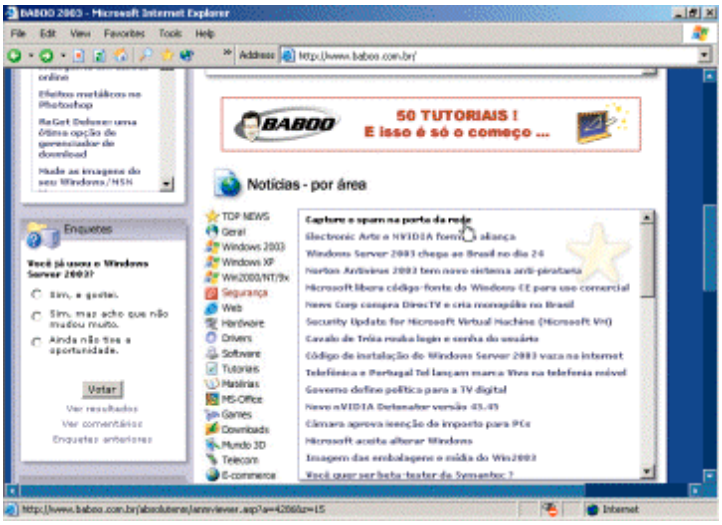
Tudo sobre TCP/IP

TCP/IP

O conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de Controle de Transmissão/Protocolo da Internet) está presente em quase na totalidade dos sistemas operacionais de rede disponíveis atualmente. É um protocolo flexível, recomendável tanto para redes pequenas quanto para redes gigantescas como a Internet, e compatível com uma enormidade de hardwares diferentes. Neste tutorial, discutiremos o funcionamento básico do TCP/IP incluindo uma descrição dos protocolos que o formam e explicação sobre como utilizar suas principais ferramentas.

As Origens

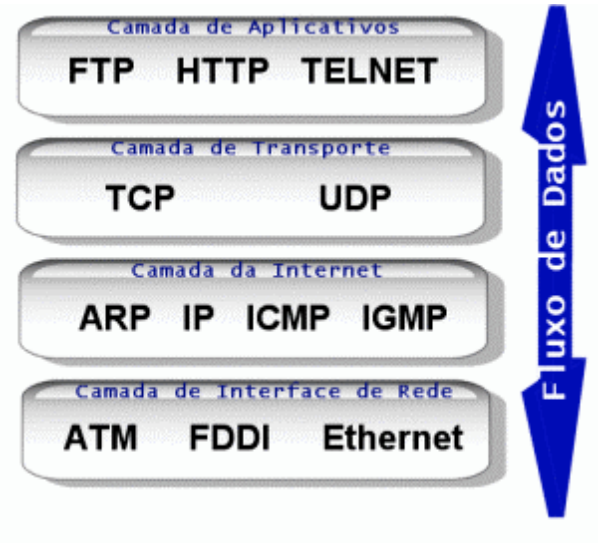
O TCP/IP foi primariamente desenvolvido nos anos 60 por uma agência do Departamento de Defesa Americano (DOD): a DARPA (Defense Advanced Research Projects Agency). Ele foi projetado para permitir que diferentes tipos de sistemas de computador se comunicassem como se fossem um sistema só em uma época que as arquiteturas variavam muito e eram guardadas a sete chaves. Vários fatores levaram à popularidade do TCP/IP e ele acabou sendo incorporado ao Unix da universidade de Berkeley no início da década de 80, tornando-se em seguida um padrão nas grandes universidades. Além disso, todas as propostas do governo dos Estados Unidos que incluíam redes na época incluiam também o TCP/IP. A criação de uma interface amigável para o usuário utilizar-se dos recursos do conjunto de protocolos (o navegador Web) permitiu que o usuário comum pudesse aproveitar-se das vantagens do protocolo.



Uma interface amigável ao usuário sempre ajudou programas de computador a deslancharem no mercado, incluindo o Windows e o conjunto de protocolos TCP/IP.

Arquitetura do TCP/IP

Os diversos tipos de protocolo disponíveis no TCP/IP trabalham em conjunto para que a comunicação possa ser efetuada. São organizados em um modelo de 4 camadas, como ilustrado abaixo.



Quando as informações são enviadas elas passam por todas essas camadas. Por exemplo, quando você transfere um arquivo para um servidor FTP (File Transfer Protocol, será explicado mais adiante), os dados e mais um cabeçalho contendo informações de controle do FTP serão enviados ao TCP: este adiciona suas informações de controle também e repassa os dados ao IP. Este por sua vez adiciona seu próprio cabeçalho e repassa o bloco de informações (incluindo todos os cabeçalhos) para o Ethernet, que então codifica os dados em uma forma que possa trafegar no cabo da rede. Ufa! Assim também ocorre quando o servidor FTP envia dados para o seu computador, só que no sentido inverso. Você entenderá melhor esse processo ao longo do tutorial.

Camada de Interface de Rede

Esta camada controla como os dados são formatados ou interpretados quando chegam diretamente do fio à sua placa de rede. Ela dita ao dispositivo de rede como enviar e receber os dados binários. Contém protocolos de Redes Locais (Local Area Networks) como Token Ring, FDDI (Fiber Distributed Data Interface - Interface de Dados Distribuídos na Fibra) e Ethernet (a mais utilizada em redes locais) e protocolos de Redes Amplas (Wide Area Networks), como ATM (Assynchronous Transfer Mode - Modo de Transferência Assíncrona), Frame Relay (Transmissão de Quadros) e redes Seriais.

