Endereçamento IP

Luiz Arthur

Endereçamento IP

Um sistema de comunicação permite que **qualquer host** se **comunique** com **qualquer host**. E para tornar o sistema de comunicação universal, ele precisa de um método aceito globalmente a fim de identificar cada computador que se conecta a ele. Em redes TCP/IP isto é possível usando-se o endereçamento IP.

O protocolo TCP/IP é roteável, isto é, ele foi criado pensando-se na interligação de diversas redes. Onde **podemos ter diversos caminhos interligando um transmissor e o receptor**. Isso possibilitou a criação da rede mundial de computadores (Internet).

Para isso o TCP/IP utiliza um esquema de **endereçamento lógico** chamado de endereçamento IP. Onde em cada rede TCP/IP cada dispositivo conectado em rede necessita usar pelo menos um endereço IP. Então o endereço **IP permite identificar o dispositivo e a rede na qual ele pertence**.

Para interligar diversas redes faz-se necessário à figura de um ***roteador***. O roteador utiliza informações contidas nos pacotes para realizar a entrega dos pacotes aos seus respectivos destinos, então uma rota é um caminho a ser seguido para entrega de um dado pacote ao seu destino.

Esse esquema de entrega de pacotes é feito facilmente pelo roteador porque os pacotes de dados possuem o endereço IP do computador de destino e de origem. Neste endereço IP há a informação de qual a rede o pacote deve ser entregue.

Endereçamento IP

Formato do endereço IPv4

Cada host em uma rede TCP/IP recebe um endereço de **32 bits** que é usado em toda a comunicação com esse host.

Exemplo:

00000001 . 00000010 . 00000011 . 00000100

Porém o endereço IPv4 de 32 bits, que daqui para frente só chamaremos de endereço IP, normalmente é representado em decimal em forma de quatro números de oito bits separados por um ponto, no formato a.b.c.d. assim, o menor endereços IP possível é **0.0.0.0** e o maior, **255.255.255.255**. Então seguindo o exemplo anterior, o IP seria:

1 . 2 . 3 . 4

O endereçamento IP possui basicamente duas partes uma que indica a rede e outra que indica o dispositivo dentro desta rede.

Uma rede TCP/IP usando **o IPv4 pode ter até 4.294.967.296 endereços IP** ou 2^32. Teoricamente porque existem alguns números de IP, que são reservados e não podem ser usados, nós veremos isto depois.

Endereçamento IP

Luiz Arthur

Considere um endereço IP muito comum em binário e em decimal respectivamente:

11000000.10101000.00000000.00000001
192.168.0.1

Um endereço IP tem quatro números separados por pontos. Esse tipo de sistema de notação é chamado de *notação decimal separada por pontos*.

O conjunto de quatro números é chamado de *octeto*, uma vez que eles na verdade representam um número binário de 8 bits ou 1 byte. Conseqüentemente, o valor decimal máximo para cada um dos quatro números em um endereço IP é 255, e não 999.

O *valor binário de bit* (*binary bit value – BBV*) permite facilmente converter os bits em um valor decimal comum, pois é só somar os números da coluna BBV quando o bit um estiver ativo, caso nenhum bit estiver ativo (todos em zero) o número em decimal é zero. Então no exemplo, o 1˚ octeto temos de somar 128+64=192, 2˚ octeto 128+32+8=168, 3˚ octeto não soma nada pois é tudo zero então o decimal é 0 e no 4˚ octeto soma-se apenas 1 então o valor em decimal é 1, o que forma o IP: 192.168.0.1

Tabela de conversão de binário para decimal									
BBV	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	Decimal
1 octeto	1	1	0	0	0	0	0	0	192
2 octeto	1	0	1	0	1	0	0	0	168
3 octeto	0	0	0	0	0	0	0	0	0
4 octeto	0	0	0	0	0	0	0	1	1

