

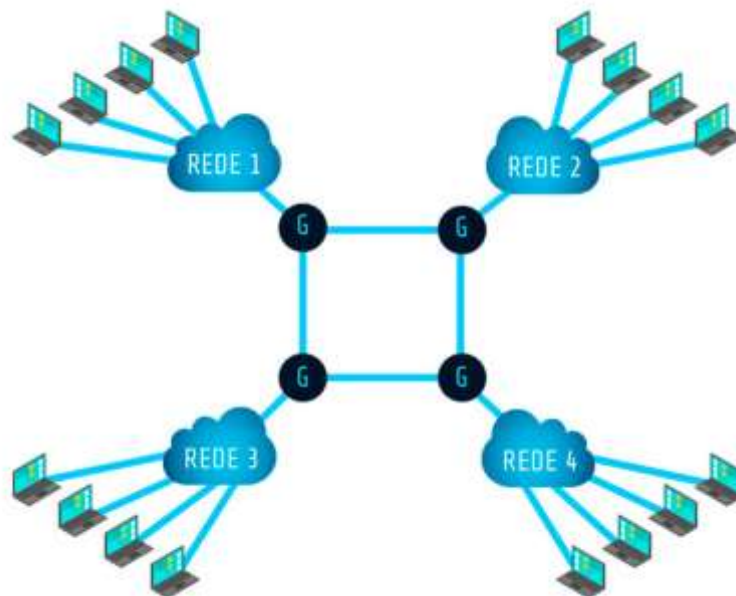


CONFIGURAÇÕES DE REDE IP

A camada de rede na Internet

Na camada de rede, a Internet pode ser vista como um conjunto de sub-redes ou Sistemas Autônomos (SA) conectados entre si. Não existe uma estrutura real, mas diversos backbones que interligam redes regionais, que por sua vez estão conectadas às redes locais.

O protocolo que mantém a Internet unida é o **protocolo de camada de rede IP** (Internet Protocol). A tarefa do IP é fornecer a melhor forma de transportar datagramas da origem para o destino, independentemente de esses hospedeiros estarem na mesma rede ou em outras redes intermediárias.



Imagine que você está solicitando a transferência de dados de seu computador para um hospedeiro remoto (está fazendo o upload do arquivo). A camada de transporte de seu computador receberá o fluxo de dados referente à transferência de seu arquivo. Como provavelmente esse fluxo é muito grande para caber em um único pacote IP, ele será quebrado em partes menores pela camada de transporte e cada parte desta será entregue para a camada de rede (cada um será colocado em um datagrama IP).

Esses datagramas serão transmitidos pela Internet, podendo ainda serem fragmentados ao longo do caminho. Quando todos os fragmentos de um

datagrama chegam ao destino, o datagrama original é remontado pela camada de rede do destino sendo entregue à camada de transporte que recriará o fluxo original para o processo de recepção.

Protocolo de endereços IPv4

Protocolo IP versão 4 (IPv4)

Na Internet, a camada de rede trata cada pacote de forma independente, não tendo qualquer relação com pacotes anteriores ou posteriores. Pacotes com mesma origem e destino podem, inclusive, passar por diferentes rotas.

O IPv4 é definido pela RFC 791, sendo atualizado pelas RFC 1349, RFC 2474 e RFC 6864.

