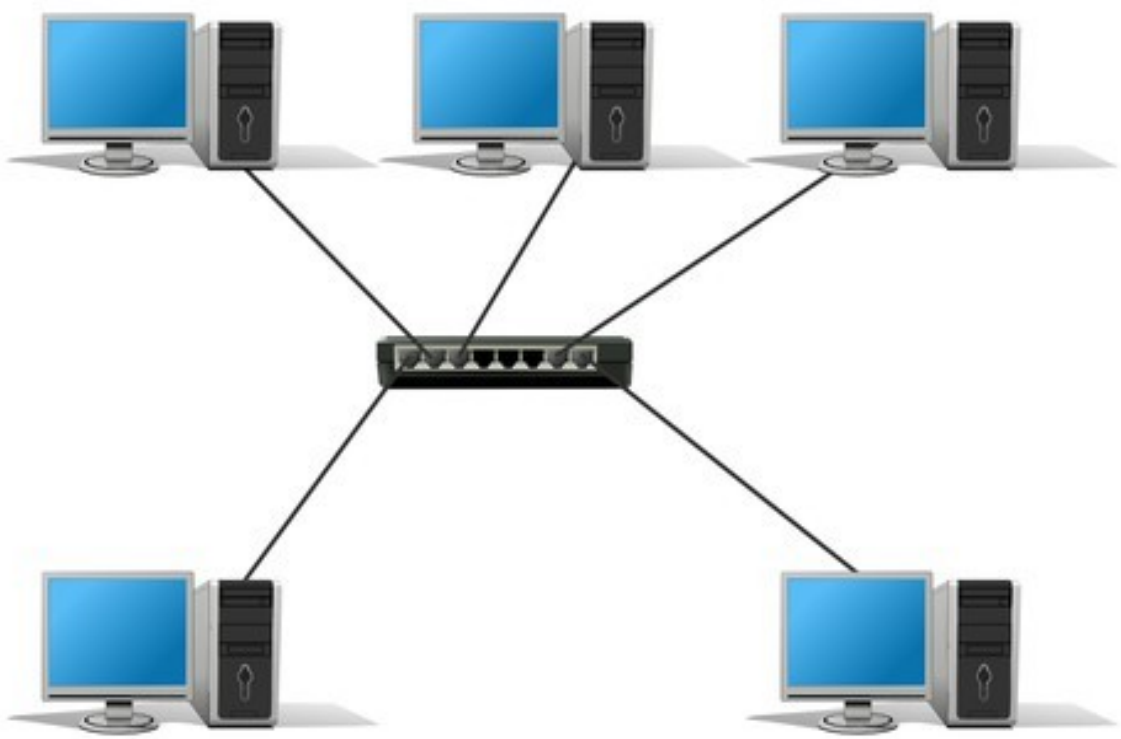
Um resumo sobre redes e TCP/IP

1. Introdução

Podemos dizer que a função de qualquer rede é simplesmente transportar informações de um ponto a outro. Pode ser entre dois micros ligados através de um simples cabo cross-over, ou pode ser entre dois servidores situados em dois continentes diferentes. Do ponto de vista do sistema operacional e dos aplicativos, não faz muita diferença.

No nível mais baixo, temos os cabos de rede, que são enquadrados no primeiro nível do modelo OSI (camada física) e se destinam unicamente a transportar os impulsos elétricos de um micro a outro. Ao utilizar uma rede wireless ou cabos de fibra óptica, os sinais são transmitidos (respectivamente) na forma de sinais de rádio ou luz, mas a função básica (transportar dados de um ponto a outro) continua a mesma, independentemente da mídia utilizada.



Existem basicamente 3 tipos diferentes de cabos de rede: os cabos de par trançado (que são, de longe, os mais comuns), os cabos de fibra óptica (usados principalmente em links de longa distância) e os cabos coaxiais, que são usados em cabos de antenas para redes wireless e em algumas redes antigas.

Entre os cabos de par trançado, existem cabos de cat 1 até cat 7. Como os cabos cat 5 são suficientes tanto para redes de 100 quanto de 1000 megabits, eles são os mais comuns e mais baratos, mas os cabos cat 6 e cat 6a estão se

popularizando e devem substituí-los ao longo dos próximos anos. Os cabos são vendidos originalmente em caixas de 300 metros, ou 1000 pés (que equivale a 304.8 metros):

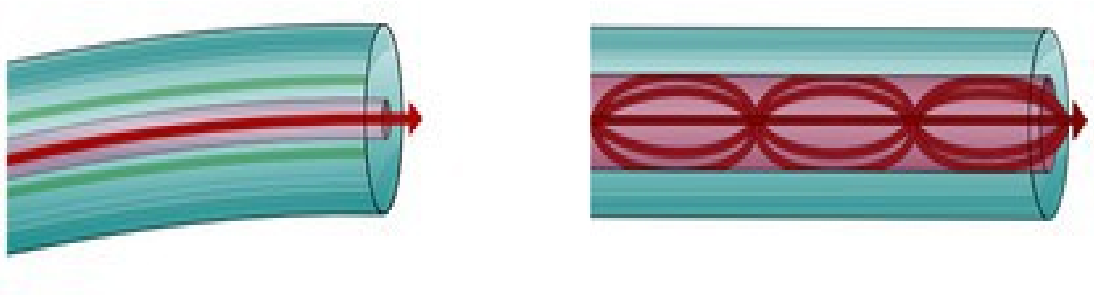
No caso dos cabos cat 5e, cada caixa custa em torno de 200 reais aqui no Brasil, o que dá cerca 66 centavos o metro. Os cabos de categoria 6 e 6a ainda são mais caros, mas devem cair a um patamar de preço similar ao longo dos próximos anos.

Entre os cabos de fibra óptica, existem dois tipos: os cabos de fibra multimodo ou MMF (multimode fibre) e os monomodo ou SMF (singlemode fibre). As fibras monomodo possuem um núcleo muito mais fino, de 8 a 10 mícrons de diâmetro, enquanto as multimodo utilizam núcleos mais espessos, tipicamente com 62.5 microns.