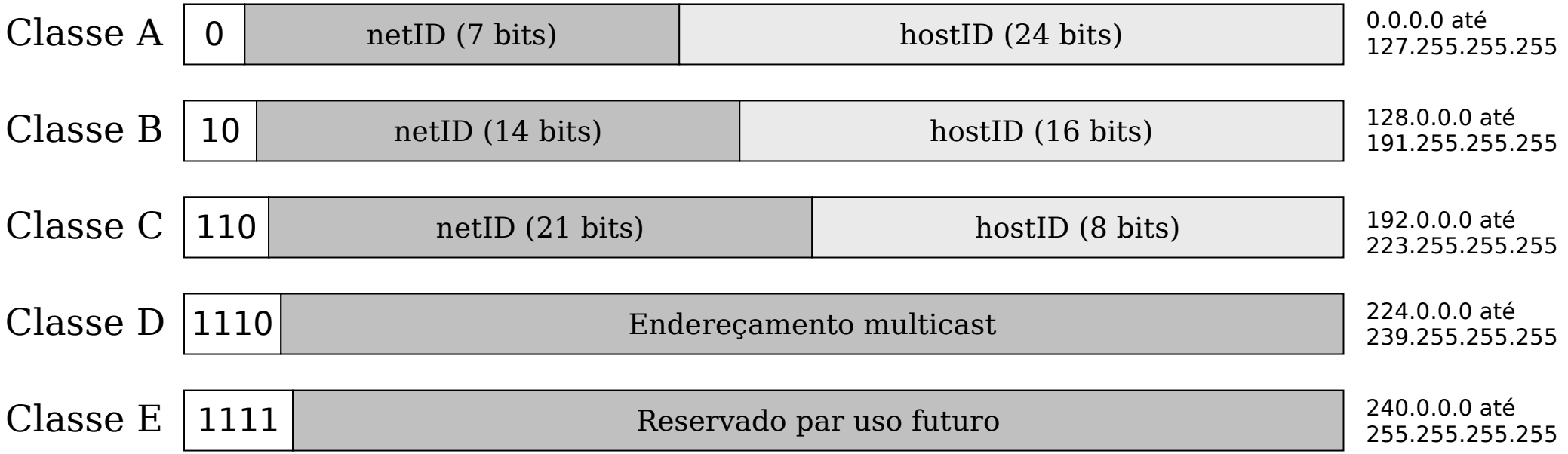
Endereçamento IP

Luiz Arthur

O esquema original de endereçamento IP Classful

Conceitualmente, cada endereço é um par (netID e hostID), em que netID identifica uma rede e hostID identifica um host nessa rede.

Para facilitar a distribuição dos endereços IP em redes e hosts, foram especificadas cinco classes de endereços IP, no qual cada endereço é considerado como auto-identificável, pois o limite entre prefixo e sufixo pode ser calculado a partir do endereço isolado, sem referência a informações externas. Em particular, a classe de um endereço pode ser determinada a partir dos três bits de alta ordem.



Em suma apenas as classes A, B e C são usadas na prática.

Endereçamento IP

Os números de **redes na Internet são atribuídos por uma corporação sem fins lucrativos** chamada ICANN (Internet Corporation for Assigned Names and Numbers) para evitar conflitos. Por sua vez, a ICANN tem partes delegadas do espaço de endereços para diversas autoridades regionais, e estas fazem a doação de endereços IP a ISPs e outras empresas.

Na Internet, cada host e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host. A combinação é exclusiva: em princípio, **duas máquinas na Internet nunca têm o mesmo endereço IP**. Todos os endereços IP têm 32 bits e são usados nos campos Source address e Destination address dos pacotes IP. É importante observar que um endereço IP não se refere realmente a um host. Na verdade, ele se refere a uma interface de rede; assim, se um host estiver em duas redes, ele precisará ter dois endereços IP. Porém, na prática, a maioria dos hosts está em uma única rede e, portanto, só tem um endereço IP.

Existe situações em que um computador convencional tem duas ou mais conexões físicas de rede, esses computadores são conhecidos como hosts **multihomed**, no qual cada uma das conexões de rede da máquina precisa receber um endereço.

Como os endereços IP codificam uma rede quanto um host nessa rede, um **endereço não especifica um computador individual, mas uma conexão com uma rede.**

Endereço IP de rede e de broadcast

A principal vantagem do endereço IP é que ele possibilita um encaminhamento eficiente entre origem e destino. Outra vantagem é que os **endereços IPs podem se referir a redes e também a hosts**.

Por convenção, o **hostID com todos os bits marcados com 0** nunca endereça um host individual, pois entes **representa uma rede**. Assim, os endereços um endereço IP pode simbolizar a rede.

Da mesma forma, outra vantagem do endereço IP é a representação de um endereço de broadcast que é usado quando se deseja enviar uma mensagem para todas as máquinas de uma dada rede. De acordo com o padrão, qualquer endereço com o **hostID consistindo em todos os bits marcados em 1 é reservado para o broadcast (Broadcast direcionado)**. Sem o endereço de broadcast caso alguma máquina precise enviar uma mesma mensagem para todos na rede, esta deveria enviar uma a uma, no caso de uma rede classe A, serão aproximadamente 16 milhões de mensagens iguais, já com o uso de broadcast será apenas uma mensagem.