1. Datagramas

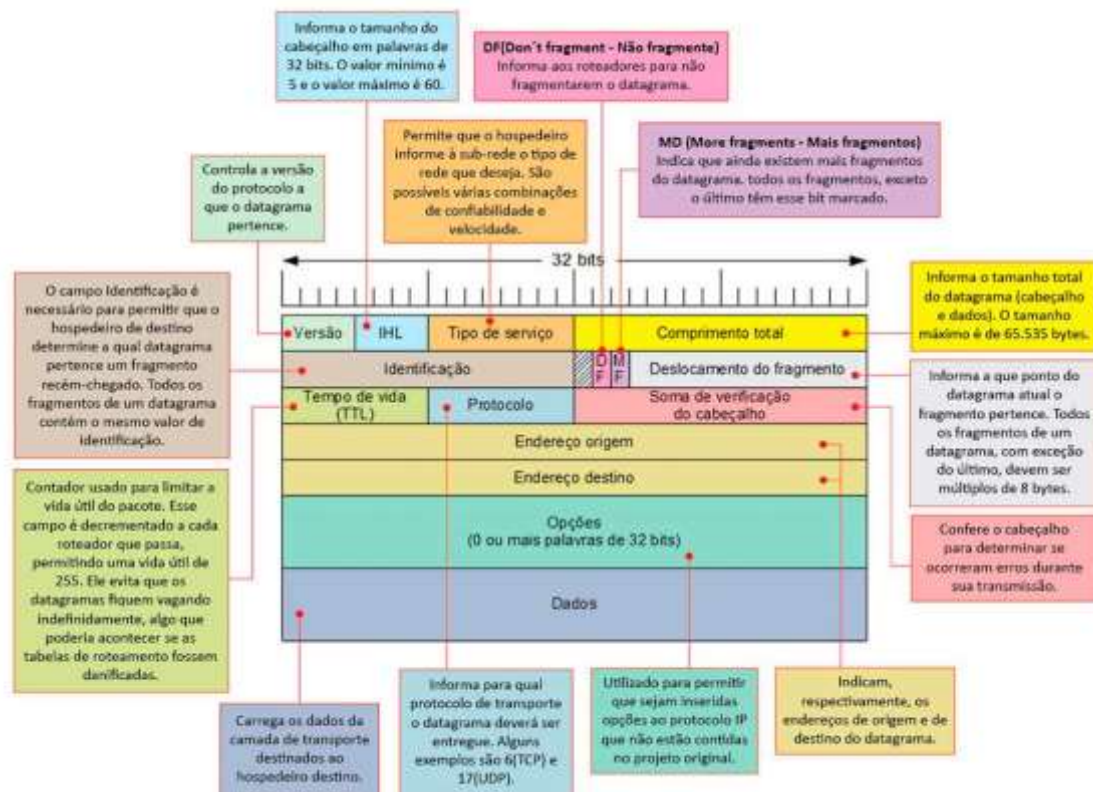
São unidades básicas de informações que passam pela Internet. Dentro do datagrama está seu cabeçalho, que contém informações sobre sua origem e seu destino, assim como informações sobre para qual protocolo o IP deverá passar os dados. Também fazem parte dele os dados que devem ser entregues à camada de transporte no destino.

2. Fragmentos

São partes de um datagrama muito grande que foi quebrado em unidades menores. Como os dados precisam caber dentro da porção de dados da rede física, pode ser que seja necessário fragmentar os dados da aplicação para que eles possam ser transportados pela rede. O tamanho do fragmento é determinado pelo MTU da interface de hardware da rede. O IPv4 especifica que a fragmentação ocorre em cada roteador baseado na MTU da interface pela qual o datagrama IP deve passar.

Quando um datagrama é quebrado em fragmentos, cada um desses fragmentos passa a ser um novo datagrama que está passando pela rede.

Um datagrama IP consiste em duas partes: cabeçalho e dados. O cabeçalho tem uma parte fixa de 20 bytes e uma parte opcional de tamanho variável.



Endereço IPv4

Endereçamento IPv4

Um hospedeiro normalmente possui apenas uma interface com a rede de computadores. Quando o protocolo IP de um hospedeiro quer enviar um datagrama, ele o faz por meio dessa interface.

A interface de rede é a fronteira entre o hospedeiro e a rede física.

Considere, neste momento, um roteador e suas interfaces. Como a tarefa de um roteador é receber um datagrama por uma interface e repassá-lo por outra interface, ele estará ligado a duas ou mais redes físicas. A fronteira entre o roteador e qualquer uma dessas redes também é denominada uma interface. Assim, um roteador tem múltiplas interfaces, uma para cada uma das redes às quais está conectado.