As fibras multimodo são mais baratas e o núcleo mais espesso demanda uma precisão menor nas conexões, o que torna a instalação mais simples, mas, em compensação, a atenuação do sinal luminoso é muito maior.

Isso acontece porque o pequeno diâmetro do núcleo das fibras monomodo faz

com que a luz se concentre em um único feixe, que percorre todo o cabo com um número relativamente pequeno de reflexões. O núcleo mais espesso das fibras multimodo, por sua vez, favorece a divisão do sinal em vários feixes separados, que ricocheteiam dentro do cabo em pontos diferentes, aumentando brutalmente a perda durante a transmissão, como você pode ver nos desenhos a seguir:



Para efeito de comparação, as fibras multimodo permitem um alcance de até 550 metros no Gigabit Ethernet e 300 metros no 10 Gigabit, enquanto as fibras monomodo podem atingir até 80 km no padrão 10 Gigabit. Esta brutal diferença faz com que as fibras multimodo sejam utilizadas apenas em conexões de curta distância, já que sairia muito mais caro usar cabos multimodo e repetidores do que usar um único cabo monomodo de um ponto ao outro.

2. Hubs, switches e hub-switches

Em seguida temos os switches ou hub-switches que utilizamos para interligar os micros da rede local. Na verdade, o termo "hub-switch" foi inventado pelos fabricantes para diferenciar os switchs mais baratos, que carecem de funções mais avançadas dos switchs "de verdade", que possuem mais portas e incluem interfaces de administração elaboradas.

O termo "switch" está mais relacionado ao modo de funcionamento do aparelho e não ao seu custo ou suas funções. Um switch é capaz de encaminhar os frames Ethernet para o destinatário correto, fechando "circuitos" entre as duas portas envolvidas, enquanto um hub antigo simplesmente repete os sinais recebidos em todas as portas.

Assim como as placas de rede, os switchs trabalham no nível 2 do modelo OSI (link de dados), enviando frames Ethernet e endereçando os outros dispositivos da rede usando endereços MAC ao invés de endereços IP. Só para efeito de comparação, os hubs "burros" trabalham no nível 1, assim como os cabos de rede. Eles são meros dispositivos de transmissão, que não realizam processamento.

Um switch pode operar de quatro formas. No sistema **cut-through** o switch inicia a retransmissão dos frames imediatamente após receber os headers (que contém os endereços de origem e de destino). Nesse modo o switch não faz nenhum tipo de verificação no frame, simplesmente o retransmite da forma como os dados foram recebidos. No modo **store-and-forward** o switch armazena o pacote na memória, realiza algumas verificações básicas e só então envia o pacote ao destinatário, descartando pacotes inválidos e solicitando a retransmissão de pacotes corrompidos.

A vantagem do modo cut-through é a baixa latência, já que o switch executa muito pouco processamento e vai retransmitindo os dados do pacote conforme eles são recebidos. Entretanto, além da questão da estabilidade e melhor uso da banda da rede, o modo store-and-forward oferece uma vantagem importante, que é o fato de permitir que as portas do switch trabalhem a diferentes velocidades, sem precisar reduzir a taxa de transmissão da porta mais rápida, limitando-a à da porta mais lenta.

Uma terceira tecnologia é a **adaptative cut-through**, disponível em modelos mais recentes. Nesse modo, o switch opera inicialmente em modo cut-through (para minimizar a latência), mas passa automaticamente a operar em modo store-and-forward caso detecte um grande volume de frames inválidos ou corrompidos, ou caso precise transmitir frames entre duas portas operando a diferentes velocidades (100 e 1000, por exemplo). No caso dos switches

adaptative cut-through gerenciáveis, é possível também forçar um dos dois modos de operação.

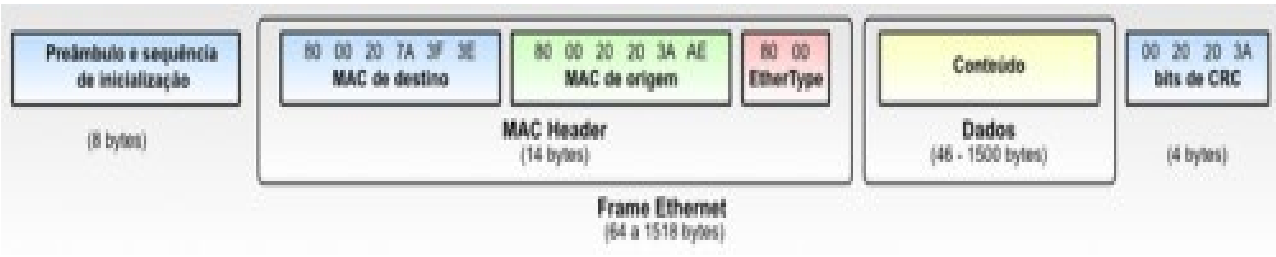
Hoje em dia, o modo de operação do switch é mais uma opção de design do que uma diferença prática, pois em redes de 100 e 1000 megabits o tempo de latência é sempre muito baixo, independentemente do modo de operação. A maioria dos switches gigabit atuais operam com tempos de latência inferiores a 20 microsegundos (0.02 ms), o que é uma necessidade, já que um switch lento não conseguiria encaminhar 1 gigabit de dados por segundo em primeiro lugar.

O quarto modo de operação, pouco relevante hoje em dia, é o fragment-free, onde o switch aguarda o recebimento dos primeiros 64 bytes do frame, certifica-se de que não ocorreu uma colisão e só então o retransmite. Este modo foi desenvolvido para minimizar a ocorrência de colisões, mas se tornou irrelevante com a popularização do modo full-duplex, onde é negociado um canal exclusivo de transmissão entre cada estação e o switch, eliminando o problema.