O endereço IP **0.0.0.0 é usado pelos hosts quando eles estão sendo inicializados**. Os endereços IP que têm 0 como número de rede se referem à rede atual. Esses endereços permitem que as máquinas façam referência às suas próprias redes sem saber seu número (mas elas precisam conhecer sua classe para saber quantos zeros devem ser incluídos).

O **endereço que consiste apenas em dígitos 1 permite a difusão na rede local (Broadcast limitado)**, que em geral é uma LAN. Os endereços com um número de rede apropriado e que tiverem apenas valores 1 no campo de host permitem que as máquinas enviem pacotes de difusão para LANs distantes (Broadcast direcionado), em qualquer parte da Internet (embora muitos administradores de redes desativem esse recurso).

Endereço de loopback

Todos os endereços com o formato **127.xx.yy.zz são reservados para teste de loopback e para comunicação entre processos no computador local**. Os pacotes enviados para esse endereço não são transmitidos; eles são processados localmente e tratados como pacotes de entrada. Isso permite que os pacotes sejam enviados para a rede local, sem que o transmissor saiba seu número. Um host ou um roteador nunca deverá rotear pacotes com endereços 127.xx.yy.zz, assim esses não são roteáveis em lugar algum e ficam restrito ao próprio host.

Resumo para endereços especiais

- Todos os bits em 0: Endereço de origem inicial;
- Todos os bits em 1: Broadcast limitado (rede local);
- netID e os bits de hostID em 1: Broadcast direcionado para a rede;
- netID e os birs de hostID em 0: Endereço de rede;
- 127.xx.yy.zz: endereço de loopback.

Sub-rede

No esquema de endereçamento IP original **Classful**, **cada rede física recebe um endereço de rede** exclusivo; cada host em uma rede tem o endereço de rede como um prefixo do endereço individual do host.

A principal **vantagem** de dividir o endereço IP em duas partes surge do tamanho das tabelas de roteamento exigidas nos roteadores. Em vez de manter uma entrada de roteamento por host de destino, um roteador pode **manter uma entrada de roteamento por rede** e examinar apenas a parte de rede de um endereço de destino quando tomar decisões de encaminhamento de pacotes.

O esquema de endereçamento IP original **classful** parece tratar de todas as possibilidades, mas **possui um pequeno problema**. Como ele foi inventado no mundo dos mainframes caros, os projetistas não anteciparam o crescimento da Internet, que hoje cresce assombrosamente, por fim os endereços **IPv4 parecem estar findados a se esgotarem rapidamente**, por isto já existe o IPv6 que pode atribuir mais de 1500 IPs por metro quadrado da terra.

Proxy ARP

Uma maneira de tentar amenizar o problema de faltas de endereços IPs é com o proxy ARP, que é uma técnica que visa manter um único prefixo de rede para mais de uma rede física, este só se aplica a redes que usam ARP para vincular endereços de redes a endereços físicos.

A principal **desvantagem** do **proxy ARP** é que ele **não funciona para as redes** a menos que utilizem o ARP para tradução de endereços. Além do mais, ele não generaliza para uma topologia de rede mais **complexa**, nem tem suporte para uma forma razoável de encaminhamento. De fato, a maioria das implementações de proxy conta com gerentes para manter tabelas de máquinas e endereços manualmente, tornando-o tanto demorado quanto passível de erros, por isto está técnica é pouco usada em larga escala.

