**Endereços e Segmentação no IPv4**

* **Meios de Envio**

*Unicast*

Há maneiras diferentes de enviar um pacote de um dispositivo de origem e que envolvem os endereços IPv4 de destino. Na transmissão unicast um dispositivo envia uma mensagem individual a outro dispositivo (comunicação um a um). Um pacote unicast  tem um IP de destino que é unicast e para um único destinatário. Um IP de origem é sempre um endereço unicast, porque o pacote sempre se origina de uma única origem. Isso acontece independente do endereço IP de destino ser unicast, broadcast ou multicast. Os endereços unicast IPv4 de host situam-se no intervalo de 1.1.1.1 a 223.255.255.255. Mas, neste intervalo, há endereços reservados para fins especiais.

*Broadcast*

Um dispositivo envia uma mensagem a todos os dispositivos (um para todos). Um pacote de broadcast é entregue a todos os dispositivos (no mesmo domínio de broadcast). O broadcast pode ser direcionado (enviado a todos os hosts de uma rede específica) ou limitado (enviado para 255.255.255.255). Os roteadores não propagam broadcasts. Os pacotes broadcast utilizam recursos da rede e todos os hosts da rede processam o pacote. Por isso, o tráfego broadcast deve ser limitado para não prejudicar o desempenho da rede ou dos dispositivos. Existe o endereço IPv4 de broadcast 255.255.255.255 e, também, há um endereço de broadcast para cada rede (chamado de broadcast direcionado e usa o maior endereço da rede). Um dispositivo não conectado diretamente à rede de destino encaminha um broadcast direcionado por IP da mesma maneira que encaminha pacotes IP unicast destinados a um host nessa rede.

*Multicast*

O multicast reduz o tráfego na rede ao possibilitar que um host envie um único pacote a determinados hosts que se inscrevem em um grupo multicast.

Um pacote multicast tem um endereço IP de destino com um endereço multicast. O IPv4 reservou os endereços 224.0.0.0 a 239.255.255.255 para multicast. Os hosts que recebem pacotes multicast são chamados de clientes multicast. Cada grupo multicast é representado por um único endereço de destino IPv4 multicast. Ao se inscrever em um grupo multicast, o host IPv4 processa os pacotes desse endereço multicast e os endereçados ao seu endereço unicast alocado exclusivamente. O protocolo de roteamento OSPF usa transmissões multicast. Por exemplo, os roteadores configurados com OSPF comunicam-se uns com os outros com o endereço de multicast OSPF reservado 224.0.0.5.

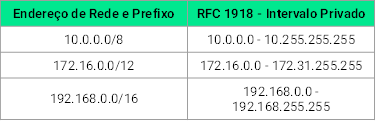
* **Tipos de Endereços IPv4**

*Públicos e Privados*

Há diferenças entre os endereços IP. Alguns endereços IP não acessam a Internet e outros são alocados para roteamento na Internet.  Tem os que são usados ​​para verificar uma conexão e outros são atribuídos a si mesmos.

Os endereços IP públicos são roteados globalmente entre roteadores de Provedores de Serviço de Internet (ISP). Parte dos endereços IP disponíveis podem ser usados ​​na Internet. Há blocos de endereços privados usados ​​pelas organizações (corporações) para atribuir endereços IPv4 a hosts internos.

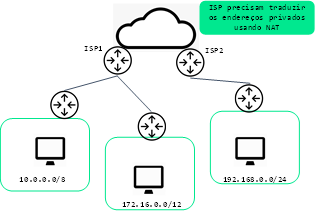
Os endereços IPv4 privados foram introduzidos em meados da década de 1990 devido ao esgotamento do IPv4. Os IPv4 privados não são exclusivos e são utilizados ​​internamente nas redes privadas.



As redes internas, de empresas a redes domésticas, usam endereços IPv4 privados para endereçar os dispositivos internos (intranet), incluindo hosts e roteadores. Porém, os endereços privados não são roteáveis na Internet. Por exemplo, pacotes têm um IPv4 de origem que é um endereço privado e um IPv4 de destino que é público (roteável globalmente na Internet). Os pacotes com endereço privado são filtrados (descartados) ou traduzidos para um endereço público antes de seguir para um ISP.

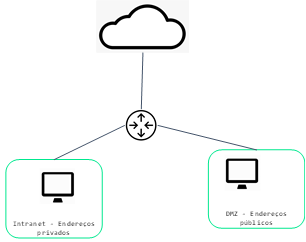
Para o ISP encaminhar este pacote, traduz o endereço IPv4 de origem, que é privado, para um endereço público através do NAT (Network Address Translation). O NAT é usado para traduzir endereços IPv4 privados em públicos (e vice-versa).  Normalmente isso é feito no roteador que conecta a rede interna (LAN) à rede do ISP.