3. Frames e pacotes

Os frames Ethernet são "envelopes" para os pacotes TCP/IP. O aplicativo (um navegador, um servidor web, ou qualquer outro aplicativo transmitindo dados pela rede) envia os dados ao sistema operacional, que divide o fluxo em pacotes TCP/IP e os envia à placa de rede. As placas de rede (que não entendem o protocolo TCP/IP) tratam os pacotes como um fluxo de dados qualquer e adicionam mais uma camada de endereçamento, desta vez baseada nos endereços MAC dos dispositivos da rede, gerando o frame Ethernet que é finalmente transmitido. Ao chegar do outro lado, o "envelope" é removido e o pacote TCP/IP é entregue.

O uso dos frames adiciona alguns bytes adicionais a cada pacote transmitido, reduzindo sutilmente o desempenho da rede. Veja o diagrama de um frame Ethernet:

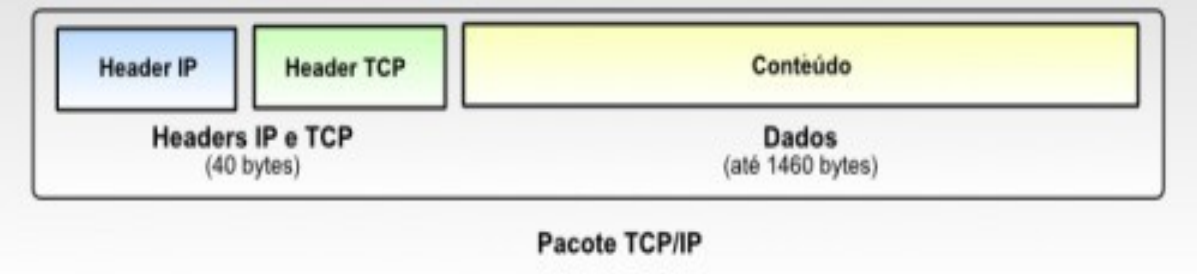


A transmissão de cada frame começa com o envio de 8 bytes contendo um preâmbulo e uma sequência de inicialização. Ele serve para avisar outros micros da rede de que uma transmissão está prestes a começar. Estes 8 bytes iniciais não fazem parte do frame e são descartados pelas placas de rede depois de recebidos, por isso não aparecem no relatório mostrado por sniffers

de rede, como o wireshark.

O pacote TCP/IP está contido dentro do campo de dados, que pode incluir até 1500 bytes por frame. Junto com os dados é transmitido o cabeçalho do frame (14 bytes no total), que inclui o endereço MAC de destino, endereço MAC de origem e um campo para o tipo de dados e mais 4 bytes finais, que contém códigos de CRC, usados (pelas placas de rede) para verificar a integridade do frame recebido. Caso o frame chegue incompleto ou corrompido, a placa de rede solicita a retransmissão.

Dentro do pacote TCP/IP temos novos headers, que contém o endereço IP de origem, endereço IP de destino, porta de origem, porta de destino, códigos de verificações, número do pacote, campo para inclusão de opções e assim por diante. No total, temos 20 bytes para os headers do protocolo TCP e mais 20 bytes para os headers do protocolo IP, totalizando 40 bytes de headers por pacote. Desta forma, temos 1460 bytes de dados em um pacote de 1500 bytes e 536 bytes de dados em um pacote de 576 bytes, por exemplo:



À primeira vista, pode parecer estranho que sejam incluídos headers separados para o TCP e o IP, mas a verdade é que os dois são complementares e por isso não podem ser dissociados. É por isso que usamos o termo "TCP/IP", como se os dois protocolos fossem uma coisa só.

Os headers do protocolo IP incluem o endereço IP de origem e o endereço IP de destino, enquanto os headers do TCP incluem a porta de origem e de destino, por exemplo. Em resumo, podemos dizer que o IP se encarrega da entrega dos pacotes, enquanto o TCP se encarrega da verificação de erros, numeração de portas e tudo mais.

Como disse, os pacotes podem ter até 1500 bytes no total, onde temos até 1460 bytes de dados e 40 bytes dos headers. Arquivos e outros tipos de informações são transmitidas na forma de sequências de vários pacotes. Um arquivo de 15 KB, por exemplo, seria dividido em um total de 11 pacotes; os 10 primeiros contendo 1460 bytes cada um e o último contendo os últimos 760 bytes. É graças aos códigos de verificação e numeração dos pacotes que arquivos grandes podem ser transmitidos de forma íntegra mesmo através de conexões via modem ou links wireless, onde diversos pacotes são corrompidos ou perdidos. Basta retransmitir os pacotes extraviados ou danificados quantas vezes for necessário. :)