Sub-rede

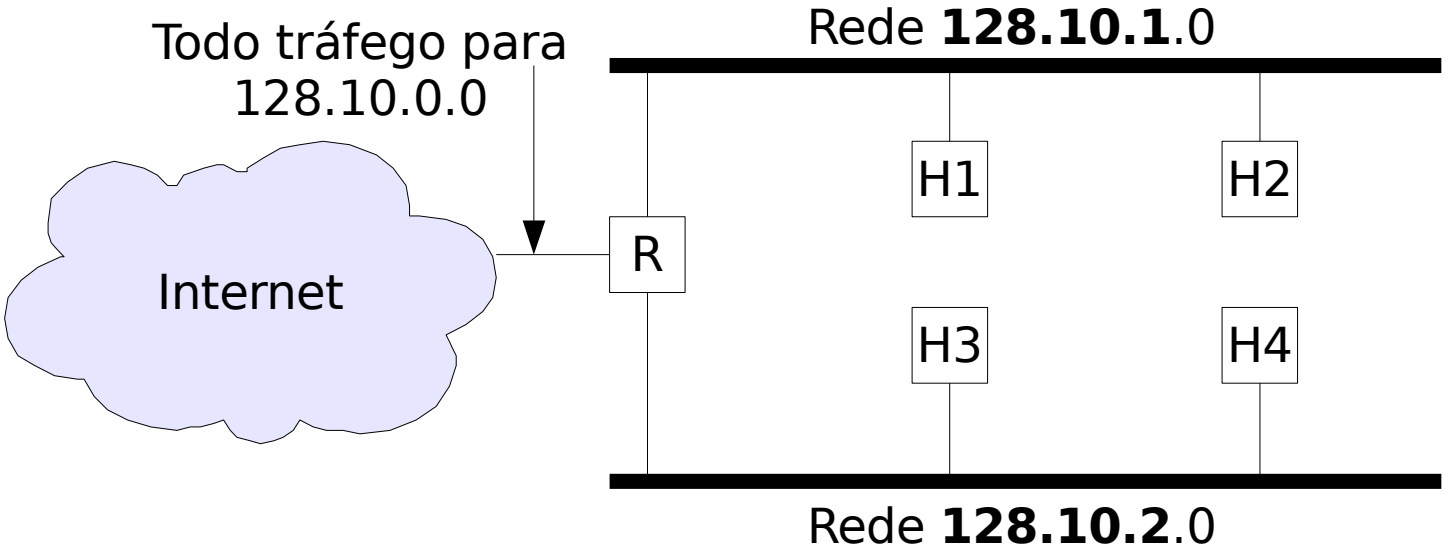
Uma segunda técnica que permite que um único endereço de rede se espalhe por várias redes físicas é chamada endereçamento de sub-rede, encaminhamento de sub-rede ou subdivisão de redes. Está é a técnica mais genérica e padrão para a subdivisão de redes, na verdade **a subdivisão de redes é parte obrigatória do endereçamento IP**.

Para entender a subdivisão de redes, é importante observar que os sites individuais têm liberdade de modificar endereços e rotas desde que as modificações permaneçam invisíveis a outros sites, então:

- Todos os hosts e roteadores no site concordem em honrar o esquema de endereçamento do site;
- Outros sites na Internet possam tratar dos endereços como um prefixo de rede e um sufixo de host.

Endereçamento IP

O modo mais fácil de entender o endereçamento de sub-rede é imaginar que um site possui um único endereço de rede, porém mas duas ou mais redes físicas. Somente os roteadores locais sabem que existem várias redes físicas e como encaminhar o tráfego entre elas; todos os outros roteadores na Internet encaminham tráfego como se houvesse uma única rede física no site.



Ao usar o **endereço de sub-rede**, pensamos em um endereço IP de 32 bits como tendo uma parte de **Rede e uma parte de Rede Local**, em que a parte de Rede identifica um site, possivelmente com várias redes físicas, e a parte local identifica uma rede física **e host nesse site**. O resultado é um endereçamento hierárquico que leva ao roteamento hierárquico correspondente.

Implementação de sub-redes com máscaras

A tecnologia de sub-rede facilita a configuração de tamanho fixo ou variável. O padrão especifica que uma **máscara de 32 bits**, tal como o endereço IP, seja **usada para especificar a divisão de sub-rede**.

Assim, um site usando o endereçamento de sub-rede precisa escolher uma máscara de sub-rede de 32 bits para cada rede.

Os bits **na máscara** de sub-rede são definidos como **1** se as máquinas na **rede** tratarem o bit correspondente no endereço IP como parte do prefixo de sub-rede, e **0** se tratarem o bit como parte do **identificador de host**. Ou seja, é necessário casar bit-a-bit o endereço IP e a máscara de sub-rede. Exemplo de uma máscara:

IP Host	:	**11000000**	.	**10101000**	.	**00000000**	. *00000001*
Mascara	:	**11111111**	.	**11111111**	.	**11111111**	. *00000000*

Esta máscara apresentada anteriormente em decimal, pela tabela BBV, seria 255.255.255.0 é diz que os três primeiros octetos do IP representam **rede** e apenas o último octeto representa *hosts*.

O endereçamento de sub-rede não restringe a máscara de bits contíguos do endereço, embora seja altamente recomendado não fazer uso deste artifício, pois ela complica a atribuição de endereços e complica a tabela de roteamento.

Para ver como as sub-redes funcionam, é necessário explicar **como os pacotes IP são processados em um roteador**. Cada roteador tem uma tabela que lista algum número de endereços IP (rede, 0) e uma série de endereços IP (para essa rede ou host). O primeiro tipo informa como chegar a redes distantes. O segundo, como chegar a hosts locais. Associadas a essa tabela estão a interface de rede usada para alcançar o destino e algumas outras informações.