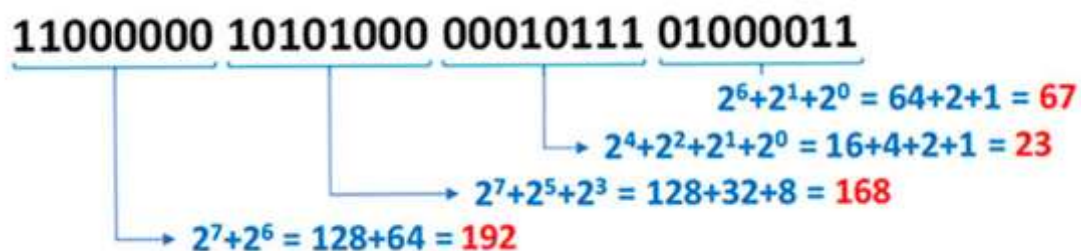
Atenção!

Independentemente de quantas interfaces tenha um hospedeiro, o IP exige que cada uma delas tenha seu próprio endereço IP de modo que este, tecnicamente, esteja associado a uma interface, e não ao hospedeiro que a contém.

Cada endereço IP tem comprimento de 32 bits (4 bytes), havendo um total de 232 endereços possíveis (aproximadamente 4 bilhões de endereços IP), os quais são escritos em notação decimal separada por pontos, na qual cada byte do endereço é escrito em sua forma decimal e separado dos outros bytes por um ponto.

Considere o endereço IP 192.168.23.67. O 192 é o número decimal equivalente aos primeiros 8 bits do endereço; o 168 é o decimal equivalente ao segundo conjunto de 8 bits do endereço, e assim por diante. Em notação binária, o endereço 192.168.23.67 fica:

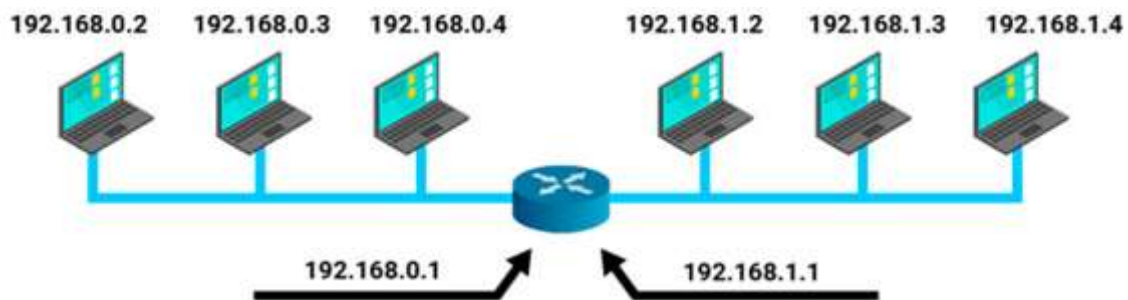
11000000 10101000 00010111 01000011



Cada interface em cada hospedeiro da Internet precisa de um endereço IP globalmente exclusivo, ou seja, não pode haver duas interfaces com o mesmo endereço IP na Internet válida.

A figura, a seguir, fornece um exemplo de endereçamento IP e interfaces em que um roteador com 2 interfaces é usado para interconectar os 6 hospedeiros. Observando os endereços dos hospedeiros da esquerda e da interface do roteador que os liga, percebe-se que todos possuem endereço IP na forma 192.168.0.x, enquanto os hospedeiros e a interface do roteador localizados na parte direita da figura possuem endereço na forma 192.168.1.x. Diz-se que cada

uma dessas redes que interconecta 3 hospedeiros mais a interface do roteador formam uma sub-rede.



