0.50.12	FF.FF.FC.80(hexa)	Host 2.12 na Subnet 40.0.48.0
40.0.50.76	FF.FF.FC.80(hexa)	Host 2.76 na Subnet 40.0.48.0
40.0.50.204	FF.FF.FC.80(hexa)	Host 2.76 na Subnet 40.0.48.128

7.6 - Roteamento

O roteamento é o processo pela qual os dados passam para ir de um Host ao outro. Para isso, é necessário que os *Gateways* conheçam ou saibam como e para onde mandar o pacote de dados. Os roteadores, servidores e até mesmo PC´s são capazes de rotear dados.

Bibliografia

Fontes retiradas da Internet e Livros:

Estudo 1

Internet: *Origem desconhecida*

Estudo 2

Internet: *Origem desconhecida*

Estudo 3

A pricipal fonte deste estudo é o livro *Internetworking with TCP/IP – by Douglas Comer – Prentice Hall International Editions*

Estudo 4

Vitória (ES), 17/10/97, por: Fabricio B. Dias, adaptado por: {[CrAsHrOoT]}

Estudo 5

Vitória (ES), 17/10/97, por: Fabricio B. Dias

Estudo 6

Vitória (ES), 17/10/97, por: Fabricio B. Dias