Faixas de endereços IP, CIDR e máscaras de tamanho variável

Referencia: Guia do Hardware - http://www.guiadohardware.net/tutoriais/endereco-ip-cidr/

Introdução

O endereçamento IP é sempre 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 se popularizar a partir de 2012 ou 2014, 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 (cobrindo as 256 possibilidades permitidas por 8 bits), como "200.156.23.43" ou "64.245.32.11". Os grupos de 8 bits que formam o endereço são chamados de "octetos", o que dá origem a expressões como "o primeiro octeto do endereço". De qualquer forma, a divisão dos endereços em octetos e o uso de números decimais serve apenas para facilitar a configuração para nós, seres humanos. Quando processados, os endereços são transformados em binários, como "11001000100110010001011100101011".

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

No caso dos endereços válidos na Internet, as regras são mais estritas. A entidade global responsável pelo registro e atribuição dos endereços é a IANA (http://www.iana.org/), que delega faixas de endereços às RIRs (Regional Internet Registries), entidades menores, que ficam responsáveis por delegar os endereços regionalmente. Nos EUA, por exemplo, a entidade responsável é a ARIN (http://www.arin.net/) e no Brasil é a LACNIC (http://www.lacnic.net/pt/). Estas entidades são diferentes das responsáveis pelo registro de domínios, como o Registro.br.

As operadoras, carriers e provedores de acesso pagam uma taxa anual à RIR responsável, 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. Note que estes valores são apenas as taxas pelo uso dos endereços, não incluem o custo dos links, naturalmente.

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 e 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. Nesse 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. Esse 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.

O servidor DHCP incluído no ICS do Windows utiliza uma configuração fixa, fornecendo endereços dentro da faixa "192.168.0.x", mas ao utilizar um servidor Linux, ou qualquer outro dispositivo de rede que ofereça um servidor DHCP com mais recursos, você pode escolher qualquer faixa de endereços e também configurar uma "zona" para os

endereços do servidor DHCP, permitindo que você tenha micros com IPs fixos e IPs dinâmicos (fornecidos pelo servidor DHCP) na mesma rede. Nesse caso, você poderia ter uma configuração como a seguinte:

192.168.0.1: Gateway da rede
192.168.0.2: Ponto de acesso wireless
192.168.0.3: Servidor de arquivos para a rede interna
192.168.0.4 até 192.168.0.99: Micros da rede configurados com IP fixo
192.168.0.100 até 192.168.0.254: Faixa de endereços atribuída pelo servidor DHCP

Veja que usar uma das faixas de endereços reservadas não impede que os PCs da sua rede possam acessar a Internet. Embora eles não acessem diretamente, por não possuírem IPs válidos, eles podem acessar através de uma conexão compartilhada via NAT ou de um servidor proxy. É possível inclusive configurar o firewall, ativo no gateway da rede para redirecionar portas (port forwarding) para micros dentro da rede local, de forma que eles possam ser acessados remotamente. O servidor nesse caso "empresta" uma porta, ou uma determinada faixa de portas para o endereço especificado dentro da rede local. Quando alguém da Internet acessa uma das portas encaminhadas no servidor, é automaticamente redirecionado para a porta correspondente no micro da rede interna, de forma transparente.

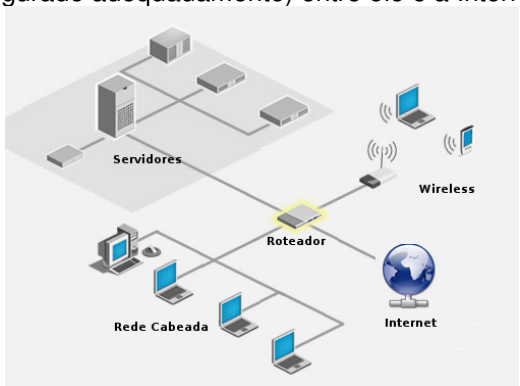
O uso dos endereços de rede local tem aliviado muito o problema da falta de endereços IP válidos, pois uma quantidade enorme de empresas e usuários domésticos, que originalmente precisariam de uma faixa de endereços completa para colocar todos os seus micros na Internet, pode sobreviver com um único IP válido (compartilhado via NAT entre todos os micros da rede). Em muitos casos, mesmo provedores de acesso chegam a vender conexões com endereços de rede interna nos planos mais baratos, como, por exemplo, alguns planos de acesso via rádio, onde um roteador com um IP válido distribui endereços de rede interna (conexão compartilhada) para os assinantes.

Embora seja possível, pelo menos em teoria, ter redes com até 24 milhões de PCs, usando a faixa de endereços de rede local 10.x.x.x, na prática é raro encontrar segmentos de rede com mais de 100 ou 200 micros. Conforme a rede cresce, o desempenho acaba caindo, pois, mesmo ao utilizar um switch, sempre são transmitidos alguns pacotes de broadcast (que são retransmitidos a todos os micros do segmento). A solução nesse caso é dividir a rede em segmentos separados, interligados por um roteador.