Camada da Internet

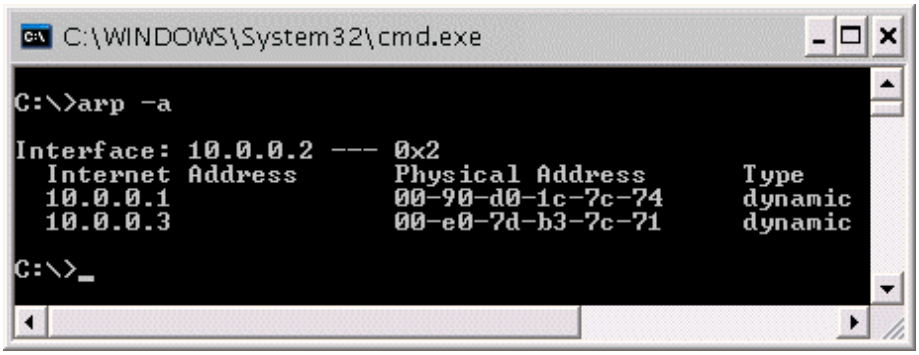
A camada da internet contém quatro protocolos principais: ARP, IP, ICMP e IGMP, descritos e explanados a seguir.

Address Resolution Protocol (ARP)

O Protocolo de Resolução de Endereços cuida da resolução de endereços IP para endereços físicos, ou endereços MAC (Media Access Control - Controle de Acesso à Mídia). Estes endereços MAC são compostos por 48 bits, representados por 16 números hexadecimais de dois algarismos separados por traços, e identificam o computador em uma rede Ethernet. Por esta definição, 00-E0-2D-03-1A-7B é um endereço físico válido. Cada placa de rede ethernet possui um número único (não são fabricadas duas placas de rede com o mesmo número) que não pode ser mudado.

Um número hexadecimal é de base 16. Além dos números de 0-9 usa também letras de A-F. Foi criado para simplificar a exibição de números binários extensos, já que um dígito hexadecimal representa quatro dígitos binários (bits). Por exemplo, o número binário "1101" pode ser simplesmente escrito como "D" na base hexadecimal.

Cada vez que o computador resolve um endereço IP para endereço físico, ele grava esta informação em uma tabela que é mantida na memória chamada de cache do ARP. Assim, caso esta informação seja necessária mais tarde, um novo processo de resolução não será executado. No entanto, cada entrada na tabela tem um tempo de expiração, para evitar erros no caso de algum dispositivo na rede trocar de endereço IP.



*A tabela cache do ARP pode ser exibida no Windows através do comando **arp -a**.*

Processo de Resolução de Endereços MAC

1. O computador compara o endereço IP de destino de todos os pacotes de saída com o Cache do ARP, para ver se o endereço MAC já não foi resolvido anteriormente.

2. Caso o cache não tenha a informação, o ARP envia um broadcast na rede, pedindo para que o computador com o referido endereço IP responda com seu endereço físico. Esta solicitação inclui seu próprio MAC.

Broadcast é uma forma de transmissão de pacotes de dados na qual todos os clientes TCP/IP da rede processam o pacote. Opõe-se ao Unicast (pacote direcionado a um host específico) e Multicast (um grupo de hosts determinado recebe o pacote).

3. O dispositivo na rede com o endereço IP de destino adiciona a informação do endereço MAC do computador que enviou a solicitação ao seu cache ARP e responde a solicitação com seu próprio endereço físico.

4. A resposta é recebida e o endereço físico solicitado é armazenado no cache do ARP. O pacote finalmente é enviado ao destino.

Internet Protocol (IP)

O Protocolo da Internet é responsável por endereçar e entregar os dados em uma comunicação de rede TCP/IP: ele sempre tenta entregar os dados, mas não garante que eles sejam entregues, que eles sejam entregues livres de erros ou que sejam entregues na mesma ordem pois isto é função de um protocolo da camada superior, (como o TCP) ou da aplicação. O IP não estabelece uma sessão (link virtual) entre o computador de origem e o de destino: ele também é responsável por pegar os dados da camada de Interface de Rede e apresentá-los ao protocolo da camada acima que os solicitou.

O IP, quando os dados chegam a ele vindos da camada superior, adiciona suas informações de controle e um cabeçalho aos dados. A partir daí, aquele bloco de dados é chamado de *datagrama.*

O datagrama, ao receber as informações de cabeçalho da camada de interface de rede (como o protocolo Ethernet) é chamado de *pacote*. Não estranhe se ouvir falar em pacote no lugar de datagrama: muitas pessoas confundem os dois termos.

- O cabeçalho do IP tem vários campos, a saber:

Versão: Este campo define a versão do protocolo IP utilizada. A versão atual é a 4, mas já está em testes a versão de número 6.

Comprimento do Cabeçalho: Este campo define o tamanho, em blocos de 32 bits, do cabeçalho do IP. O menor cabeçalho possível conteria 5 neste campo, o que equivale a 5*32bits = 160bits.

Tipo de Serviço: Este campo contém quatro subcampos. O primeiro é o campo de precedência, que permite configurar a prioridade com que estes dados devem ser enviados na rede. Ele ocupa dois bits, e, por isso, seus valores variam de 0 a 7. Os outros três campos são bits únicos e, teoricamente, deveriam controlar como o datagrama deve ser roteado na rede: são os bits de baixo Retardo (Delay), Rendimento (Troughput) e Confiabilidade (Reliability).