Um dispositivo com IPv4 privado não é acessível (de forma direta) de outro dispositivo pela Internet, mas o IETF não considera endereços IPv4 privados ou NAT como formas de segurança eficazes. A Figura a seguir ilustra um exemplo de redes privadas com acesso à Internet e uso do NAT.



*DMZ*

As organizações (corporações) que têm recursos disponíveis para a Internet, por exemplo, um servidor web, também tem dispositivos com endereços IPv4 públicos. Tal parte da rede é conhecida como DMZ (zona desmilitarizada). O roteador executa o roteamento e, também, o NAT. Assim atua como um firewall para segurança. A Figura a seguir mostra uma rede privada com endereços públicos (DMZ) e uso de NAT.



*Uso especial*

Há alguns endereços, como o de rede e de broadcast, que não podem ser atribuídos a hosts. Além disso, há endereços especiais que são atribuídos a hosts, mas com restrições de como tais hosts podem interagir na rede:

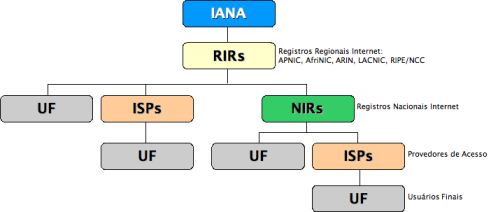
* Os endereços de loopback (127.0.0.0/8 ou 127.0.0.1 a 127.255.255.254) são geralmente identificados como apenas 127.0.0.1, são endereços especiais usados ​​por um host para orientar o tráfego para si mesmo.
* Os endereços locais de enlace (169.254.0.0/16 ou 169.254.0.1 a 169.254.255.254) são conhecidos como do endereçamento IP privado automático (APIPA - Automatic Private IP Addressing) ou endereços autoatribuídos. São usados ​​por um cliente DHCP do Windows para se autoconfigurar caso não tenha servidores DHCP disponíveis. Os endereços locais de enlace podem ser usados ​​em uma conexão ponto a ponto, porém não são normalmente usados ​​para essa finalidade.

Para a alocação de endereços, os IPv4 foram atribuídos conforme definido na RFC 790. Os clientes obtiveram um endereço de rede de uma das três classes, A, B ou C. A RFC organizou intervalos unicast em classes específicas (classful) da seguinte forma:

* Classe A (0.0.0.0/8 a 127.0.0.0/8): designada para grandes redes com mais de 16 milhões de endereços de host. A classe A usa um prefixo /8 fixo com o primeiro octeto para o endereço de rede e os três octetos restantes para endereços de host.
* Classe B (128.0.0.0/16 - 191.255.0.0/16): designada para as redes de tamanho moderado a grande com até entorno de 65.000 endereços de host. A classe B usa um prefixo /16 fixo com os dois octetos para o endereço de rede e os dois octetos restantes para endereços de host.
* Classe C (192.0.0.0/24 - 223.255.255.0/24): designada para as pequenas redes com no máximo 254 hosts. A classe C usa um prefixo /24 fixo com os três primeiros octetos para a rede e o octeto restante para os endereços de host (254 endereços de host por rede).

Com a introdução da World Wide Web (www), em meados da década de 1990, mudou-se o endereçamento classful para o classless. Obteve-se mais eficiência no espaço de endereço IPv4 limitado. O endereçamento sem classes ignora as regras das classes A, B e C. Os endereços de rede IPv4 públicos (rede e máscaras de sub-rede) são alocados baseados no número de endereços que podem ser justificados. Os endereços IPv4 públicos são exclusivos e roteados na Internet. Os endereços IPv4 e IPv6 são gerenciados pela Internet Assigned Numbers Authority (IANA). A IANA, além de gerenciar, aloca blocos de endereços IP aos Registros Regionais da Internet (RIRs): ARIN (American Registry for Internet Numbers), LACNIC (Latin America and the Caribbean Network Information Centre), AFRINIC (African Network Information Centre), RIPE NCC (Réseaux IP Européens Network Coordination Centre) e APNIC (Asia Pacific Network Information Centre).

Os RIRs são responsáveis pela alocação de endereços IP para os ISPs que fornecem blocos de endereços para organizações e ISPs menores. As organizações (corporações) também podem obter endereços diretamente de um RIR (sujeito às políticas deste).



* **Segmentação de redes**

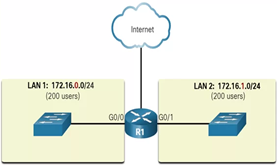
*Relembrando*

Em uma rede local (LAN) Ethernet, os dispositivos usam broadcast e ARP para se comunicarem. O ARP envia broadcast da camada 2 para um IPv4 conhecido na LAN para descobrir o endereço MAC associado. Dispositivos em redes locais Ethernet também localizam outros dispositivos através de serviços. Um host geralmente adquire sua configuração de endereço IPv4 através do protocolo de configuração dinâmica de hosts (DHCP), que envia pacotes na LAN para localizar um servidor DHCP.

