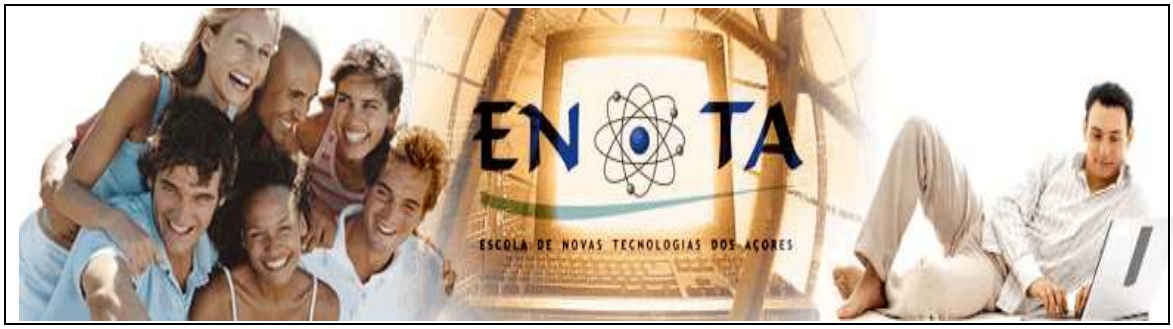
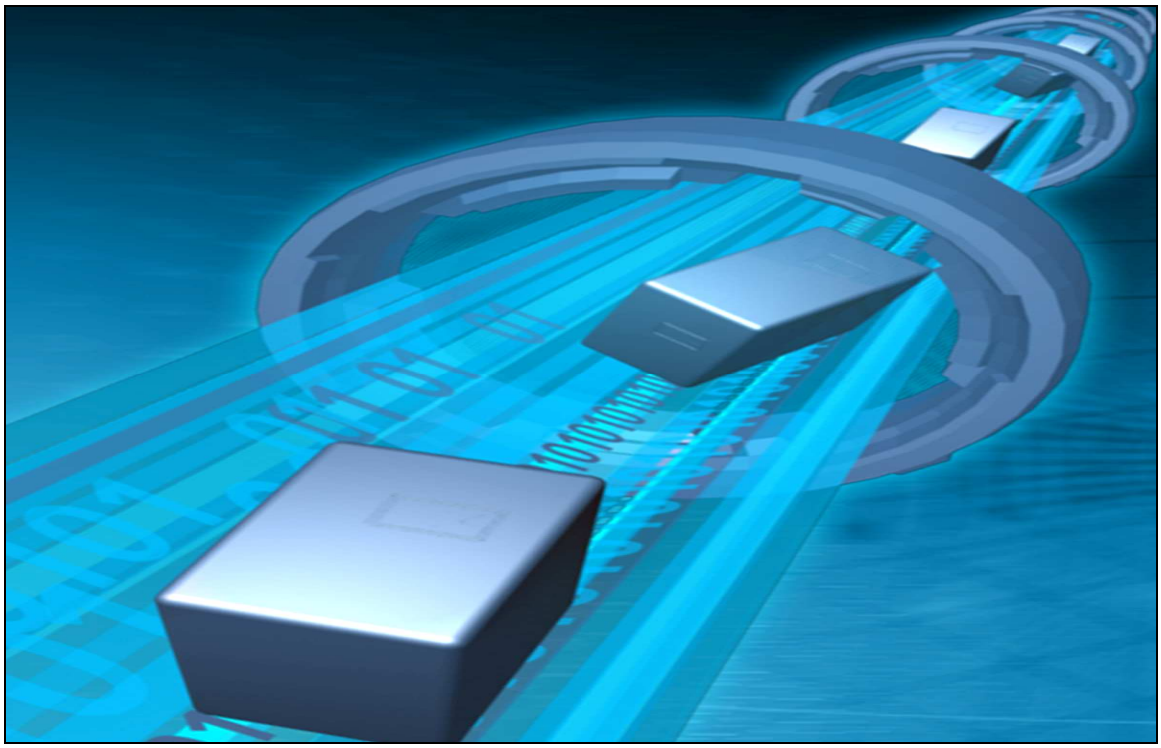


ETHERNET & UDP & ICMP



Técnico de Instalação e Gestão de Redes Informáticas

Segunda-feira, 5 de Maio de 2008

Trabalho elaborado por:
Norberto Vargas
Bruno Fortuna

Índice

Ethernet

A necessidade de diminuir custos, aumentar a confiabilidade, disponibilizar o compartilhamento de recursos físicos (HD, impressoras,...) e informações (banco de dados, programas,...) fez surgir as redes de computadores. Estas características fazem com que estas redes não parem de evoluir.