Como pode-se observar, no exemplo, os 3 campos mais à esquerda do endereço (formados por 24 bits) nunca mudam dentro da sub-rede. Desse modo, temos à esquerda a sub-rede 192.168.0.0/24 e à direita a sub-rede 192.168.1.0/24. O “/24” indica que os 24 bits mais à esquerda do endereço definem a **sub-rede**.

A estratégia de atribuição de endereços da Internet é conhecida como Roteamento Interdomínio sem Classes (*Classless Inter-domain Routing – CIDR*).

O CIDR generaliza a noção de endereçamento de sub-rede. O endereço IP de 32 bits é dividido em 2 partes sendo representado por A.B.C.D/X, em que X indica o número de bits existentes na primeira parte do endereço.

Os X bits mais significativos de um endereço na forma A.B.C.D/X constituem a parcela da rede do endereço IP e normalmente são denominados prefixo (ou prefixo de rede). Esse prefixo determina qual parte do endereço IP identifica a rede. Uma organização normalmente recebe um bloco de endereços contíguos, ou seja, uma faixa de endereços com um prefixo comum. Assim, os endereços IP de hospedeiros dentro da organização compartilharão o prefixo comum, o que reduz consideravelmente o tamanho da tabela de repasse nos roteadores, visto que um único registro da forma A.B.C.D/X será suficiente para transmitir pacotes partindo de fora para qualquer destino dentro da organização.

Os últimos (32-X) bits de um endereço podem ser considerados como os bits que distinguem os hospedeiros dentro da sub-rede. Esses bits menos significativos podem (ou não) ter uma estrutura adicional de sub-rede tal como aquela discutida anteriormente. Por exemplo, suponha que os primeiros 24 bits do endereço A.B.C.D/24 especificam o prefixo da rede da organização e são comuns aos endereços IP de todos os hospedeiros da organização. Os 8 bits restantes, então, identificam os hospedeiros específicos da organização.

A estrutura interna da organização poderia ser tal que esses 8 bits mais à direita seriam usados para criar uma sub-rede dentro da organização, como discutido. Por exemplo, A.B.C.D/28 poderia se referir a uma sub-rede específica dentro da organização.

Anteriormente ao CIDR, os bits reservados para indicar a parte da sub-rede possuíam exatamente 8, 16 ou 24 bits. Esse esquema é conhecido como endereçamento de classes cheias, e as sub-redes com endereços de sub-rede de 8, 16 e 24 eram conhecidas, respectivamente, como redes de classe A, B e C. Tal divisão em classes cheias se mostrou problemática para suportar o rápido crescimento da quantidade de organizações com sub-redes de pequeno e médio portes.

Uma sub-rede de classe C (/24) poderia acomodar apenas $2^8 - 2 = 254$ hospedeiros (dois dos $2^8 = 256$ endereços são reservados para uso especial). Essa sub-rede é muito pequena para muitas organizações, por outro lado, uma sub-rede de classe B (/16), que suporta até $2^{16} - 2 = 65.534$ hospedeiros, seria demasiadamente grande. Com o endereçamento de classes cheias, uma organização com 2.000 hospedeiros recebia um endereço de sub-rede de classe B (/16), o que resultava no rápido esgotamento do espaço de endereços de classe B e na má utilização do espaço de endereço alocado.

Os 2 endereços especiais de uma sub-rede que não podem ser utilizados são o primeiro e o último endereço da faixa de endereços da organização. O primeiro é reservado para o endereço de rede, que identifica a rede como um todo. Nele, todos os bits que não fazem parte do prefixo de rede recebem o valor 0.

Já o último endereço é utilizado como endereço de difusão (*broadcast*). Roteadores não repassam mensagens de difusão, portando, em uma rede IP a difusão fica limitada ao segmento de rede limitado pelo roteador. No endereço de difusão, todos os bits que não fazem parte do prefixo de rede recebem o valor 1.

O 255.255.255.255 é um endereço especial de difusão em que a mensagem é entregue a todos os demais hospedeiros que estão na mesma sub-rede do hospedeiro que enviou a mensagem.