Quando um **pacote IP é recebido**, seu endereço de destino é procurado na **tabela de roteamento**. Se o destino for uma rede distante, o pacote será encaminhado para o **próximo roteador** da interface fornecida na tabela. Caso o destino seja um **host local** (por exemplo, na LAN do roteador), o pacote será enviado diretamente para lá. Se a rede não estiver presente, o pacote será enviado para um roteador predefinido que tenha tabelas maiores (**roteador padrão/default**). Esse algoritmo significa que cada roteador só precisa controlar as outras redes e hosts locais, deixando de lado os pares (rede, host), o que reduz muito o tamanho da tabela de roteamento.

Quando a **divisão em sub-redes** é introduzida, as tabelas de roteamento são alteradas acrescentando-se entradas da forma (esta rede, sub-rede, 0) e (esta **rede**, esta **sub-rede**, **host**). Sendo assim, um roteador da sub-rede k sabe como alcançar todas as outras sub-redes, e também como chegar a todos os hosts da sub-rede k. Ele **não precisa** saber detalhes sobre os hosts **de outras sub-redes**. Na realidade, a única modificação é fazer com que cada roteador seja submetido a um **AND booleano** com a máscara de sub-rede, a fim de eliminar o número do host e pesquisa o endereço resultante em suas tabelas (depois de determinar qual é a classe da rede).

Por exemplo, um pacote endereçado a 130.50.15.6 recebido no roteador principal passa pela operação AND booleana com a máscara de sub-rede 255.255.252.0/22 para gerar o endereço 130.50.12.0. Esse endereço é usado para acessar as tabelas de roteamento com a finalidade de descobrir que linha de entrada usar para chegar ao roteador correspondente à sub-rede. Desse modo, a divisão em sub-redes reduz o espaço na tabela do roteador, criando uma hierarquia de três níveis que consiste em rede, sub-rede e host.

Endereçamento classless e super-redes

Por volta de 1993, ficou aparente que técnicas isoladas não impediriam que o crescimento da Internet rapidamente esgotasse o espaço de endereços válidos na Internet. É claro que isto exige um novo esquema de endereço o que deve ser fornecido pelo **IPv6**. Mas enquanto isto não acontece, é usado uma solução temporária.

Conhecida como endereçamento **classless**, o esquema de endereçamento estende a idéia usada no endereçamento de sub-rede para **permitir que um prefixo de rede tenha um tamanho qualquer**. Além de um novo modelo de endereçamento, os projetistas inventaram técnicas de encaminhamento e propagação de rota. Como resultado, a tecnologia inteira ficou conhecida como **Classless Inter-Domain Routing (CIDR)**.

A idéia básica por trás do **CIDR**, é alocar os endereços IP restantes em blocos de tamanho variável, **sem levar em consideração as classes**. Se um site precisar, digamos, de 2000 endereços, ele receberá um bloco de 2048 endereços.

Como o endereçamento de sub-rede, o CIDR usa máscara de endereços de 32 bits para especificar o limite entre o que representa rede e o que representa hosts. Por exemplo voltando a organização que recebeu 2048 endereços, isto é possível começando com o endereço 128.211.168.0:

	Decimal com ponto	**Equivalente binário de 32 bits**
Endereço mais baixo	128.211.168.0	**10000000.11010011.10101**000.00000000
Endereço mais alto	128.211.175.255	**10000000.11010011.10101**111.11111111
Máscara de 21 bits		**11111111.11111111.11111**000.00000000

Como a identificação de um bloco CIDR exige um endereço e uma máscara, criou-se uma notação abreviada para expressar os dois itens. Denominada **notação CIDR**, mas conhecida informalmente como notação slash, a abreviação **representa o tamanho da máscara em decimal** e sua uma barra para separá-la do endereço. Assim, na notação CIDR, o bloco de endereço é expresso como:

128.211.168.0**/21**

Onde /21 indica uma máscara de endereços com 21 bits marcados como 1. A seguir podemos ver os valores decimais pontuados para todas as máscaras CIDR possíveis. Os prefixos /8, /16, /24 correspondem à divisões tradicionais classe A, B e C.

Notação CIDR	Decimal pontuada	Notação CIDR	Decimal pontuada
/1	128.0.0.0	/17	255.255.128.0
/2	192.0.0.0	/18	255.255.192.0
/3	224.0.0.0	/19	255.255.224.0
/4	240.0.0.0	/20	255.255.240.0
/5	248.0.0.0	/21	255.255.248.0
/6	252.0.0.0	/22	255.255.252.0
/7	254.0.0.0	/23	255.255.254.0
/8	**255.0.0.0**	**/24**	**255.255.255.0**
/9	255.128.0.0	/25	255.255.255.128
/10	255.192.0.0	/26	255.255.255.192
/11	255.224.0.0	/27	255.255.255.224
/12	255.240.0.0	/28	255.255.255.240
/13	255.248.0.0	/29	255.255.255.248
/14	255.252.0.0	/30	255.255.255.252
/15	255.254.0.0	/31	255.255.255.254
/16	**255.255.0.0**	**/32**	**255.255.255.255**

O endereçamento **classless**, que agora **é usado por toda a Internet**, trata os endereços IP como inteiros quaisquer, e permite que um administrador de rede particione endereços em blocos contíguos, nos quais o número de endereços em um bloco é uma potência de dois.