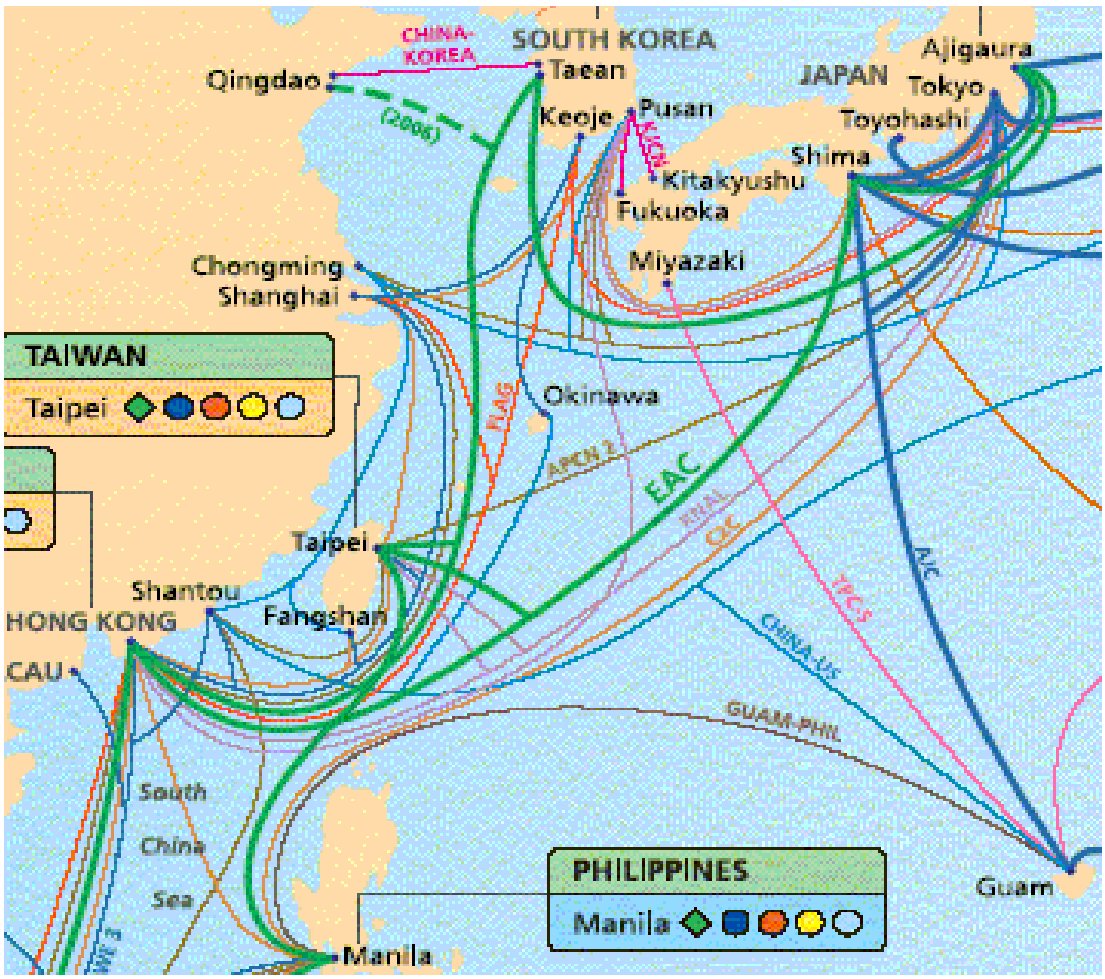
Embora os pacotes TCP/IP de 1500 bytes sejam os mais comuns, o tamanho pode variar de acordo com o meio de transmissão usado. No ADSL PPPoE (o ADSL com autenticação, usado na maioria das instalações atuais), por exemplo, são utilizados pacotes de 1492 bytes, enquanto que nas conexões discadas são geralmente utilizados pacotes de apenas 576 bytes. Existem ainda casos de pacotes maiores, utilizados em situações específicas.

Dentro da rede local, temos (incluindo o preâmbulo do frame Ethernet) um total de 1526 bytes transmitidos para cada pacote TCP/IP de 1500 bytes. Em uma rede local, que trabalha a 100 ou 1000 megabits, isso não faz muita diferença, mas na internet isso seria um grande desperdício. Por isso, os roteadores se encarregam de eliminar estas informações desnecessárias, retransmitindo apenas os pacotes TCP/IP propriamente ditos. É por causa disso que não é possível criar regras de firewall baseadas em endereços MAC para pacotes vindos da Internet: os endereços MAC fazem parte das informações incluídas no frame Ethernet, que são descartadas pelos roteadores.

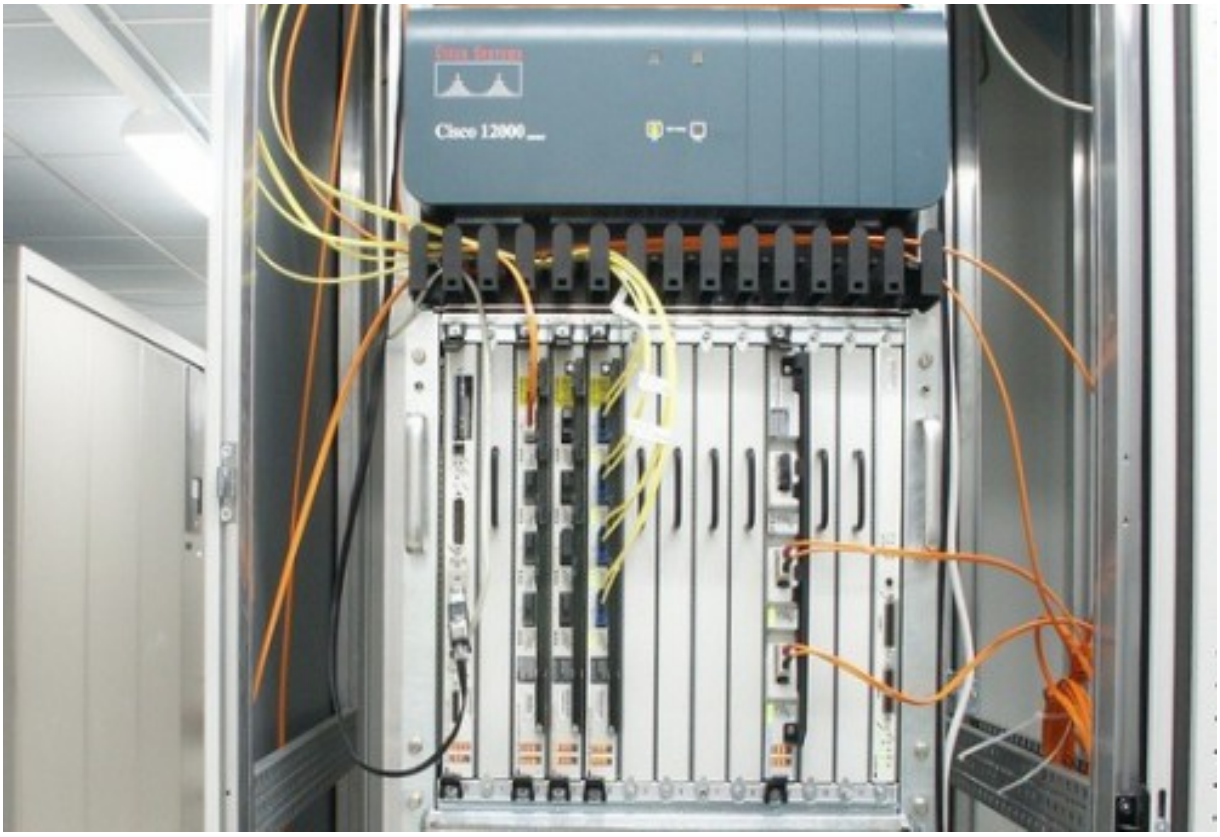
4. Roteadores e links de longa distância

Por trabalharem diretamente com endereços IP, os roteadores podem ser enquadrados na camada 3 do modelo OSI (camada de rede). Basicamente, são roteadores que cuidam de todo o trafego de dados na internet. Você pode utilizar um hub ou switch dentro da sua rede local, mas ao acessar a internet você sempre utiliza um roteador, seja um roteador Cisco de grande porte, seja um micro com duas placas de rede compartilhando a conexão, ou seja um roteador dentro da rede do provedor de acesso. Na internet, o mais comum é o uso de links de fibra óptica, mas os roteadores podem se interligados utilizando qualquer tipo de mídia.