No endereçamento de classes cheias, **o número total de redes e hospedeiros para cada classe é:**

Classe A

126 redes com aproximadamente 16 milhões de hospedeiros cada.

Classe B

16.384 redes com até 64K hospedeiros cada.

Classe C

Cerca de 2 milhões de redes com até 254 hospedeiros cada.

Classe D

Cerca de 268 milhões de grupos multicast.



A distribuição de endereços IP é controlada pela ICANN (Internet Corporation for Assigned Names and Numbers).

Sub-Redes

O mundo exterior a uma organização enxerga sua rede como sendo única, e nenhuma informação sobre sua estrutura interna é necessária. Porém, sem a utilização de sub-redes, o espaço de endereçamento pode se tornar muito ineficiente.

A fim de tornar mais eficiente a utilização da rede, é comum sua divisão em várias sub-redes. O mecanismo que permite tal divisão é conhecido como **máscara de rede**.

Assim como um endereço IP, uma máscara de rede possui 32 bits divididos em 4 campos com 8 bits cada, seguindo o padrão:

Bits da rede – bit 1

Bits da sub-rede – bit 1

Bits do hospedeiro – bit 0

Os bits da sub-rede são utilizados para especificar quais bits no campo do hospedeiro são usados para especificar as sub-redes de uma rede.

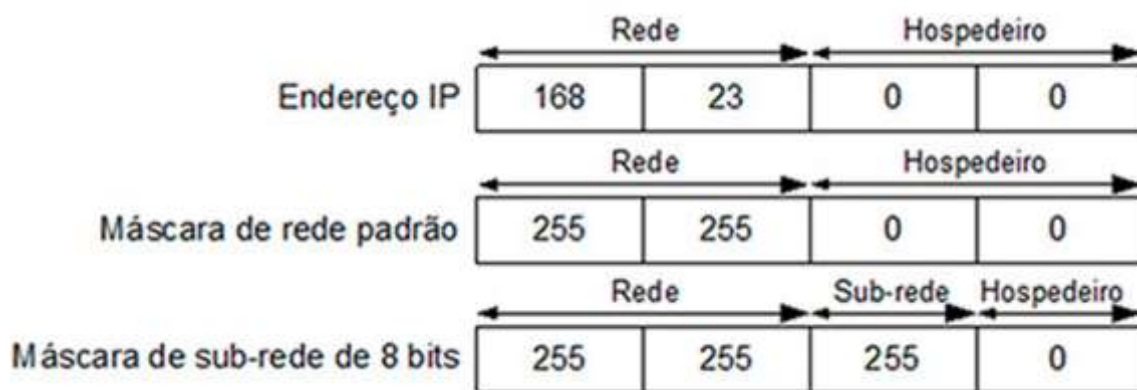
A máscara padrão (default) para cada classe é dada por:

Classe	Decimal	Notação IDR	Hexadecimal
A	255.0.0.0	/8	FF:00:00:00
B	255.255.0.0	/16	FF:FF:00:00
C	255.255.255.0	/24	FF:FF:FF:00

A máscara padrão (default) para cada classe.

Fábio Contarini Carneiro.

Veja o exemplo abaixo:



Ao se dividir uma rede em sub-redes, deve-se alocar os bits para a sub-rede a partir dos bits de mais alta ordem (bits mais à esquerda) do campo do hospedeiro. A tabela a seguir mostra os valores usados no campo do hospedeiro quando se divide uma rede em sub-redes.

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240
1	1	1	1	1	0	0	0	248
1	1	1	1	1	1	0	0	252
1	1	1	1	1	1	1	0	254

Campo do hospedeiro.

Fábio Contarini Carneiro.

Uma rede pode ser dividida em diversas partes para uso interno, continuando a ser vista como uma única rede externamente. Essas partes são as sub-redes.