Por exemplo, em uma videoconferência o aplicativo poderia definir o bit de retardo como 1, indicando que o programa necessita de baixo retardo (as informações de uma videoconferência devem chegar o mais rápido possível ao destino); o bit de rendimento como 1 também (já que enormes quantidades de dados precisam chegar ao destino) e o bit de confiabilidade como 0 (as informações que não chegarem em tempo ao destino não serão mais necessárias). Uma transferência de arquivos priorizaria a confiabilidade e assim por diante. Dizemos que isso deveria acontecer na teoria porque todos os roteadores por onde o datagrama passa devem suportar esta função para que ela funcione, o que é bem difícil em uma rede grande como a internet.

Roteador é um componente da rede que se encarrega de destinar os dados que devem ser encaminhados a outras redes que não a que seu computador se encontra.

Comprimento Total: Tamanho total do datagrama medido em bytes. Como este campo é composto por 16 bits, o tamanho máximo de um datagrama IP é de 65535 bytes.

Identificação: Este campo tem a ver com a fragmentação de datagramas IP. Ele identifica quais fragmentos pertencem a qual datagrama, para que o destino não se confunda na hora de remontá-lo.

A fragmentação pode ocorrer quando um datagrama é enviado entre duas redes diferentes e que têm tamanhos máximos de datagrama (MTU - Maximum Transmission Unit ou Unidade Máxima de Transmissão) diferentes. Tomemos por exemplo um datagrama de 3.000 bytes trafegando em uma rede FDDI e que chega em um roteador que deve encaminhá-lo por uma rede Ethernet, cuja MTU é de 1518 bytes. Ele deverá ser fragmentado pelo roteador para ser depois remontado pelo computador de destino.

Sinalizadores: Indicam, em uma fragmentação de datagramas, se mais fragmentos chegarão ou se não serão enviados mais dados pertencentes ao datagrama identificado no campo acima. Também indicam se um datagrama pode ou não ser fragmentado. Caso o bit de não fragmentação for definido, o roteador que receber o datagrama e precisar fragmentá-lo para seguir adiante simplesmente descartará aquele datagrama e enviará uma mensagem de erro ao computador de origem.

Offset do Fragmento: Indica de que parte do datagrama a estação de destino deve continuar a remontá-lo para determinado fragmento. Por exemplo, se o primeiro fragmento fosse de 576 bytes e este fragmento fosse o segundo, o campo offset conteria 577, indicando que este fragmento inicia o 577º byte do datagrama.

Tempo de Vida (TTL - Time to Live): O TTL define o tempo máximo que um datagrama pode trafegar na rede antes de ser descartado. Cada vez que o datagrama passa por um roteador, este campo é diminuído. Foi criado para que um pacote não fique eternamente dando voltas na rede. Ele é definido pela estação de origem e é de 8 bits, ou seja, seus valores variam de 0 a 255.

Protocolo: Este campo o protocolo da camada superior para o qual os dados devem ser repassados.

Soma de Verificação: Aqui está contida uma CRC (Cyclic Redudancy Check - Checagem Cíclica Redundante) do cabeçalho IP com o objetivo de evitar erros na transmissão. O CRC é um número que é calculado pelo computador de origem com base no conteúdo do cabeçalho. Quando a estação de destino receber o datagrama, ela calculará a sua CRC com base nos dados de cabeçalho que foram recebidos e caso os valores sejam diferentes dos contidos no campo soma de verificação, um erro na transmisão ocorreu - e o datagrama será descartado. Note que este campo é recalculado cada vez que o datagrama passa por um roteador, pois este altera o campo TTL do cabeçalho.

Endereço IP de Origem e Destino: Estes campos dispensam explicações. O endereçamento IP será discutido posteriormente neste tutorial.

Opções do IP: Pode ou não estar presente (pouco utilizado atualmente). Especifica diversas opções do datagrama IP, como a que permite que os pontos por onde o datragrama passa sejam "ecoados" para o computador de origem e a que configura uma rota restrita, limitando a liberdade dos roteadores em encaminhar o datagrama.

Endereçamento IP

O endereço IP é composto por 32 bits. No entanto, é representado por quatro números de 8 bits separados por pontos chamados de octetos. Cada octeto tem seus valores variando de 0 a 255 (2^8 possibilidades). Por essa definição, 55.82.254.13 é um endereço IP válido. O endereço IP identifica, ao mesmo tempo, a rede em que o host se encontra e o próprio host.

É chamado de host (em português significa anfitrião) qualquer cliente TCP/IP, como computadores, roteadores, impressoras conectadas diretamente à rede e assim por diante.

Mas como o computador faz para descobrir qual parte se refere à rede e qual identifica o host?

Método Baseado em Classes

Antigamente na Internet (note como a história do TCP/IP se confunde com a da Internet), o método existente para determinar qual a parte da rede e qual a pertencente à identificação de host era muito simples: o primeiro byte (8 bits) era utilizado para identificar a rede. Isto permitia cerca de 250 redes e um número quase que incontável de hosts por rede ([2^24] -2 = 16.777.214 hosts). É praticamente impossível uma rede com tantos hosts, o que resultava em desperdício de números IP. Como a internet ainda engatinhava, não havia escassez de endereços. Com seu crescimento (as universidades e grandes escolas passaram a ter acesso a ela), foi necessário inventar um método melhor. Desta maneira que surgiram as classes de IP.

Cinco classes foram criadas: A, B, C, D e E.