Os switches propagam broadcast por todas as interfaces, exceto pela interface na qual foi recebido. Os roteadores não propagam broadcast. Ao receber um broadcast o roteador não o encaminha para outras interfaces. Assim, cada interface do roteador se conecta a um domínio de broadcast. Os pacotes broadcast são propagados somente dentro do domínio de broadcast específico.

*Problemas e Razões*

Um domínio de broadcast grande é uma rede que conecta muitos hosts. O problema com um domínio de broadcast grande é que tais hosts podem gerar broadcasts em excesso e comprometer a rede. Por exemplo, uma LAN que conecta 400 hosts que podem gerar uma quantidade excessiva de tráfego broadcast já que cada dispositivo deve processar cada pacote transmitido. A solução é dividir a rede para criar domínios de broadcast menores (processo de sub-redes). Esses 400 hosts da LAN com endereço de rede 172.16.0.0/16 podem ser divididos em duas sub-redes de 200 hosts cada: 172.16.0.0/24 e 172.16.1.0/24. O tráfego é propagado apenas em cada domínio. Desta forma, um broadcast na LAN 1 não se propaga para a LAN 2. Coloca–se um roteador para conectar as duas LANs que representam dois domínios de broadcast diferentes. Por exemplo, R1 conectado via G0/0 a um switch que suporta 200 usuários na LAN 1 e via G0/1 a um switch com suporte para 200 usuários na LAN 2. Observe que o comprimento do prefixo mudou de uma única rede /16 para duas redes /24.



A criação de sub-redes reduz o tráfego geral da rede, bem como melhora o desempenho. Também permite que o administrador implemente políticas de segurança. Por exemplo, quais sub-redes têm permissão para se comunicarem. Outra vantagem é que reduz o número de dispositivos prejudicados por tráfego anormal devido a erros de configuração, problemas de hardware ou software ou má intenção.

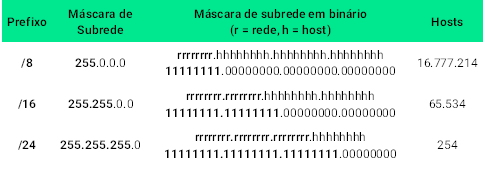
Os administradores de rede criam sub-redes com qualquer outra divisão adequada para a rede: por localização, por grupo ou função e por tipo de dispositivo.

Saber como criar sub-redes é uma habilidade fundamental que todo administrador de rede deve desenvolver. Vários métodos foram criados para ajudar a entender este processo.

* **Sub-redes**

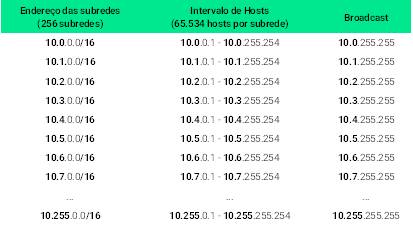
*Octet Boundary*

As sub-redes IPv4 são criadas com o uso de um ou mais bits de host como bits de rede. Estende a máscara de sub-rede para “emprestar” alguns dos bits de host. Com mais bits de host “emprestados”, mais sub-redes podem ser definidas e é menor o número de hosts por sub-rede. As redes podem ser divididas em sub-redes no limite do octeto de /8, /16 e /24.



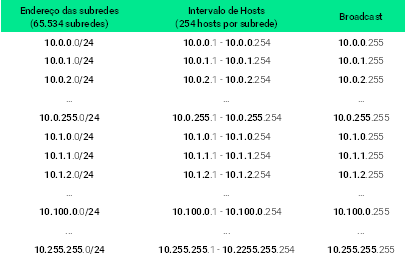
Exemplo /16 - Octet Boundary

Uma empresa escolhe o endereço privado 10.0.0.0/8 como  endereço de rede interna. Com tal endereço de rede pode conectar 16.777.214 hosts em um domínio de broadcast. A empresa pode criar uma sub-rede do endereço 10.0.0.0/8 no limite do octeto de /16, de forma que a empresa possa definir até 256 sub-redes (ou seja, 10.0.0.0/16 - 10.255.0.0/16) e cada sub-rede conectar até 65.534 hosts.