Em uma empresa, poderíamos (por exemplo) 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 interfaces de rede (uma 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. Quando falo em "roteador", tenha em mente que você pode perfeitamente usar um servidor Linux com diversas placas de rede.

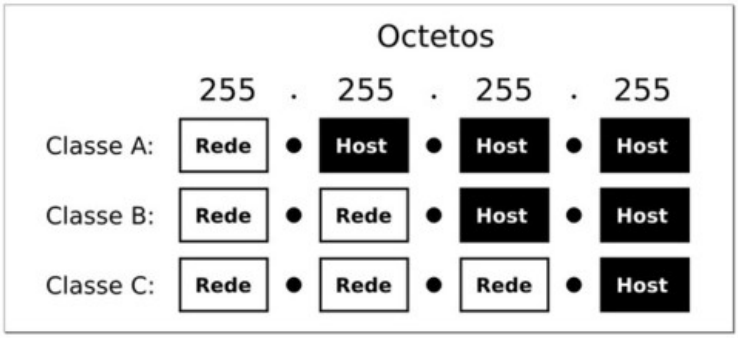
Com relação à proteção da rede contra acessos provenientes da Internet, você poderia tanto configurar o próprio firewall ativo no roteador, de forma a proteger os micros da rede local, quanto instalar um firewall dedicado (que pode ser um PC com duas placas de rede, configurado adequadamente) entre ele e a Internet:



Voltando à questão dos endereços: inicialmente os endereços IP foram divididos em classes, denominadas A, B, C, D e E. Destas, apenas as classe A, B e C são realmente usadas, já que as classes D e E são reservadas para recursos experimentais e expansões futuras.

Cada classe reserva um número diferente de octetos para o endereçamento da rede. Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C temos os três primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos hosts dentro dela.

O que diferencia uma classe de endereços da outra é o valor do primeiro octeto. Se for um número entre 1 e 126 temos um endereço de classe A. Se o valor do primeiro octeto for um número entre 128 e 191, então temos um endereço de classe B e, finalmente, caso o primeiro octeto seja um número entre 192 e 223, temos um endereço de classe C.



Ao configurar uma rede local, você pode escolher a classe de endereços mais adequada. Para uma pequena rede, uma faixa de endereços de classe C (como a tradicional 192.168.0.x com máscara 255.255.255.0) é mais apropriada, pois você precisa se preocupar em configurar apenas o último octeto do endereço ao atribuir os endereços. Em uma rede de maior porte, com mais de 254 micros, passa a ser necessário usar um endereço de classe B (com máscara 255.255.0.0), onde podemos usar diferentes combinações de números nos dois últimos octetos, permitindo um total de 65.534 endereços.

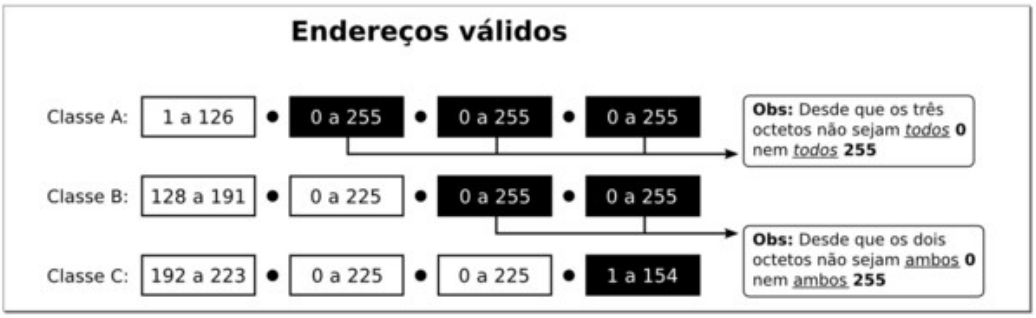
Continuando, temos a configuração das máscaras de sub-rede, que servem para indicar em que ponto termina a identificação da rede e começa a identificação do host. Ao usar a máscara "255.255.255.0", por exemplo, indicamos que os três primeiros números (ou octetos) do endereço servem para identificar a rede e apenas o último indica o endereço do host dentro dela.

Como vimos, na divisão original (que não é mais usada hoje em dia, como veremos a seguir) os endereços das três faixas eram diferenciados pelo número usado no primeiro octeto. Os endereços de classe A começavam com números de 1 a 126 (como, por exemplo, "62.34.32.1"), com máscara 255.0.0.0. Cada faixa de endereços classe A era composta de mais de 16 milhões de endereços mas, como existiam apenas 126 delas, elas eram reservadas para o uso de grandes empresas e órgãos governamentais.