Identificando uma Classe

Aqui explicaremos como o IP faz para descobrir a qual classe pertence um determinado endereço IP. Para fazermos isso, usaremos apenas o primeiro octeto do endereço em sua forma binária, já que é para ele que o sistema olha para determinar a classe:

1. O protocolo verifica o primeiro bit do primeiro octeto do endereço: caso ele seja **0** (zero), o endereço é de Classe A. Se ele for **1**, o protocolo passa para o segundo bit.
2. Se o segundo bit for **0**, o endereço é de classe B. Se for 1, o próximo bit é analisado.
3. Se o primeiro e o segundo bits são **1** e o terceiro bit é **0**, o endereço IP é da classe C. E assim o protocolo continua a analisar os bits até chegar na classe E.

Por esse processo, podemos inferir alguns detalhes de cada classe de IP:

Classe A: Os valores do primeiro octeto variam de 1 à 126. Permite 126 redes e 16.777.214 hosts por rede. Por essa definição, o endereço 110.224.16.15 (**01101110.11100000.00010000.00001111**) é da classe A. Na classe A, o primeiro byte é reservado à identificação de rede e os três últimos identificam o host.

Classe B: O primeiro octeto varia de 128 à 191. Permite 16.384 redes e 65.534 hosts por rede. Exemplo de endereço classe B: 135.200.223.5 (**10000111.11001000.11011111.00000101**). Na classe B, os dois primeiros bytes são reservados à identificação de rede e os dois restantes identificam o host.

Classe C: O byte inicial tem seu valor variando de 192 a 223. Nesse caso, 2.097.152 redes são possíveis, com 254 hosts por rede. Exemplo: 200.248.170.1 (**11001000.11111000.10101010.00000001**). Na

classe C, os três primeiros bytes identificam a rede e o último byte identifica um host.

Classe D: A classe D está reservada para endereços de Multicast, que permite enviar datagramas IP para um grupo de computadores. O intervalo reservado vai do IP 224.0.0.0 ao 239.255.255.255.

Classe E: Esta classe está reservada para uso futuro (240.0.0.0 à 254.255.255.255).

A identificação de rede **127.0.0.0** (normalmente seria um endereço classe A) está reservada para testes de conectividade do TCP/IP. Note que o endereço **127.0.0.1** é chamado de endereço de loopback, ou seja, ele aponta para a própria máquina.

Um endereço de host válido **NUNCA** pode conter todos os bits para identificação de host definidos como 0 ou definidos como 1. Se todos referentes à parte de host do endereço IP forem definidos como zero, este IP identificará aquela rede em específico (um roteador utiliza o endereço 10.0.0.0 em sua tabela de roteamento para representar os hosts de 10.0.0.1 até 10.0.0.254). Já se os bits de host forem todos definidos como 1, este endereço designará o endereço de broadcast para aquela rede. Por exemplo, todos os datagramas IP enviados para o endereço 192.168.255.255 (classe B) serão recebidos elos computadores dentro do intervalo de 192.168.0.1 ao 192.168.255.254.

Endereçamento IP Sem Classe

Subredes

As subredes surgiram pelo mesmo motivo do endereçamento IP com classes: evitar o desperdício de números IP. Com a internet crescendo, poucos endereços da classe A tinham sido distribuídos (poucos necessitavam de todos os hosts que esta classe permite), a classe B era freqüentemente solicitada e a classe C, como permitia poucos hosts por rede, geralmente era distribuída em blocos causando entradas desnecessárias nas tabelas de roteamento da Internet. Para contornar este problema, a subrede permite que um endereço IP seja dividido em várias redes menores: desta maneira um endereço classe A pode ser dividido em quantas subredes forem necessárias. Mas, novamente, pergunta-se: como o computador consegue descobrir qual a porção pertencente ao número de rede e qual a que identifica um host?

A resposta para esta pergunta é "Máscaras de Subrede": as máscaras de subrede definem como um endereço de certa classe será dividido. "Binariamente" falando, a máscara deve ser composta de números 1 contíguos (representando a parte que será utilizada para identificar a rede) e completada com zeros. Exemplo: **255.255.248.0** (**11111111.11111111.11111000.00000000**). O computador faz uma operação de E lógico (AND) entre o número IP e a máscara de subrede para identificar a qual rede o computador pertence.

Uma operação de E lógico (AND) trabalha com números binários. A seguinte tabela pode ser montada com os possíveis valores para as duas parcelas da operação e o respectivo resultado:

*__1__ AND __1__ = __1__
*__0__ AND __0__ = __0__
*__1__ AND __0__ = __0__

Exemplo de Subredes

Agora iremos explicar o processo de identificação da rede à qual um host pertence. Por este processo, o computador pode saber se o destino dos dados a serem enviados é local (mesma subrede) ou remoto (o destino encontra-se em uma subrede diferente). Caso for remoto (a identificação calculada para o destino não é igual à sua própria identificação), o computador enviará os dados para o seu roteador padrão e este se encarregará de rotear o datagrama. Vamos tomar, para este exemplo, o IP 172.36.224.53 e aplicá-lo a máscara de subrede 255.255.248.0:

IP: **10101100.00100100.11100000.00110101**
Máscara: **11111111.11111111.11111000.00000000**

10101100.00100100.11100000.00000000

A identificação de rede calculada para este exemplo é 172.36.224.0. A parte destacada em amarelo no endereço acima representa os bits usados para identificação de rede e a parte com fundo azul representa os bits disponíveis para números de host. No exemplo, o primeiro host da subrede teria o endereço 172.36.224.1 (dois últimos bytes: **11100000.00000001**) e o último host, o endereço 172.36.231.254 (dois últimos bytes: **11100111.11111110**).