Com o CIDR, os **algoritmo padrão de roteamento não funciona mais**. Em vez disso, cada entrada de tabela de roteamento é estendida com uma máscara de 32 bits.

Desse modo, **agora existe uma única tabela de roteamento** para todas as redes, consistindo em um array de triplas (endereço IP, máscara de sub-rede, linha de saída).

Quando um pacote chega, seu endereço IP de destino é extraído. Depois (conceitualmente), a tabela de roteamento é varrida entrada por entrada, mascarando-se o endereço de destino e comparando-se esse endereço com a entrada de tabela, em busca de uma correspondência.

É possível que várias entradas (com diferentes comprimentos de máscaras de sub-redes) **correspondam** e, nesse caso, será usada a máscara mais longa. Portanto, se houver uma correspondência para a máscara /20 e uma máscara /24, será usada a entrada /24.

Foram criados algoritmos complexos para acelerar o processo de comparação de endereços. Os roteadores comerciais utilizam chips VLSI personalizados com esses algoritmos incorporados em hardware.

Blocos de CIDR reservados para redes privadas

Alguns prefixos de rede foram reservados pelo IETF de forma a serem somente utilizados em **redes privadas**, estes prefixos reservados nunca serão atribuídos a redes na Internet.

Coletivamente, os prefixos reservados são conhecidos com endereços privados ou **endereços não-roteáveis**. Este último surge porque os roteadores na Internet entendem que os endereços são reservados; se um datagrama destinado a um dos endereços privados for acidentalmente encaminhado para a Internet, um roteador na Internet será capaz de detectar o problema e descartar o datagrama.

O último bloco de endereços listados, 169.254.0.0/16, é incomum porque é usado por sistemas que autoconfiguram endereços IP.

Prefixo	Endereço mais baixo	Endereço mais alto
10.0.0.0/8	10.0.0.0	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255
169.254.0.0/16	169.254.0.0	169.254.255.255

NAT – Network Address Translation

Um grande problema hoje na Internet é que os endereços **IPs válidos na Internet estão escassos**. Porém os clientes de negócios (empresas) esperam estar continuamente on-line durante o horário comercial. Tanto pequenas empresas, como as agências de viagens com três funcionários, quanto as grandes corporações têm vários computadores conectados por uma LAN. Alguns computadores são PCs de funcionários; outros podem ser servidores da Web. Em geral, existe um roteador na LAN que está conectada ao ISP por uma linha dedicada com a finalidade de fornecer conectividade contínua. Essa organização significa que cada computador deve ter seu próprio endereço IP durante o dia inteiro. Na realidade, o número total de computadores pertencentes a to dos os clientes comerciais combinados não pode ultrapassar o número de endereços IP que o ISP tem.

Para piorar, mais e mais usuários estão assinando os serviços de **ADSL** ou Internet via cabo. Duas características desses serviços são (1) o usuário recebe um endereço IP permanente e (2) não existe nenhuma tarifa por conexão (apenas uma tarifa mensal), de forma que muitos usuários de ADSL e cabo simplesmente ficam conectados de modo permanente. Esse desenvolvimento acelera a redução da quantidade de endereços IP. Atribuir endereços IP no momento da utilização, como ocorre no caso dos usuários de discagem (DHCP), não tem utilidade, porque o número de endereços IP em uso em qualquer instante pode ser muitas vezes maior que o número de clientes do ISP.

Apenas para complicar um pouco mais, muitos usuários de ADSL e cabo têm dois ou mais computadores em casa, muitas vezes um computador para cada membro da família, e todos eles querem estar on-line o tempo todo, usando o único endereço IP que o ISP lhes forneceu.

A solução aqui é conectar todos os PCs por meio de uma LAN e inserir um roteador nessa LAN. Do ponto de vista do ISP, agora a família equivale a uma pequena empresa com alguns computadores.

O problema de esgotar os endereços IP não é um problema teórico que pode ocorrer em algum momento no futuro distante. Ele está acontecendo aqui mesmo e agora mesmo. A solução a longo prazo é a Internet inteira migrar para o IPv6, que tem endereços de 128 bits. Essa transição está ocorrendo com lentidão e a conclusão do processo irá demorar muitos anos. Em conseqüência disso, algumas pessoas consideraram necessário fazer uma rápida correção a curto prazo.