Temos aqui um exemplo, que mostra Backbones de fibra óptica interligando países da Ásia:



Este é um exemplo do que você veria em pontos de interconexão: um roteador Cisco com diversos links de fibra óptica:



Quando você usa um PC com duas placas de rede para compartilhar a conexão com os micros da rede local, você está configurando-o para funcionar como um roteador simples, que liga uma rede (a Internet) a outra (a sua rede doméstica). O mesmo acontece ao configurar seu modem ADSL como roteador. Pense que a diferença entre os switches e os roteadores é justamente esta: os switches permitem que vários micros sejam ligados formando uma única rede, enquanto que os roteadores permitem interligar várias redes diferentes, criando redes ainda maiores, como a própria Internet.

Dentro de uma mesma rede é possível enviar pacotes de broadcast, que são endereçados a todos os integrantes da rede simultaneamente e, ao usar um hub burro, todos os micros recebem todas as transmissões. Um roteador filtra tudo isso, fazendo com que apenas os pacotes especificamente endereçados a endereços de outras redes trafeguem entre elas. Lembre-se de que, ao contrário das redes locais, os links de Internet são muito caros, por isso é essencial que sejam bem aproveitados.

5. TPC/IP e endereçamento

O endereçamento IP é um tema importante, já que é ele que permite que o brutal número de redes e hosts que formam a internet sejam capazes de se comunicar entre si.

Existem duas versões do protocolo IP: o **IPV4** é a versão atual, que utilizamos na grande maioria das situações, enquanto o **IPV6** é a versão atualizada, que prevê um número brutalmente maior de endereços e deve começar a se popularizar a partir de 2010 ou 2012, quando os endereços IPV4 começarem a se esgotar.

No IPV4, os endereços IP são compostos por 4 blocos de 8 bits (32 bits no total), que são representados através de números de 0 a 255, como "200.156.23.43" ou "64.245.32.11".

As faixas de endereços começadas com "10", com "192.168" ou com de "172.16" até "172.31" são reservadas para uso em redes locais e por isso não são usados na internet. Os roteadores que compõe a grande rede são configurados para ignorar estes pacotes, de forma que as inúmeras redes locais que utilizam endereços na faixa "192.168.0.x" (por exemplo) podem conviver pacificamente.

No caso dos endereços válidos na internet as regras são mais estritas. A entidade responsável pelo registro e atribuição dos endereços é a ARIN (http://www.arin.net/). As operadoras, carriers e provedores de acesso pagam uma taxa anual, que varia de US$ 1.250 a US$ 18.000 (de acordo com o volume de endereços requisitados) e embutem o custo nos links revendidos aos clientes.

Ao conectar via ADSL ou outra modalidade de acesso doméstico, você recebe um único IP válido. Ao alugar um servidor dedicado você recebe uma faixa com 5 ou mais endereços e, ao alugar um link empresarial você pode conseguir uma faixa de classe C inteira. Mas, de qualquer forma, os endereços são definidos "de cima para baixo", de acordo com o plano ou serviço contratado, de forma que você não pode escolher quais endereços utilizar.

Embora aparentem ser uma coisa só, os endereços IP incluem duas informações. O endereço da rede e o endereço do host dentro dela. Em uma rede doméstica, por exemplo, você poderia utilizar os endereços "192.168.1.1", "192.168.1.2" e "192.168.1.3", onde o "192.168.1." é o endereço da rede (e por isso não muda) e o último número (1, 2 e 3) identifica os três micros que fazem parte dela.

Os micros da rede local podem acessar a internet através de um roteador, que pode ser tanto um servidor com duas placas de rede, quando um modem ADSL ou outro dispositivo que ofereça a opção de compartilhar a conexão. Neste caso, o roteador passa a ser o gateway da rede e utiliza seu endereço IP válido para encaminhar as requisições feitas pelos micros da rede interna. Este recurso é chamado de NAT (Network Address Translation).

Um dos micros da rede local, neste caso, poderia usar esta configuração de rede:

Endereço IP: 192.168.1.2
Máscara: 255.255.255.0
Gateway: 192.168.1.1 (o servidor compartilhando a conexão)
DNS: 200.169.126.15 (o DNS do provedor)

O servidor, por sua vez, utilizaria uma configuração similar a esta:

Placa de rede 1 (rede local):
Endereço IP: 192.168.1.1
Máscara: 255.255.255.0

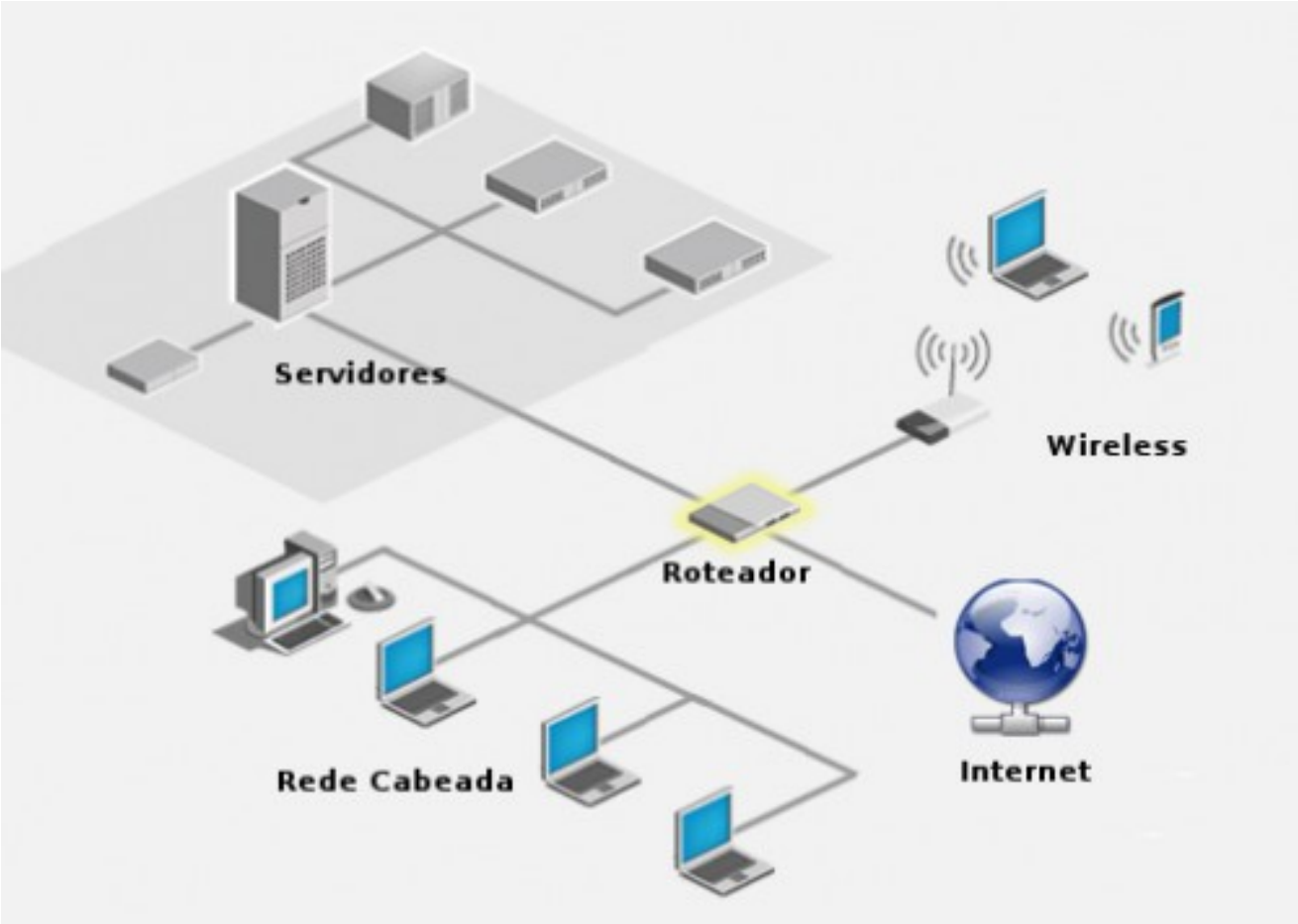
Placa de rede 2 (internet):
Endereço IP: 200.213.34.21
Máscara: 255.255.255.0
Gateway: 200.213.34.1 (o gateway do provedor)
DNS: 200.169.126.15 (o DNS do provedor)

A configuração da segunda placa de rede seria obtida automaticamente, via DHCP, de forma que você só precisaria realmente se preocupar com a configuração da sua rede local. Normalmente, você primeiro configuraria a rede local, depois conectaria o servidor à internet e, depois de checar as duas coisas, ativaria o compartilhamento da conexão via NAT.

É possível instalar mais placas de rede no roteador e dividir a rede em vários

segmentos distintos, interligados através dele. Em uma empresa, poderíamos ter três segmentos diferentes, um para a rede cabeada e a maior parte dos micros, outro para a rede wireless e outro para os servidores, que ficariam isolados em uma sala trancada.

O roteador nesse caso teria 4 placas de rede (um para cada um dos três segmentos e outra para a internet). A vantagem de dividir a rede desta maneira é que você poderia criar regras de firewall no roteador, especificando regras diferentes para cada segmento. Os micros conectados à rede wireless (menos segura), poderiam não ter acesso aos servidores, por exemplo. O firewall, ativo no roteador, poderia também ser configurado para proteger os micros das redes internas de ataques provindos da internet:



Fonte: http://www.hardware.com.br/tutoriais/resumo-redes/pagina5.html

6. Máscaras e classs

Continuando, temos a configuração das máscaras de sub-rede, que servem para indicar em que ponto termina a identificação da rede e começa a identificação do host. No nosso exemplo, utilizaríamos a máscara "255.255.255.0", que indica que os três primeiros números (ou octetos) do endereço servem para identificar a rede e apenas o último indica o endereço

do host dentro dela.

Na internet, os endereços IP são divididos em três faixas, que se diferenciam pela máscara utilizada. Os endereços de classe A começam com números de 1 a 126 (como, por exemplo, "62.34.32.1") e utilizam máscara 255.0.0.0. Cada faixa de endereços classe A é composta de mais de 16 milhões de endereços, mas como existem apenas 126 delas, elas são reservadas para o uso de grandes empresas e órgãos governamentais.

Em seguida temos os endereços de classe B, que abrangem os endereços iniciados com de 128 a 191. Eles utilizam máscara 255.255.0.0, o que permite a existência de um número muito maior de faixas, cada uma composta por 65 mil endereços.

Finalmente temos o "terceiro mundo", que são as faixas de endereços classe C, que abrangem os endereços que começam com de 192 a 223. Elas são mais numerosas, pois utilizam máscara 255.255.255.0, mas em compensação cada faixa de classe C é composta por apenas 254 endereços. Com a escassez de endereços válidos, as faixas de classe C são praticamente as únicas que ainda podem ser obtidas hoje em dia.

Existe ainda a possibilidade de utilizar máscaras complexas para dividir uma faixa de endereços de classe A, B ou C em faixas menores e independentes. Esta possibilidade é usada ao extremo pelas empresas de hospedagem, que dividem faixas de endereços de classe A ou B em diversas faixas menores, com apenas 4 ou 8 endereços, que são atribuídas aos servidores dedicados hospedados em seus data-centers.