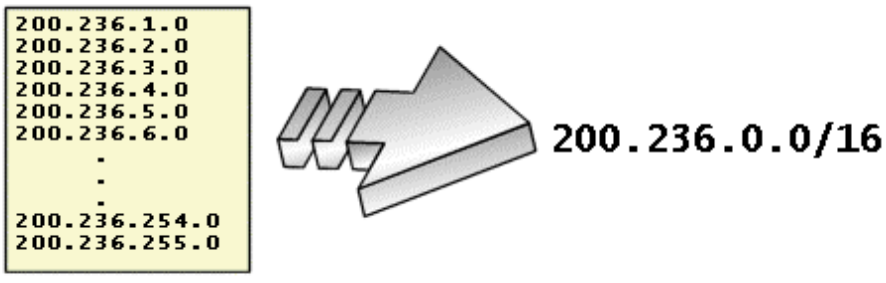
Máscaras de Subrede Padrão

Cada classe de IP (com exceção das reservadas) tem sua máscara de subrede padrão. É fácil de fazer a associação entre elas:

Classe A: 255.0.0.0, indicando que o primeiro byte é utilizado para identificação de rede.
Classe B: 255.255.0.0, indicando que os dois primeiros bytes identificam a rede.
Classe C: 255.255.255.0, indicando que somente o último byte representa a identificação de host.

Super-redes e Classless Inter-Domain Routing (CIDR)

O conceito de super-redes é exatamente o contrário do conceito de subredes: em vez de especificar uma máscara de subrede que divida um espaço de endereço definido por uma classe de IPs, a máscara é utilizada de tal forma a expandir este espaço de endereços. Tomemos um endereço de classe C qualquer: especificando uma máscara de subrede de 20 bits (255.255.240.0), estaremos dando mais espaço de endereço que normalmente a classe C suporta. Aliás, foi justamente para isso que o conceito de super-redes foi criado: combinar várias redes classe C em um bloco para que os roteadores a tratem como uma única grande rede, diminuindo assim o tamanho das tabelas de roteamento.



A notação CIDR também é utilizada para reduzir a quantidade de rotas necessárias em uma tabela de roteamento: ela é composta de um número

IP mais uma barra seguida de um número representando o número de bits definidos como 1 na máscara de subrede. Ex: 200.236.60.87/16 (no caso, a máscara de subrede seria 255.255.0.0 ou 11111111.11111111.00000000.00000000). Uma rota só é adicionada à tabela de roteamento (200.236.0.0/16, representando todos os endereços no intervalo de 200.236.0.1 à 200.236.255.254).

Internet Control Message Protocol (ICMP)

O Protocolo de Mensagens de Controle da Internet serve para suprir a necessidade de uma função para detecção de erro no TCP/IP e para solução de problemas - no entanto ele não tenta fazer do IP um protocolo confiável pois as mensagens ICMP não são confiáveis (nenhuma informação é enviada à estação de origem confirmando a entrega dos dados). Os tipos de mensagens ICMP que são enviadas de volta para a estação de origem estão descritos abaixo:

Destino Inalcançável: É enviada quando um datagrama aponta para um host que não pôde ser encontrado, por problemas na rede, no próprio host, ou em um dos elementos ativos (roteadores) dela. As mensagens possíveis são:

* Rede/Host Inalcançável (Network/Host Unreachable): enviada por um roteador quando, de acordo com sua tabela de roteamento, a rede de destino ou o computador de destino não podem ser alcançados.
* Protocolo Inalcançável (Protocol Unreachable): enviada pelo host de destino quando o protocolo de camada superior indicado no datagrama IP não existe ou não está ativo.
* Porta Inalcançável (Port Unreachable): enviada pelo host de destino quando não há nenhum aplicativo associado à porta especificada nos protocolos TCP ou UDP.

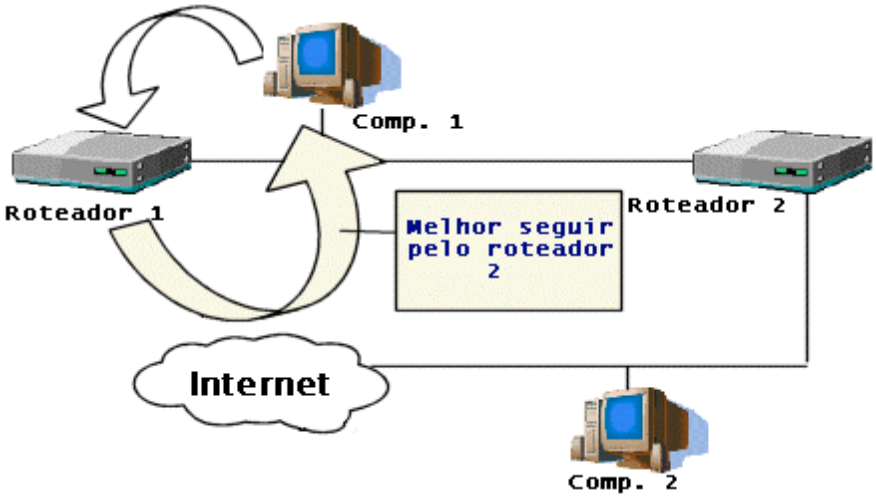
- Fragmentação do Datagrama Necessária e o Sinalizador de não-fragmentação foi definido: neste caso o bit de não-fragmentação do datagrama IP foi configurado mas o datagrama deve ser fragmentado para seguir seu percurso e com isso ele acabará sendo descartado.
- Rota de Origem Falhou: A rota especificada nas Opções do datagrama IP falhou em entregar corretamente o datagrama. Isto geralmente ocorre quando o roteamento restrito está desabilitado no roteador. Este simplesmente descarta o datagrama.