Essa correção veio sob a forma da NAT (Network Address Translation), descrita na RFC 3022 e que resumiremos a seguir.

A idéia básica por trás da NAT é atribuir a cada empresa um único endereço IP (ou no máximo, um número pequeno deles) para tráfego da Internet. Dentro da empresa, todo computador obtém um endereço IP exclusivo, usado para roteamento do tráfego interno. Porém, quando um pacote sai da empresa e vai para o ISP, ocorre uma conversão de endereço.

Para tornar esse esquema possível, é preciso usar os IPs privados não roteáveis na Internet. As empresas podem utilizá-los internamente como desejarem. A única regra é que nenhum pacote contendo esses endereços pode aparecer na própria Internet.

O que vai acontecer com o **uso do NAT** é o seguinte:

- (1) quando o pacote for sair da rede privada para a Internet, o ponto de acesso a Internet (normalmente um modem ADSL) irá “mascarar” o pacote, ou seja ele trocará o IP de origem contendo um IP privado (ex. 10.1.1.1) pelo por um IP válido (ex. 200.1.2.3 do ADLS);
- (2) Quando o pacote voltar com a resposta, está troca deve ser desfeita pelo ponto de acesso a Internet (no nosso exemplo, pelo modem ADSL), isto é possível porque o ponto de acesso a Internet armazena algumas características do pacote (endereços IP's de origem e destino, portas de origem presentes na camada de transporte e destino, etc).
- (3) Depois de desfazer o NAT o ponto de acesso a Internet (ADSL) envia o pacote original (destinado a rede com IP não roteável a Internet, para a rede, no nosso exemplo 10.1.1.1).
-

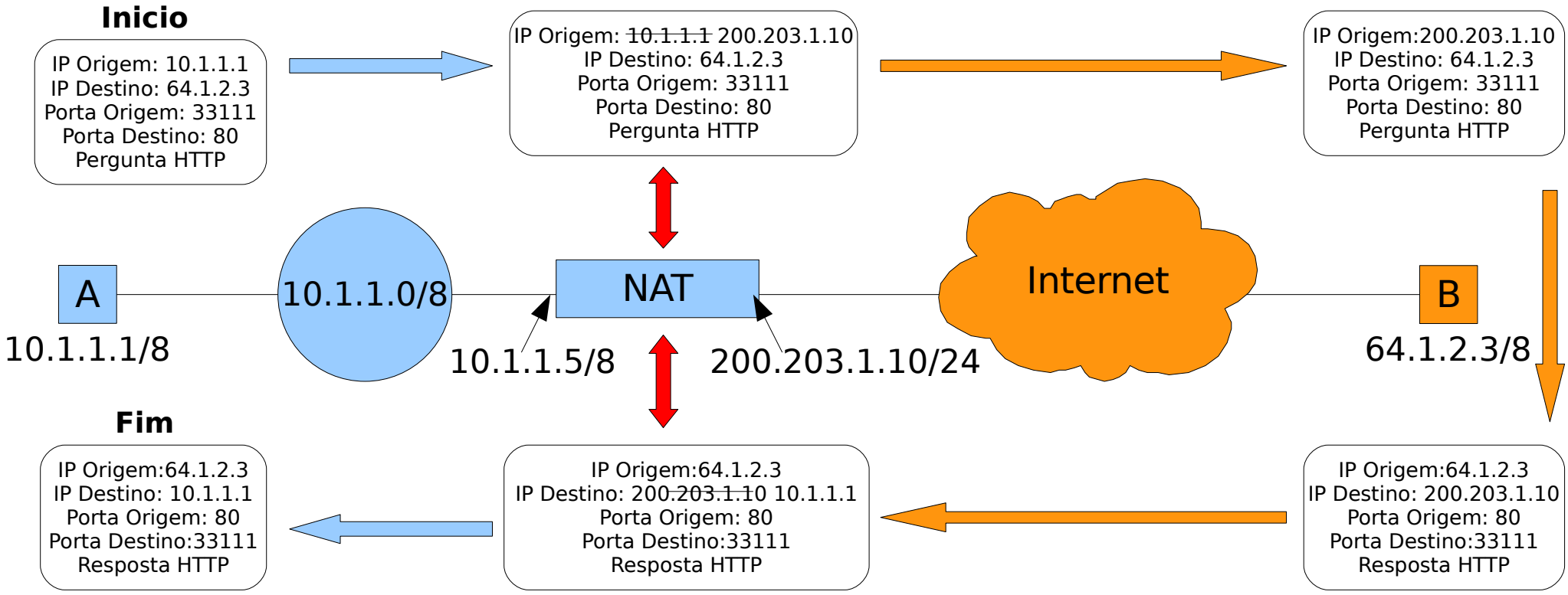
Este **processo é totalmente transparente** para o usuário da rede privada e da Internet, porém não para o ponto de acesso a Internet (á máquina que fará o NAT), já que está máquina terá de armazenar informações sobre a conexão de rede para poder fazer a tarefa de NAT, usando muito de sua memória e processamento. O que não seria necessário usando apenas roteadores e IP's válidos na Internet.