Ao usar a máscara 255.255.255.248, por exemplo, apenas 3 bits do endereço são reservados ao endereçamento dos hosts (convertendo 255.255.255.248 para binário, você teria 11111111.11111111.11111111.11111000), permitindo que a empresa de hospedagem divida uma faixa de endereços classe A (16 milhões de hosts) em 2.080.768 pequenas redes, uma para cada servidor dedicado que for locado.

Três bits permitem 8 combinações, mas o primeiro e o último endereço são reservados ao endereço da rede e ao endereço de broadcast, fazendo com que apenas 6 endereços possam realmente ser utilizados. Destes, mais um é sacrificado, pois é atribuído ao gateway (sem o gateway o servidor não acessa a internet), de forma que no final apenas 5 endereços ficam realmente disponíveis.

Ao locar um servidor dedicado, você precisa de uma faixa de endereços inteira para poder configurar o DNS reverso, um pré-requisito para que seus e-mails não sejam rotulados como spam por outros servidores.

Ao registrar um domínio, você precisa fornecer os endereços de dois servidores DNS, que responderão por ele. Ao invés de ter dois servidores, você pode

utilizar outro dos seus 5 endereços disponíveis para criar um alias (apelido) para a placa de rede do seu servidor dedicado e assim poder configurá-lo para responder simultaneamente como servidor DNS primário e secundário, eliminando a necessidade de utilizar dois servidores. Novamente, esta configuração é possível apenas caso o servidor possua uma faixa de endereços própria.

No final, a configuração de rede de um servidor dedicado acaba sendo algo similar a isto:

Endereço IP: 72.232.35.106
Máscara: 255.255.255.248
Gateway: 72.232.35.105
Endereço da rede: 72.232.35.104
Endereço de broadcast: 72.232.35.111
Alias da placa de rede (para o DNS secundário): 72.232.35.107
Endereços vagos: 72.232.35.108, 72.232.35.109 e 72.232.35.110

Como se não bastasse, é possível ainda instalar o VMware Server, Xen, ou outro sistema de virtualização e aproveitar estes três endereços vagos para criar três máquinas virtuais, cada uma com seu próprio endereço IP e configurada como se fosse um servidor separado. O princípio é o mesmo que ao rodar um segundo sistema operacional dentro do VMware Player no seu micro de trabalho, a única grande diferença é que neste caso toda a configuração é feita remotamente.

7. IPV6

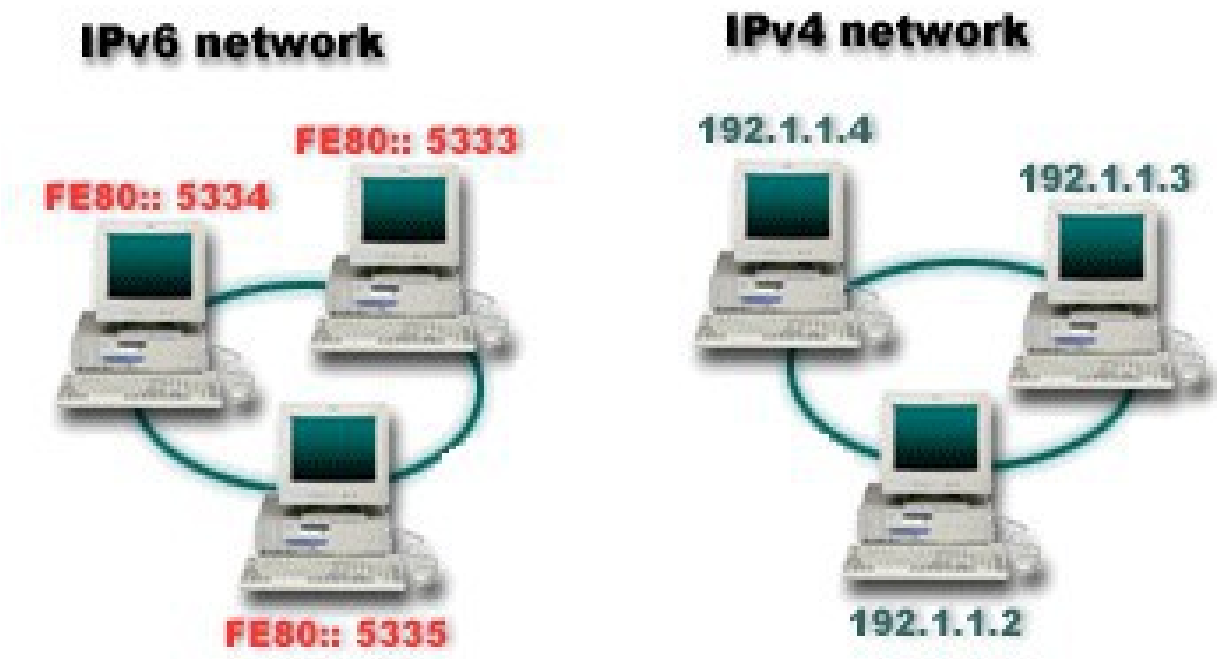
Em seguida temos a questão do **IPV6**, que é uma fonte frequente de dúvidas. Ele é uma evolução do padrão de endereçamento atual onde, ao invés de endereços de 32 bits, são usados endereços de 128 bits. O número de endereços disponíveis no IPV6 é simplesmente absurdo; seria o número 340.282.366.920 seguido por mais 27 casas decimais. Tudo isso para prevenir a possibilidade de, em um futuro distante, ser necessária uma nova migração.

Por serem muito mais longos, os endereços IPV6 são representados através de caracteres em hexa. No total temos 32 caracteres, organizados em oito quartetos e separados separados por dois pontos.

No conjunto hexadecimal, cada caracter representa 4 bits (16 combinações). Devido a isso, temos, além dos números de 0 a 9, também os caracteres A, B, C, D, E e F, que representariam (respectivamente), os números 10, 11, 12, 13, 14 e 15. Um exemplo de endereço IPV6, válido na internet, seria "2001:bce4:5641:3412:341:45ae:fe32:65".