O padrão ethernet surgiu em 1972 nos laboratórios da Xerox com Robert Metcalfe.

Com uma rede onde todas as estações compartilhavam do mesmo meio de transmissão, um cabo coaxial; a configuração utilizada para esta conexão foi a de barramento, utilizava uma taxa de transmissão de 2,94 Mbps.

No início este padrão era chamado de “Network Alto Aloha”, depois foi modificado para “ethernet” para deixar claro que este padrão pode suportar qualquer computador e para mostrar que pode ser desenvolvido fora de seus laboratórios.

Metcalfe optou pela palavra “ether” de maneira a descrever uma característica imprescindível do sistema: o meio físico transporta os bits para todas as estações, como se acreditava que acontecia com o éter, o meio que preenchia o universo e o espaço entre os corpos celestes que propagava as ondas electromagnéticas pelo espaço.

A falta de padronização dificultava o progresso das pesquisas e a venda de equipamentos, com o intuito de resolver este problema foi homologado ao IEEE – Institute of Electrical and Electronic Engineers, em 1980, a responsabilidade de criar e administrar a padronização da ethernet. Desde a sua regulamentação pelo IEEE as suas especificações foram totalmente disponibilizadas. Esta abertura combinada com a facilidade na utilização e com a sua robustez resultou no largo emprego desta tecnologia.

Modo de transmissão

- ***Simplex***: durante todo o tempo apenas uma estação transmite, a transmissão é feita unilateralmente;
- ***Half-duplex***: cada estação transmite ou recebe informações, não acontecendo transmissão simultânea;
- ***Full-duplex***: cada estação transmite e/ou recebe, podendo ocorrer transmissões simultâneas.

CSMA/CD

Do inglês (Carrier Sense Multiple Access with Collision Detection*),* é um protocolo de telecomunicações que organiza a forma como os computadores compartilham o canal.

- *CS (*Carrier Sense): Capacidade de identificar se está ocorrendo transmissão;
- *MA (*Multiple Access): Capacidade de múltiplos nós concorrerem pela utilização da mídia;
- CD (Collision Detection**):** É responsável por identificar colisões na rede;

Funcionamento:

O CSMA identifica quando a mídia está disponível (idle time) para a transmissão. Neste momento a transmissão é iniciada. O mecanismo CD (Collision Detection ou em português detecção de colisão) ao mesmo tempo obriga que os nós escutem a rede enquanto emitem dados, razão pela qual o CSMA/CD é também conhecido por “Listen While Talk“ (traduzido como "escute enquanto conversa").

Se o mesmo detecta uma colisão, toda transmissão é interrompida e é emitido um sinal (“jam” de 48 bits) para anunciar que ocorreu uma colisão. Para evitar colisões sucessivas o nó espera um período aleatório e volta a tentar transmitir.

Esquema de funcionamento:

1. Se o canal está livre, inicia-se a transmissão, senão vai para o passo 4;
2. (transmissão da informação) se a colisão é detectada, a transmissão continua até que o tempo mínimo para o pacote seja alcançado (para garantir que todos os outros transmissores e receptores detectem a colisão), então segue para o passo 4;
3. (fim de transmissão com sucesso) informa sucesso para as camadas de rede superiores, sai do modo de transmissão;
4. (canal está ocupado) espera até que o canal esteja livre;
5. (canal se torna livre) espera-se um tempo aleatório, e vai para o passo 1, a menos que o número máximo de tentativa de transmissão tenha sido excedido;
6. (número máximo de tentativa de transmissão excedido) informa falha para as camadas de rede superiores, sai do modo de transmissão;