Em seguida tínhamos os endereços de classe B, que englobavam os endereços iniciados com de 128 a 191, com máscara 255.255.0.0 (criando faixas compostas por 65 mil endereços) e o "terceiro mundo", que eram as faixas de endereços classe C. Elas abrangiam os endereços que começam com números de 192 a 223. As faixas de endereços de classe C eram mais numerosas, pois utilizavam máscara 255.255.255.0, mas, em compensação, cada faixa de classe C era composta por apenas 254 endereços. Veja alguns exemplos:

Ex. de endereço IP	Classe do endereço	Parte referente à rede	Parte referente ao host	Máscara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

Ao alugar um backbone vinculado a uma faixa de endereços classe C, por exemplo, você receberia uma faixa de endereços como "203.107.171.x", onde o "203.107.171" é o endereço de sua rede dentro da Internet, e o "x" é a faixa de 254 endereços que você pode usar para identificar seus servidores e os hosts dentro da rede. Na ilustração temos um resumo das regras para endereços TCP/IP válidos:



Como você pode notar no diagrama, nem todas as combinações de endereços são permitidas, pois o primeiro endereço (0) é reservado à identificação da rede, enquanto o último (255) é reservado ao endereço de broadcast, que é usado quando alguma estação precisa enviar um pacote simultaneamente para todos os micros dentro do segmento de rede.

Os pacotes de broadcast são usados para, por exemplo, configurar a rede via DHCP e localizar os compartilhamentos de arquivos dentro de uma rede Windows (usando o antigo protocolo NetBIOS). Mesmo os switches e hub-switches detectam os pacotes de broadcast e os transmitem simultaneamente para todas as portas. A desvantagem é que, se usados extensivamente, eles prejudicam o desempenho da rede.

Veja alguns exemplos de endereços **inválidos**:

0.xxx.xxx.xxx: Nenhum endereço IP pode começar com zero, pois ele é usado para o endereço da rede. A única situação em que um endereço começado com zero é usado, é quando um servidor DHCP responde à requisição da estação. Como ela ainda não possui um endereço definido, o pacote do servidor é endereçado ao endereço MAC da estação e ao endereço IP "0.0.0.0", o que faz com que o switch o envie para todos os micros da rede.
127.xxx.xxx.xxx: Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes e para a interface de loopback. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1, ele acabará usando o servidor instalado na sua própria máquina. O mesmo acontece ao tentar acessar o endereço 127.0.0.1 no navegador: você vai cair em um servidor web habilitado na sua máquina. Além de testes em geral, a interface de loopback é usada para comunicação entre diversos programas, sobretudo no Linux e outros sistemas Unix.
255.xxx.xxx.xxx, xxx.255.255.255, xxx.xxx.255.255: Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço, pois estes endereços são usados para enviar pacotes de broadcast. Outras combinações são permitidas, como em 65.34.255.197 (em um endereço de classe A) ou em 165.32.255.78 (endereço de classe B).
xxx.0.0.0, xxx.xxx.0.0: Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço, pois estes endereços são reservados para o endereço da rede. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B).
xxx.xxx.xxx.255, xxx.xxx.xxx.0: Nenhum endereço de classe C pode terminar com 0 ou com 255, pois, como já vimos, um host não pode ser representado apenas por valores 0 ou 255, já que eles são usados para o envio de pacotes de broadcast.

Dentro de redes locais, é possível usar máscaras diferentes para utilizar os endereços IP disponíveis de formas diferentes das padrão. O importante neste caso é que todos os micros da rede sejam configurados com a mesma máscara, caso contrário você terá problemas de conectividade, já que tecnicamente os micros estarão em redes diferentes.

Um exemplo comum é o uso da faixa de endereços 192.168.0.x para redes locais. Originalmente, esta é uma faixa de endereços classe C e por isso a máscara padrão é 255.255.255.0. Mesmo assim, muita gente prefere usar a máscara 255.255.0.0, o que permite mudar os dois últimos octetos (192.168.x.x). Neste caso, você poderia ter dois micros, um com o IP "192.168.2.45" e o outro com o IP "192.168.34.65" e ambos se enxergariam perfeitamente, pois entenderiam que fazem parte da mesma rede. Não existe problema em fazer isso, desde que você use a mesma máscara em todos os micros da rede.

Classes especiais - http://pt.wikipedia.org/wiki/Endere%C3%A7o_IP

Existem classes especiais na Internet que não são consideradas públicas, não são consideradas como endereçáveis, são reservadas, por exemplo, para a comunicação com uma rede privada ou com o computador local ("localhost").

Blocos de Endereços Reservados

CIDR Bloco de Endereços	Descrição	Referência
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)	RFC 1700
10.0.0.0/8	Rede Privada	RFC 1918
14.0.0.0/8	Rede Pública	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Localhost	RFC 3330
128.0.0.0/16	Reservado (IANA)	RFC 3330
169.254.0.0/16	Zeroconf	RFC 3927
172.16.0.0/12	Rede Privada	RFC 1918
191.255.0.0/16	Reservado (IANA)	RFC 3330
192.0.2.0/24	Documentação	RFC 3330
192.88.99.0/24	IPv6 para IPv4	RFC 3068
192.168.0.0/16	Rede Privada	RFC 1918
198.18.0.0/15	Teste de benchmark de redes	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multicasts (antiga rede Classe D)	RFC 3171
240.0.0.0/4	Reservado (antiga rede Classe E)	RFC 1700
255.255.255.255	Broadcast	