Tempo Limite atingido: Esta mensagem é enviada quando o tempo de vida do pacote se esgotou e o datagrama foi descartado (enviada por um roteador) ou quando o tempo de reintegração de um datagrama fragmentado se esgotou (típico de quando nem todos os fragmentos conseguem chegar ao destino, um host a envia).

Problema em um Parâmetro: Caso algum campo do datagrama IP tenha sido mal configurado a ponto de impedir sua transmissão pela rede, esta mensagem é enviada à origem e o datagrama, descartado.

Páre Origem! (Source Quench): O roteador está na sua capacidade máxima de destinar datagramas e "pede" à estação de origem para parar de enviar ou diminuir a freqüência de envio dos datagramas. O roteador, ao enviar estas mensagens, está descartando pacotes.

Redirecionamento: A seguinte situação causaria o envio de uma mensagem de redirecionamento ao host de origem do datagrama:



O computador 1 quer enviar um datagrama ao computador 2 mas ele descobre que o computador 2 não está na mesma subrede - então ele envia o pacote através do Roteador 1. O próximo roteador a ser encaminhado o pacote, de acordo com a tabela de roteamento do roteador 1, é o Roteador 2. No entanto, o Roteador 1 nota que o computador 2 está na mesma rede que o Roteador 2, então envia uma mensagem ICMP de Redirecionamento ao Computador 1 dizendo que melhor seria se ele enviasse o datagrama diretamente através do Roteador 2.

- **Eco (Echo):** Tipo de mensagem utilizada por vários utilitários do TCP/IP (incluindo Ping), em que a mensagem do datagrama original deve voltar à estação de origem.

Marca de Tempo (Timestamp): Mensagem de eco que inclui uma marca de tempo. O destinatário lê e adiciona sua própria marca de tempo. Utilizada para determinar o tempo necessário para um datagrama ir até o destinatário e voltar à estação de origem.

Resposta/Requerimento de Informação: Esta mensagem ICMP foi criada para permitir que estações de rede sem disco pudessem descobrir seus próprios IPs na hora da inicialização. Tornou-se obsoleta.

Utilitários que funcionam com base no ICMP

Trace Route

O trace route serve para descobrir o caminho que um datagrama percorre entre um determinado host e outro na rede. No Windows, entre em um prompt de comando e digite **tracert host**, onde host é o nome ou o IP do host para o qual você deseja a rota. O seguinte processo é executado:

1. O programa envia uma mensagem ICMP de eco para o destino com um TTL suficiente apenas para chegar ao próximo roteador.

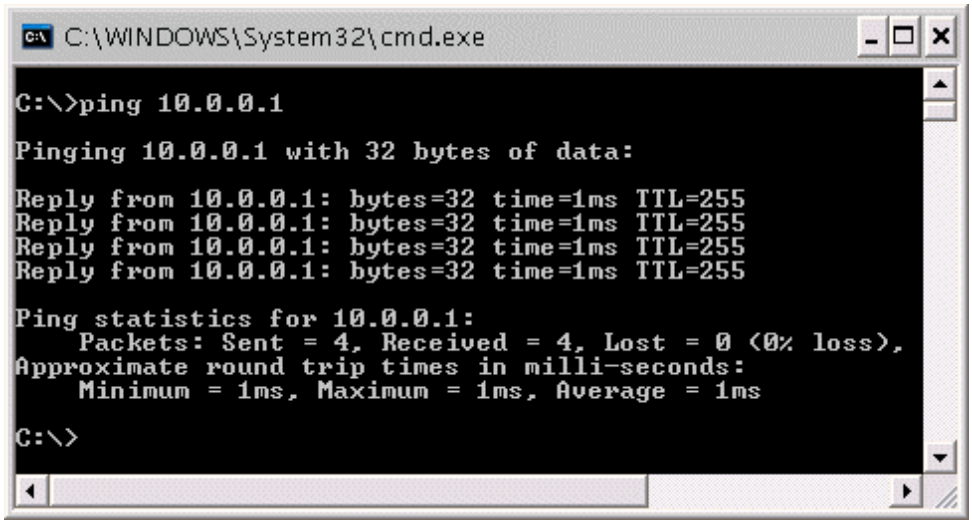
2. O roteador diminuiu o TTL e, como chegou a zero, descarta o pacote e envia uma mensagem de Tempo Limite Atingido de volta para o originador.

3. O trace route examina o datagrama do tempo limite e determina de onde veio. Após isso, ele coloca estas informações na tela.

O trace route continua a incrementar o TTL até atingir o destino ou até o tempo de vida máximo permitido. Ele é muito útil para determinar em qual parte da rede o datagrama pára, em caso de um problema de comunicação entre dois hosts.

Ping

O ping se utiliza de uma mensagem ICMP de eco para determinar se um host está online e funcionando corretamente: caso o host estiver online, ele retornará com uma mensagem de resposta ao eco. O ping analisará esta mensagem e determinará quanto tempo se passou entre a mensagem de eco enviada e a resposta e mostrará os resultados na tela.



Internet Group Message Protocol (IGMP)

O Protocolo de Mensagens em Grupo da Internet foi desenhado para que os hosts pertencentes a um determinado grupo multicast possam informar os roteadores da rede sobre os participantes do grupo. Assim, os roteadores sabem a quem entregar os datagramas pertencentes a determinado grupo. Na versão 2 deste protocolo as mensagens para deixar o grupo também foram implementadas, agilizando o processo.