Variedades de Ethernet

10 Mbit/s Ethernet:

- 10BASE2 (também chamado ThinNet ou Cheapernet) – Um cabo coaxial de 50-ohm conecta as máquinas, cada qual usando um adaptador T para conectar seu NIC. Requer terminadores nos finais. Por muitos anos esse foi o padrão dominante de ethernet de 10 Mbit/s.
- 10BASE5 (também chamado Thicknet) – Especificação Ethernet de banda básica de 10 Mbps, que usa o padrão (grosso) de cabo coaxial de banda de base de 50 ohms. Faz parte da especificação de camada física de banda de base IEEE 802.3, tem um limite de distância de 500 metros por segmento.
- StarLAN 10 – Primeira implementação de Ethernet em cabeamento de par trançado a 10 Mbit/s. Mais tarde evoluiu para o 10BASE-T.
- 10BASE-T – Opera com 4 fios (dois conjuntos de par trançado) num cabo de cat-3 ou cat-5. Um hub ou switch fica no meio e tem uma porta para cada nó da rede. Essa é também a configuração usada para a ethernet 100BASE-T e a Gigabit.
- FOIRL – Link de fibra óptica entre repetidores. O padrão original para ethernet sobre fibra.
- 10BASE-F – Um termo genérico para a nova família de padrões de ethernet de 10 Mbit/s: 10BASE-FL, 10BASE-FB e 10BASE-FP. Desses, só o 10BASE-FL está em uso comum (todos utilizando a fibra óptica como meio físico).
- 10BASE-FL – Uma versão actualizada do padrão FOIRL.
- 10BASE-FB – Pretendia ser usada por backbones conectando um grande número de hubs ou switches, agora está obsoleta.

Fast Ethernet:

- 100BASE-T – Designação para qualquer dos três padrões para 100 Mbit/s ethernet sobre cabo de par trançado. Inclui 100BASE-TX, 100BASE-T4 e 100BASE-T2.
- 100BASE-TX – Usa dois pares, mas requer cabo cat-5. Configuração "star-shaped" idêntica ao 10BASE-T. 100Mbit/s.
- 100BASE-T4 – 100 Mbit/s ethernet sobre cabeamento cat-3 (Usada em instalações 10BASE-T). Utiliza todos os quatro pares no cabo. Actualmente obsoleto, cabeamento cat-5 é o padrão. Limitado a Half-Duplex.
- 100BASE-T2 – Não existem produtos. 100 Mbit/s ethernet sobre cabeamento cat-3. Suporta full-duplex, e usa apenas dois pares. O seu funcionamento é equivalente ao 100BASE-TX, mas suporta cabeamento antigo.
- 100BASE-FX – 100 Mbit/s ethernet sobre fibra óptica. Usando fibra óptica multimodo 62,5 mícrons tem o limite de 400 metros.

Gigabit Ethernet:

- 1000BASE-T – 1 Gbit/s sobre cabeamento de cobre categoria 5e ou 6.
- 1000BASE-SX – 1 Gbit/s sobre fibra.
- 1000BASE-LX – 1 Gbit/s sobre fibra. Optimizado para distâncias maiores com fibra mono-modo.
- 1000BASE-CX – Uma solução para transportes curtos (até 25m) para rodar ethernet de 1 Gbit/s num cabeamento especial de cobre. Antecede o 1000BASE-T, e agora é obsoleto.

UDP

O protocolo UDP (User Datagram Protocol) fornece um serviço sem conexão não confiável, usando IP (Internet Protocol) para transportar mensagens entre duas máquinas.

O protocolo UDP é normalmente utilizado por aplicações que exigem um transporte rápido e contínuo de dados entre equipamentos. Enquanto no protocolo TCP é dado prioridade à conexão e a chegada correcta dos dados no ponto de destino, o UDP não verifica o recebimento e a integridade dos dados enviados.

Por consequência, existe a possibilidade de que, eventualmente, as informações transmitidas sejam recebidas de forma incorrecta ou mesmo não cheguem ao destinatário. Entretanto, a maior simplicidade do UDP faz com que este protocolo apresente ganhos na velocidade de transmissão e recepção de dados, algo que nos dias actuais se torna cada vez mais importante.

Funcionamento

O UDP dá às aplicações acesso directo ao serviço de entrega de datagramas, como o serviço de entrega que o IP dá. O UDP é pouco confiável, sendo um protocolo não orientado para conexão. O "pouco confiável" significa que não há técnicas no protocolo para confirmar que os dados chegaram ao destino correctamente. O UDP usa número de porta de origem e de destino de 16 bits na Word 1 do cabeçalho da mensagem.