Endereçamento IP

O **NAT** normalmente **aplica** a rede um **certo nível de atraso aos pacotes**, já que o ponto de acesso a Internet tem que analisar e alterar a grande maioria dos pacotes que passam por ele. O NAT também cria uma rede pseudo orientada a conexão.

Porém, o **NAT tem** muitos **benefícios**, tal como:

- Esconder o layout da rede privada;
- Não permitir que as máquinas a trás do NAT sejam acessadas como servidor. Mas em alguns casos isto pode ser um ponto negativo;
- Manter um certo nível de segurança na rede;
- Mas a principal vantagem é permitir que várias máquinas naveguem na Internet usando apenas um único IP válido. E isso dá uma acerta folga para o problema da falta de endereços IP's na Internet.



Segue uma tabela que define alguns termos usados em redes de computadores:

Termo	Definição
Endereço IP ou Endereço de host	Um número de 32 bits, normalmente escrito em formato decimal com pontos, que identifica apenas uma interface dos computadores.
Rede	Um conjunto de hosts, em que todos têm uma parte inicial idêntica nos endereços IP.
Endereço de Rede ou Número de rede	Um número de 32 bits, normalmente escrito em formato decimal com pontos, que representa uma rede. Esse número não pode ser atribuído como um endereço IP à interface dos computadores. A parte referente à rede do número de host tem um valor formado apenas por 0s binários.
Endereço de broadcast	Um número de 32 bits, normalmente escrito em formato decimal com pontos, usado para endereçar todos os hosts da rede. Esse número não pode ser atribuído como um endereço IP à interface dos computadores. A parte referente aos hosts tem um valor formado apenas por endereços 1s binários.
Sub-rede	Um conjunto de hosts, em que todos têm uma parte inicial idêntica nos endereços IP. Uma sub-rede difere de uma rede à medida que ela é uma subdivisão de uma rede, com uma parte maior dos endereços sendo idêntica.
Endereço de sub-rede ou Número de sub-rede	Um número de 32 bits, normalmente escrito em formato decimal com pontos, que representa uma sub-rede. Esse número não pode ser atribuído como um endereço IP à interface dos computadores. A parte referente aos hosts tem um valor formado apenas por 0s binários.
Sub-redes	O resultado da subdivisão das redes em sub-redes menores. Esse é o jargão, por exemplo, “Você está criando sub-redes?”
Máscara de rede	Um número de 32 bits, normalmente escrito em formato decimal com pontos. A máscara é usada pelos computadores para calcular o número de rede de um determinado endereço IP fazendo um AND Booleano no endereço IP e na máscara. A máscara também define o número de bits de host em um endereço.
Máscara	Um termo genérico para máscara, quer seja uma máscara-padrão, quer seja uma máscara de sub-rede.
Máscara padrão Classe A	A máscara usada em redes Classe A quando as sub-redes não estão sendo usadas. O valor é 255.0.0.0.
Máscara padrão Classe B	A máscara usada em redes Classe B quando as sub-redes não estão sendo usadas. O valor é 255.255.0.0.
Máscara padrão Classe C	A máscara usada em redes Classe C quando as sub-redes não estão sendo usadas. O valor é 255.255.255.0.
Parte ou campo de rede	Termo usado para descrever a primeira parte da um endereço IP. A parte que justamente representa a rede. Está parte depende da máscara escolhida.
Parte ou campo de host	Termo usado para descrever a última parte de um endereço IP. Está parte depende da máscara escolhida.

Este material é retirado dos seguintes livros:

TANENBAUM, Andrew S. **Redes de Computadores**. Editora Campus, 4 Edição. 2003.

COMER, Douglas E. **Interligação de Redes com TCP/IP, volume 1**. Editora Campus, 5 Edição. 2006.

ODOM, Wendell. **Cisco CCNA**. Editora Altabooks, 3 Edição. 2003

Todos os slides são apenas uma base para a disciplina e não dispensa a leitura dos próprios livros para compreensão do assunto como um todo.

fim