Apesar deste protocolo ser de relativa importância para uma rede TCP/IP, neste tutorial detalharemos melhor o processo de Multicast já que, ao menos que você queira configurar opções avançadas em um roteador (o que foge da alçada deste artigo), o escrito acima é tudo que você precisa saber sobre IGMP.

Detalhando o processo de Multicasting

O processo de Multicasting pode ser dividido em duas abordagens: a abordagem da camada de Interface de rede (o protocolo utilizado nesta camada também deve suportar multicast e aqui usaremos o protocolo Ethernet, que constitui mais de 80% das redes locais) e a abordagem do protocolo IP.

Tratamento dado ao Multicast em redes Ethernet

Uma placa de rede Ethernet está continuamente analisando o tráfego da rede para saber se o endereço MAC dos pacotes que estão trafegando é o seu: quando ela identificar um pacote com o seu próprio endereço físico na parte do destinatário, ela "pegará" e processará o pacote, entregando-o à um protocolo de camada superior. O Multicast também usa um endereço MAC específico para que a placa de rede consiga saber que aquele pacote pertence a ela. Aqui temos uma pequena ajuda do driver da placa, que permite que uma aplicação que necessita utilizar-se de multicast configure os endereços MAC para os quais a placa de rede deve atentar.

Existe um padrão, definido pelo Institute of Electrical an Electronic Engineers (IEEE, uma das organizações que planejam e monitoram a Internet), para endereços físicos de multicast: "**O bit de menor ordem do octeto de maior ordem em um endereço MAC multicast deve ser definido como 1 (um)**". Muito explicativo, não? Aqui vai um exemplo:

01 - 00 - 5E - 03 - 1A - 7B
Convertendo para binário:
00000001-00000000-00101101-00000011-00011010-01111011

Note o número destacado em vermelho: este é o bit de menor ordem no octeto de maior ordem (este octeto destacado em amarelo); como ele está definido como 1, este é um endereço válido de Multicast em uma rede Ethernet. Um endereço de unicast naturalmente teria este bit definido como zero.

Tratamento de Multicast do IP

Como já explicado antes neste tutorial, o IP utiliza-se da classe D de endereços IP (224.0.0.0 ao 239.255.255.255) para diferenciar um endereço unicast de um multicast. Simples e eficiente.

Gerando Endereços MAC Multicast

Os endereços MAC de multicast não são gerados ao acaso. Também existem diretrizes (definidas pelo IEEE) para mapear um endereço MAC Multicast a um endereço IP Multicast. A seguinte regra se aplica:

"**Os 23 bits de menor ordem de um endereço IP Multicast devem representar os 23 bits de menor ordem de determinado endereço MAC Multicast. Os outros bits do endereço físico são definidos pelo IEEE**". Para facilitar, vamos a um exemplo:

224.3.26.136

Em binário:
11100000.00000011.00011010.01111011
23 bits de menor ordem

00000001-00000000-01011110-00000011-00011010-01111011
Bits definidos pelo IEEE Bits retirados do endereço IP

Em Hexadecimal:
01 - 00 - 5E - 03 - 1A - 7B

Primeiro, convertemos o endereço IP para seu formato binário. Os 23 últimos bits foram copiados para os 23 últimos bits do endereço MAC. Como os outros bits são definidos pelo IEEE, tudo o que temos de fazer é juntar os dois e converter o número para o formato usual: hexadecimal.

Camada de Transporte

Dois protocolos fundamentais ao funcionamento do TCP/IP ficam nesta camada: TCP e UDP.

Transmission Control Protocol (TCP)

Finalmente veremos um pouco de confiabilidade! Até agora, todos os protocolos explicados não ofereciam métodos para confirmar a entrega dos dados com sucesso. O Protocolo de Controle de Transmissão checa por erros em cada pacote que recebe para evitar a corrupção dos dados. Vamos começar pelo cabeçalho TCP. Ele possui os seguintes campos principais:

Porta de Origem: Uma porta define o aplicativo na camada mais acima que transmitiu e que deverá receber os dados na outra ponta. Neste campo, é especificada a porta de origem.

Porta de Destino: A porta (aplicativo) de destino.

Número de Seqüência: Aqui será definido o número de seqüência do pacote TCP. Ele serve para evitar que ocorra a corrupção dos dados se um pacote chegar ao destino antes de outro, ou para detectar algum pacote que porventura se perdeu no caminho entre a origem e o destino.

Número de Confirmação: Este número é enviado pela estação de destino para a estação de origem, para confirmar o recebimento de pacote(s) recebido(s) anteriormente.

Offset dos Dados: Indica o tamanho do cabeçalho TCP, em blocos de 32 bits.

Reservado: Um campo reservado para uso futuro, sempre planejando previamente as melhorias ao protocolo.

Bits de Controle: São os seguintes:

- URG (Urgente): Evia uma mensagem ao destino de que dados urgentes estão esperando para serem enviados a ele.
- ACK (Confirmação): Confirma o recebimento de um ou mais datagramas enviados anteriormente.
- PSH (Push): Faz com que o TCP imediatamente envie os dados pendentes.
- RST (Reset): Reinicia a comunicação entre os hosts.
- SYN: Usado na inicialização e para estabelecer um número de seqüência.
- FIN: Mais nenhum dado está vindo da estação de origem.

Window (janela): O número de octetos de dados que começam com o valor indicado no campo Acknowledgement que o remetente do segmento de dados está querendo aceitar. Este é o método de controle de fluxo do TCP e se o receptor quiser que a estação de origem páre de enviar dados, ele configurará este campo como zero.