O UDP é um acrónimo do termo inglês *User Datagram Protocol* que significa protocolo de datagramas de utilizador (ou usuário). O UDP faz a entrega de mensagens independentes, designadas por datagramas, entre aplicações ou processos, em sistemas host. A entrega pode ser entregue fora de ordem ou até em dados perdidos. A integridade dos dados pode ser gerida por um "checksum" (um campo no cabeçalho de checagem por soma).

Os pontos de acesso do UDP são geralmente designados por "Portas de protocolo" ou "portas" ou até "portos", em que cada unidade de transmissão de dados UDP identifica o endereço IP e o número de porta do destino da fonte da mensagem.

O UDP é o protocolo irmão do TCP. A diferença básica entre os dois é que o TCP é um protocolo orientado à conexão, que inclui vários mecanismos para iniciar e encerrar a conexão, negociar tamanhos de pacotes e permitir a retransmissão de pacotes corrompidos. No TCP tudo isso é feito com muito cuidado, para garantir que os dados realmente cheguem inalterados, apesar de todos os problemas que possam existir na conexão. O lema é "transmitir com segurança"

O UDP por sua vez é uma espécie de irmão adolescente do TCP, feito para transmitir dados pouco sensíveis, como streaming de áudio e vídeo. No UDP não existem verificações, nem confirmações algumas. Os dados são transmitidos apenas uma vez, incluindo apenas um frágil sistema de CRC (do inglês *Cyclic redundancy check*, ou verificação de redundância cíclica é um código detector de erros). Os pacotes que cheguem corrompidos são simplesmente rejeitados, sem que o emissor sequer saiba do problema.

A ideia é precisamente transmitir dados com o maior desempenho possível, eliminando dos pacotes quase tudo que não seja dados em si.

Em geral, os programas que utilizam portas UDP recorrem também a uma porta TCP para enviar as requisições de dados a serem enviados e também para verificar periodicamente se o cliente ainda está on-line.

Podemos concluir que o UDP é um protocolo de transporte que presta um serviço de comunicação não orientado a conexão e sem garantia de entrega. Portanto, as aplicações que utilizam este tipo de protocolo devem ser as responsáveis pela recuperação dos dados perdidos.

Cabeçalho UDP

O cabeçalho UDP é extremamente simples, contendo apenas os números de porta, comprimento da mensagem e o checksum. O cabeçalho dos datagramas UDP é colocado a seguir ao cabeçalho IP.

Porta origem	Porta destino
Comprimento da mensagem	Checksum

Selecção do número de portas no UDP

Os computadores que pretendem estabelecer uma comunicação devem definir um número de porta. Para o servidor (Processo), e aguardar pela chegada de mensagens, datagramas, o cliente selecciona uma porta local, para recebimento de datagramas e envia datagramas para a porta seleccionada para o processo do servidor. Muitos serviços conhecidos usam números de portas reservados, por exemplo: 161 para o Protocolo SNMP.

Vantagens do uso do UDP

Velocidade de processamento. Neste caso, o UDP é a escolha acertada como protocolo da camada de transporte. Aplicações que encaixam num modelo de pergunta – resposta também são fortes candidatas a usar UDP. A resposta pode ser usada como reconhecimento positivo para a pergunta. Se uma resposta não chega num período de tempo estipulado, a aplicação envia outra pergunta.

Os protocolos UDP e TCP no modelo TCP/IP

Os protocolos de transporte utilizam o IP para suportar a entrega de dados para os protocolos de aplicação

Aplicação
Transporte UDP, TCP
Internet
Interface de rede
Físico

O ICMP

(Internet Control Message Protocol***)*** é um protocolo integrante do Protocolo IP, é utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa de aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem data gramas que provoquem algum erro.

ICMP possibilita a comunicação entre o software IP numa máquina com o software IP de outra máquina, qualquer problema no caminho será sempre informado à origem, embora o mau funcionamento possa estar no núcleo da rede.

O ICMP é projectado para o envio de mensagens de controlo e ensaio em todas as redes IP.

Ao contrário da camada de transporte protocolos TCP (Transmission Control Protocol) e UDP (User datagrama Protocol) que funcionam em cima de IP, ICMP existe paralelamente ao IP.