Exemplo /24 - Octet Boundary

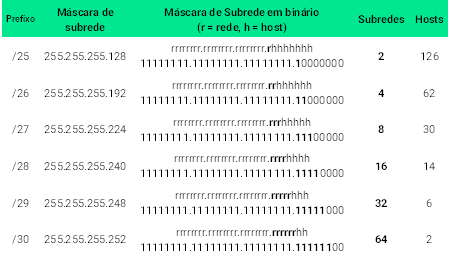
A empresa pode criar uma sub-rede da rede 10.0.0.0/8 no limite do octeto /24 (Tabela 4) . Assim, a empresa define 65.536 sub-redes e cada uma pode conectar 254 hosts. O limite /24 é muito comum para sub-redes, pois acomoda uma quantidade razoável de hosts e sub-redes de forma conveniente no limite do octeto.



Exemplo /24 - Dentro do Octet Boundary

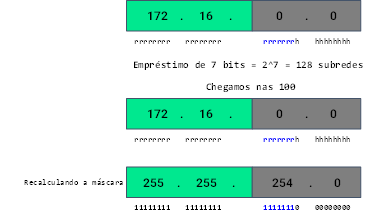
Anteriormente, “emprestou-se” bits de host dos prefixos de rede /8, /16 e /24 comuns.

Porém, as sub-redes podem emprestar bits de qualquer posição de bit de host para criar outras máscaras. Por exemplo, um endereço de rede /24 é geralmente dividido em sub-redes com o uso de tamanhos de prefixo maiores, ao emprestar bits do quarto octeto. Isso dá ao administrador flexibilidade adicional ao alocar endereços de rede a um número menor de dispositivos finais.

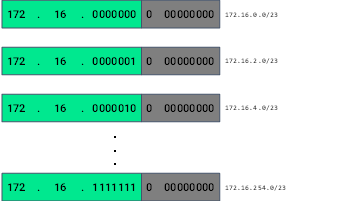


Prefixo /16

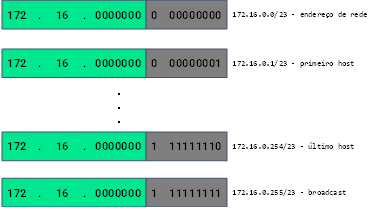
Em uma situação que necessite um número maior de sub-redes, é preciso que a rede IPv4 tenha mais bits de hosts disponíveis para empréstimo. Por exemplo, o endereço de rede 172.16.0.0 tem máscara padrão de 255.255.0.0 ou /16. Tal endereço tem 16 bits (parte da rede) e 16 bits (parte do host). Os 16 bits (parte do host) estão disponíveis para empréstimo para a criação de sub-redes. Exemplo, uma empresa necessita de pelo menos 100 sub-redes e atribui o endereço privado 172.16.0.0/16 para endereço de rede interna. Ao tomar emprestado bits de um endereço /16, inicia-se o empréstimo de bits no terceiro octeto (da esquerda para a direita) até a quantidade de bits necessária para obter 100 sub-redes. Para o requisito de 100 sub-redes, 7 bits precisam ser emprestados (ou seja, 27 = 128 sub-redes). A máscara de sub-rede deve ser modificada ao considerar os bits emprestados. Se 7 bits são emprestados, a máscara é estendida 7 bits no terceiro octeto. A máscara, em decimal, é 255.255.254.0 ou um prefixo /23, pois o terceiro octeto é 11111110 (em binário) e o quarto octeto é 00000000 (em binário). Após o empréstimo de 7 bits para a sub-rede, tem um bit de host que resta no terceiro octeto e 8 bits de host que restam no quarto octeto, num total de 9 bits que não foram emprestados. Então, 29 resulta em 512 endereços de host. O primeiro endereço de host da primeira sub-rede é 172.16.0.1 e o último endereço de host é 172.16.1.254. Para o endereço da rede é reservado o primeiro endereço e o último endereço é reservado para o endereço de broadcast. Por isso, subtrai-se esses dois endereços (29 - 2) e obtém-se 510 endereços de host disponíveis para cada sub-rede /23.



Prefixo /16 - agora /23 (subredes)



Prefixo /16 - agora /23 (hosts para  .0.0)



*Requisitos e Desafios*

A Intranet utiliza espaço de endereçamento IPv4 privado. Com isso possibilita que uma organização (corporação) use qualquer um dos endereços privados, inclusive o prefixo 10.0.0.0/8 (24 bits de host, mais de 16 milhões de hosts). O endereço de rede IPv4 privado 10.0.0.0/8 pode ser dividido em sub-redes ao usar uma máscara /16, que resulta em 256 sub-redes com 65.534 hosts por sub-rede.

Outra opção para 10.0.0.0/8 é criar sub-redes com uma máscara /24, que resulta em 65.536 sub-redes com 254 hosts por sub-rede.

Como os dispositivos na DMZ necessitam de endereços IPv4 públicos uma organização (corporação) deve maximizar seu próprio número limitado de endereços IPv4 públicos. Isso leva o administrador a minimizar o número de endereços de hosts não usados ​​por sub-rede - conhecido como VLSM (Variable Length Subnet Masking).