Soma de Verificação: Somente um método de detecção de erros.

Ponteiro Urgente: Aponta para o número de seqüência do byte após os dados urgentes. Interpretado apenas quando URG é definido.

HandShake (aperto de mão) de Três Vias

O TCP é um protocolo orientado à conexão porque os dois computadores participantes da transmissão de dados sabem da existência um do outro. Pode parecer um pouco simplório, mas nenhum protocolo explicado até agora tem essa funcionalidade. Esta conexão virtual entre eles é chamada de sessão. Entre outras coisas, o Handshake de três vias sincroniza os números de seqüência entre as duas estações de rede. O processo ocorre da seguinte maneira:

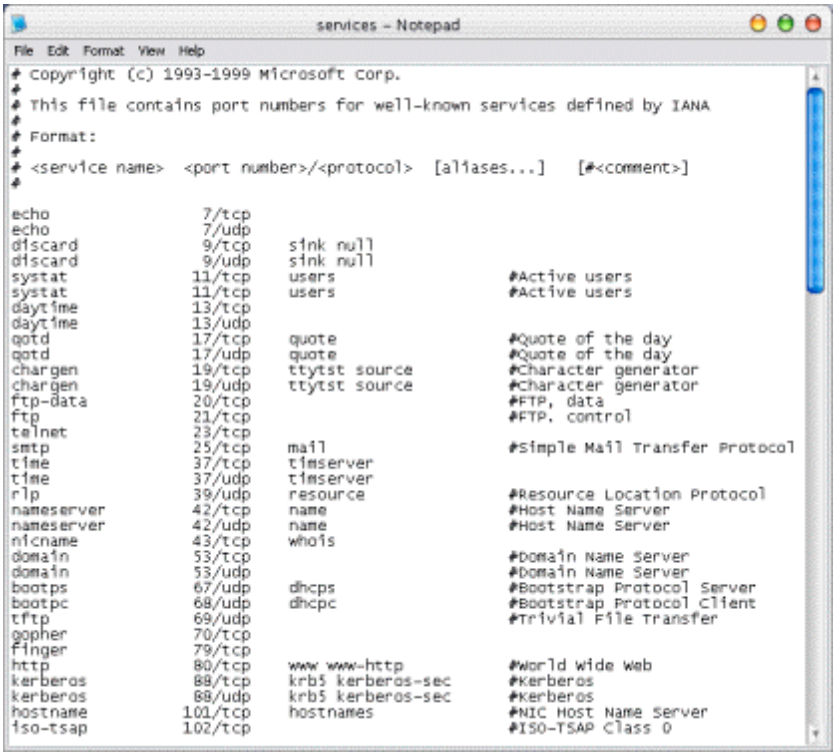
1. O computador de origem inicia a conexão, transmitindo informações da sessão como número de seqüência e tamanho do pacote.
2. O computador de destino responde com suas informações sobre a sessão.
3. O computador de origem confirma o recebimento das informações e a sessão é estabelecida. Com os números de seqüência sincronizados, a transferência de dados pode ser efetuada sem erros.

"Janelamento" (Windowing)

A transferência de arquivos seria muito lenta se cada vez que o TCP enviasse um pacote, esperasse pela confirmação de recebimento para enviar o próximo: para evitar este problema, criou-se o "janelamento". Podemos definir este processo como sendo a quantia de dados que a estação de origem pode enviar sem receber confirmação de cada pacote.

Portas

Como já explicado, uma porta se refere ao aplicativo da camada de aplicação que irá processar os dados. Como o campo sobre as Portas é de 16 bits, teremos que o TCP/IP permite 65535 números de porta diferentes, sendo as primeiras 1024 estáticas (pré-definidas) e as outras dinâmicas. Geralmente, a porta de origem é gerada aleatoriamente pela aplicação, no entanto, a porta de destino é fixa.



Você pode encontrar uma lista com os números de porta estáticos mais utilizados abrindo o arquivo C:\Windows\system32\drivers\etc\services (sem extensão) com o notepad. Para isso, clique em Iniciar -> RUN e digite: **notepad c:\Windows\System32\drivers\etc\services**. troque o drive C: e a pasta Windows por, respectivamente, o letra do drive e a pasta onde seu sistema operacional está instalado.

Não confunda Portas TCP com UDP: apesar das duas terem a mesma função (identificar a aplicação da camada superior), o mesmo número de porta em ambas não necessariamente identifica um mesmo aplicativo.

User Datagram Protocol (UDP)

Ao contrário do TCP, este protocolo não é confiável, não é baseado em sessão e não confirma cada pacote enviado - no entanto ele identifica o aplicativo da camada superior usando também um número de porta. Por não ter todos esses procedimentos para detecção de erros, o UDP é um protocolo bem mais leve do que o TCP e adiciona muito menos informações ao cabeçalho.

O UDP é geralmente utililizado por aplicativos que ou implementam seu próprio mecanismo de entrega de dados confiável ou que simplesmente não necessitam dessa função. Um bom exemplo disso são aplicações de videoconferência: as informações devem chegar rapidamente ao destino, já que um pacote atrasado não terá mais serventia. O cabeçalho do UDP contém as seguintes informações:

Porta de Origem
Porta de Destino
Tamanho da Mensagem (em blocos de 32 bits)
Soma de Verificação

Camada de Aplicações

Aqui é que residem os aplicativos que normalmente o usuário utiliza: navegador, e-mail, cliente FTP... São identificadas pela camada mais embaixo por números de porta, como já mencionado anteriormente.

Por: Agnaldo Fernandes 28/11/2003