A capacidade de compreender ICMP é um requisito para qualquer dispositivo de rede IP-compatível. No entanto, muitos dispositivos de segurança como firewalls bloqueiam ou desactivam todas ou parte das funcionalidades ICMP para fins de segurança.

Ferramentas que utilizam ICMP

Duas das ferramentas que utilizam o ICMP são o ping e o traceroute.

O ping envia pacotes ICMP para verificar se um determinado host está disponível na rede. O traceroute faz uso do envio de diversos pacotes UDP ou ICMP e, através de um pequeno truque, determina a rota seguida para alcançar um host.

Ping

Quando queremos determinar se um determinado host está disponível na rede interna ou mesmo na Internet, frequentemente é utilizado o ping como um dos primeiros recursos de troubleshooting. O facto de um host não responder ao ping não quer dizer que ele esteja realmente fora da rede, pois este serviço pode estar desabilitado neste host por questões de segurança.

É chamado de cliente o host que inicia a comunicação, ou seja, a partir do qual o utilizador executa o comando de teste de disponibilidade. Servidor é o alvo do teste, pois este deve possuir um serviço habilitado para ser capaz de receber o pacote do cliente e respondê-lo.

O cliente envia primeiro um pacote do tipo ICMP Echo Request, ou simplesmente ICMP Echo.

Traceroute

Um dos campos do cabeçalho IP é chamado TTL – Time to Live – e determina por quantas passagens em routers este pacote pode sobreviver. A cada passagem em um router ou host este campo é chamado de campo 1. Este mecanismo é utilizado para evitar que pacotes percorram a rede eternamente, rodando de um lado para outro. Se um pacote possui um TTL de 1 e este deve passar por um router antes de alcançar o seu destino final, este router irá descartá-lo ao verificar o TTL do pacote e retornar um pacote ICMP do tipo ICMP Time Exceeded para o host que o enviou. Neste pacote de resposta o router identifica-se como origem da mensagem Time Exceeded. É nessa característica do protocolo que o utilizador traceroute baseia-se para traçar uma rota entre dois pontos da rede.

Supondo que o host 1 esteja separado do host 2 por dois routers, chamados router A e router B. A partir do host 1 é executado um traceroute para o host 2. O utilizador cria um pacote UDP destinado ao host 2, mas configura o seu TTL para 1. O router A recebe este pacote e, apesar de saber para onde mandar o pacote, ao processar o TTL este torna-se 0 (zero) o que significa que este pacote deve ser descartado, retornando um ICMP Time Exceeded para o host 1. Quando o traceroute recebe esta resposta ele tem o endereço do primeiro router no caminho entre os dois hosts. O primeiro router é apresentado a o utilizador.

Em seguida, o traceroute cria outro pacote UDP, com o TTL de 2. O pacote sobrevive ao primeiro router mas é processado no segundo. Quando recebe o ICMP Time Exceeded do segundo roteador temos o endereço dele, que também é mostrado na saída do traceroute. O passo seguinte é um pacote com TTL de 3 o qual alcança o host 2. Os pacotes UDP são sempre enviados com uma porta de destino inválida, o que força que o host 2, ao receber o pacote, retorne um pacote ICMP Destination Unreachable. O traceroute sabe então que o caminho completo foi descoberto e mostra ao usuário o endereço do host 2, indicando que o trace foi finalizado.

Tipos de mensagens ICMP

- ✓ Echo Responder, tipo 0;
- ✓ Destino inacessível, tipo 3;
- ✓ Fonte Têmpera, tipo 4;
- ✓ Redirecionar, tipo 5;
- ✓ Alternate acolhimento endereço, tipo 6;
- ✓ Echo, tipo 8;
- ✓ Router Advertisement, tipo 9;
- ✓ Router Modalidade, tipo 10;
- ✓ Tempo excedido, tipo 11;
- ✓ Parâmetro Problema, tipo 12;
- ✓ Timestamp, tipo 13;
- ✓ Responder timestamp, tipo 14;
- ✓ Informações Pedido, tipo 15;
- ✓ Informações Responder, tipo 16;
- ✓ Endereço máscara pedido, tipo 17;
- ✓ Endereço máscara Responder, tipo 18;
- ✓ Traceroute, tipo 19.