Existem diversas razões para se dividir uma rede em sub-redes. Algumas destas razões são:

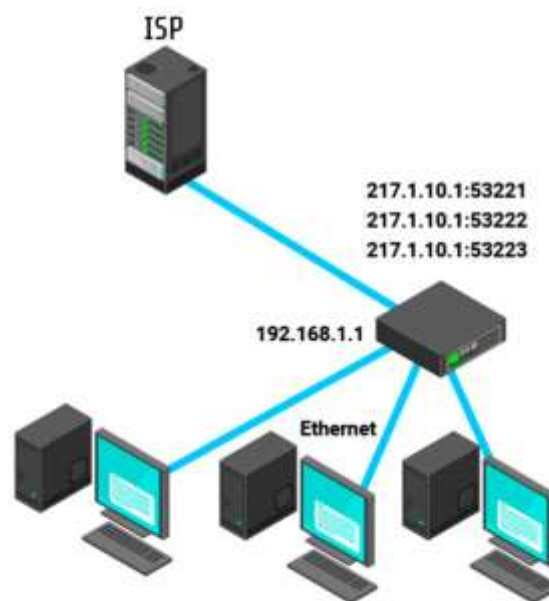
- Isolar o tráfego de uma sub-rede, reduzindo assim o tráfego total da rede.
- Proteger ou limitar o acesso a uma sub-rede.
- Permitir a associação de uma sub-rede com um departamento ou espaço geográfico específico.

NAT

Atualmente, **endereços IP são escassos** e esse esgotamento não é um problema teórico que pode ocorrer em algum momento no futuro distante, ele já

está acontecendo, e a solução atual para esse problema é o **NAT (Network Address Translation – Tradução de Endereço de Rede)**, descrito na RFC 3022.

Com essa técnica, uma organização pode utilizar internamente uma faixa de endereços que não é válida na Internet, e quando é necessário fazer acesso externo, o dispositivo responsável pelo NAT faz a tradução do endereço da rede interna para o endereço válido da organização. Dessa forma, a organização poderá obter internamente uma quantidade maior de hospedeiros do que endereços disponíveis para utilização da Internet.



A ideia básica do NAT é atribuir a cada organização uma pequena quantidade de endereços IP para tráfego na Internet. Dentro da organização, todo computador obtém um endereço IP exclusivo (também conhecido como endereço IP privado) usado para roteamento do tráfego interno e, quando um pacote sai da organização e vai para a Internet, ocorre uma conversão do endereço.

Para tornar esse esquema possível, três intervalos de endereços IP foram declarados como endereços privativos (reservados) e as organizações podem utilizá-los internamente da maneira que quiserem, a única regra é que nenhum pacote contendo esses endereços pode aparecer na própria Internet. Os três intervalos reservados são:

Faixa	Máscara	Classe
10.0.0.0 a 10.255.255.255	255.0.0.0	A
172.16.0.0 a 172.31.255.255	255.255.0.0	B
192.168.0.0 a 192.168.255.255	255.255.255.0	C

Intervalos reservados.

Fábio Contarini Carneiro.

Dentro da organização, toda máquina tem um endereço exclusivo que não é válido na Internet. Quando um pacote deixa a organização, ele passa por uma caixa NAT (normalmente um roteador), que converte o endereço de origem no endereço IP válido da organização. Desse modo, o pacote poderá transitar sem problemas pela Internet, porém, a resposta do pacote voltará para o endereço IP válido da organização, e não para a máquina que fez tal requisição. Por causa disso, a caixa NAT deverá manter uma tabela na qual poderá mapear a máquina que enviou a requisição para Internet, de forma que, quando a resposta voltar, ela possa ser mapeada para a máquina correta.

Na técnica de NAT, os endereços utilizados pelos hospedeiros de uma organização não são válidos na Internet, não há como tais equipamentos receberem acesso direto da rede externa, conferindo um certo grau de proteção aos hospedeiros da rede interna.