Um atenuante para esta complexidade dos endereços IPV6 é que eles podem

ser abreviados de diversas formas. Graças a isso, os endereços IPV6 podem acabar sendo incrivelmente compactos, como "::1" ou "fee::1".



Em primeiro lugar, todos os zeros à esquerda dentro dos quartetos podem ser omitidos. Por exemplo, ao invés de escrever "0341", você pode escrever apenas "341"; ao invés de "0001" apenas "1" e, ao invés de "0000" apenas "0", sem que o significado seja alterado. É por isso que muitos quartetos dentro dos endereços IPV6 podem ter apenas 3, 2 ou mesmo um único dígito. Os demais são zeros à esquerda que foram omitidos.

É muito comum que os endereços IPV6 incluam seqüências de números 0, já que atualmente poucos endereços são usados. Graças a isso, o endereço "2001:bce4:0:0:0:0:0:1" poderia ser abreviado para apenas "2001:bce4::1", omitimos todo o trecho central "0:0:0:0:0".

Ao usar o endereço, o sistema sabe que entre o "2001:bce4:" e o ":1" existem apenas zeros e faz a conversão internamente, sem problema algum.

O suporte a IPV6 está presente em todas as distribuições Linux atuais, assim como no Windows XP SP2 e no Vista. Uma vez que você entende como os endereços IPV6 são estruturados e que uma mesma interface de rede pode ter ao mesmo tempo um endereço IPV4 e um IPV6 (respondendo em ambos), não existe nada de exotérico em atribuir endereços IPV6 para os micros da sua rede e começar a testar o novo sistema.

Assim como no IPV4, os endereços IPV6 são divididos em dois blocos. Os primeiros 64 bits (os 4 primeiros quartetos) identificam a rede, enquanto os

últimos 64 bits identificam o host. No endereço "2001:bce4:0:0:0:0:0:1", por exemplo, temos a rede "2001:bce4:0:0" e o host "0:0:0:0:1" dentro dela.

Ao configurar endereços dentro de uma mesma rede, existem duas opções. A primeira seria simplesmente usar endereços seqüenciais, como " 2001:bce4::1", " 2001:bce4::2", "2001:bce4::3" e assim por diante. Nada de errado com isso. A segunda seria seguir a sugestão do IEFT e usar os endereços MAC das placas de rede para atribuir os endereços dos hosts. É justamente isso que é feito ao utilizar a atribuição automática de endereços no IPV6.

Digamos que o endereço da rede é "2001:bce4:0:0:" e o endereço MAC do micro é "00:16:F2:FE:34:E1". Como você pode ver, o endereço MAC contém apenas 12 dígitos hexa, enquanto no IPV6 a parte do host contém 16 dígitos. Está em estudo uma expansão dos endereços MAC das placas de rede, que passariam a ter 16 dígitos, mas, enquanto isso não é colocado em prática, usamos uma regra simples para converter os endereços de 12 dígitos atuais em endereços de 16 dígitos, adicionando um "ffff" entre o sexto e sétimo dígito do endereço.

O endereço "00:16:F2:FE:34:E1", viraria então "0016:f2**ff:ff**fe:34e1". Como viu, os 12 dígitos originais continuam os mesmos (apenas converti para minúsculas). São apenas adicionados os 4 dígitos no meio.

Adicionando o endereço da rede, o endereço IPV6 completo deste micro seria "2001:bce4:0:0:0016:f2ff:fffe:34e1", o que poderia ser abreviado para apenas "2001:bce4::0016:f2ff:fffe:34e1".

O IPV6 também oferece um recurso de compatibilidade com endereços IPV4, permitindo que você continue utilizando os mesmos endereços ao migrar para ele. Neste caso, você usaria o endereço "::FFFF:" seguido pelo endereço IPV4 usado atualmente, como em:

::FFFF:192.168.0.1

Por estranho que possa parecer, este é um endereço IPV6 completamente válido, que você pode usar para todos os fins.

Outra mudança é que no IPV6 você pode atribuir diversos endereços para o mesmo micro. Isto também era possível no IPV4 utilizando-se alises para a placa de rede, mas no caso do IPV6, este passou a ser um recurso nativo. Graças a isso, o mesmo micro pode ser acessado tanto através do endereço "2001:bce4:5641:3412:341:45ae:fe32:65" (por exemplo), quanto pelo ::FFFF:192.168.0.1 (pelos micros da rede local), sem que você precise usar duas placas de rede.

É possível também adicionar um endereço IPV6 a um micro já configurado com um endereço IPV4, na maioria dos casos sem nem mesmo precisar derrubar a

rede. Neste caso, ele continua respondendo de forma normal no endereço IPV4 antigo, mas passa a responder também no endereço IPV6. Um dos objetivos do novo sistema é justamente manter compatibilidade com o antigo, já que muitos sistemas provavelmente nunca serão atualizados.

Imagine, por exemplo, que uma migração em larga escala para o IPV6 está ocorrendo. A maior parte da internet já utiliza o novo sistema, mas seu provedor de acesso ainda oferece suporte apenas a endereços IPV4.

Prevendo situações assim, o IPV6 oferece suporte ao tunelamento de pacotes IPV6 através de redes IPV4. Ao perceber que os pacotes IPV6 precisarão passar por uma rede IPV4, o roteador empacota os pacotes IPV6, colocando-os dentro de pacotes IPV4, de forma que eles sejam roteados normalmente através da rede IPV4. Do outro lado da conexão teríamos outro roteador IPV6, que se encarregaria de remover o cabeçalho IPV4 dos pacotes, obtendo novamente os pacotes IPV6 originais.

Este sistema permite também que sistemas configurados com endereços IPV4, continuem acessando a internet normalmente, mesmo depois que a migração ocorrer. Imagine o caso de micros rodando o Windows 95/98, por exemplo, sistemas que provavelmente nunca serão atualizados.

Fonte: http://www.hardware.com.br/tutoriais/resumo-redes/pagina7.html