2- Endereçamento IP

2.1 Introdução

O IP (*Internet Protocol*) foi projetado para permitir a interconexão de redes de computadores que utilizam a tecnologia de comutação de pacotes. É um protocolo não orientado a conexão ou sem conexão. Sua função é transferir blocos de dados denominados *datagramas* da origem para o destino, onde a origem e o destino são computadores (hosts) identificados por endereços IP. Algumas das principais características desse protocolo são:

- Serviço de datagrama não confiável;
- Endereçamento hierárquico;
- Fragmentação e remontagem de pacotes;
- Roteamento adaptativo;
- Descarte e controle do tempo de vida dos pacotes.

O protocolo IP fornece o serviço de fragmentação e remontagem de datagramas longos, quando necessário, para que eles possam ser transmitidos através de redes onde o tamanho máximo permitido para os pacotes é pequeno.

O serviço oferecido pelo IP é sem conexão. Portanto, cada datagrama IP é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro datagrama. A comunicação é não confiável, não sendo usados reconhecimentos fim a fim ou entre nós intermediários. Nenhum mecanismo de controle de erros nos dados transmitidos é utilizado, exceto um *checksum* do cabeçalho que garante que as informações nele contidas, que são usadas pelos gateways (roteadores) para encaminhar os datagramas, estão corretas. Nenhum mecanismo de controle de fluxo é empregado.

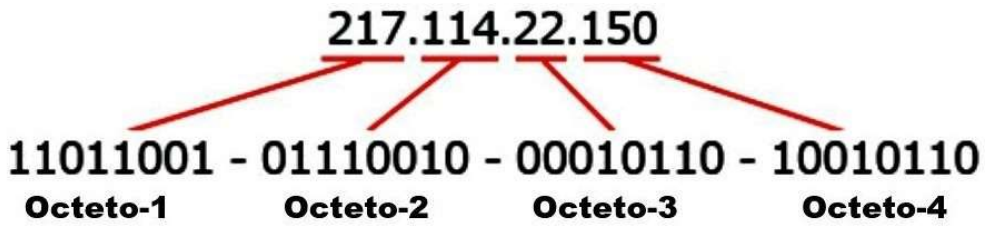
2.2 Endereçamento IP

Para que uma rede funcione, é necessário que os dispositivos dessa rede tenham uma forma de se identificar de forma única. Da mesma maneira, a interligação de várias redes só pode existir se as redes estiverem, também, identificadas no seu conjunto. Essa fórmula de identificação utilizada nas redes de computadores é o endereço IP.

Atualmente, existem duas versões de endereço IP: a versão 4 (IPv4) e a versão 6 (IPv6). A diferença entre elas é a quantidade de bits que compõe um endereço e, por conseguinte, a quantidade de redes e computadores possíveis de endereçar. Por enquanto, vamos enfatizar a versão 4, sendo que detalhes da versão 6 são comentados ao final deste capítulo. Por isso, a partir deste ponto, "endereço IP" refere-se apenas a um endereço IP versão 4 (IPv4)

O endereço IPv4 é um número de 32 bits com 4 conjuntos de 8 bits. A cada conjunto de 8 bits dá-se o nome de octecto. Apesar de sua essência ser um número binário, um endereço IP comumente é escrito em formato decimal. Observe:

Exemplo de endereço IP



Podemos dizer que um endereço IP tem duas partes:

- A identificação da rede;
- A identificação do host dentro dessa rede (host é um terminal, um nó da rede – um computador, impressora, celular...).

Um número de oito bits permite ter até 256 (0 a 255) combinações diferentes. Isto é, se o endereço tem quatro conjuntos de oito bits, teoricamente podemos ter 256^4 (4.294.967.296) números para representar redes/hosts.

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 (*Internet Service Provider*) e outras empresas.

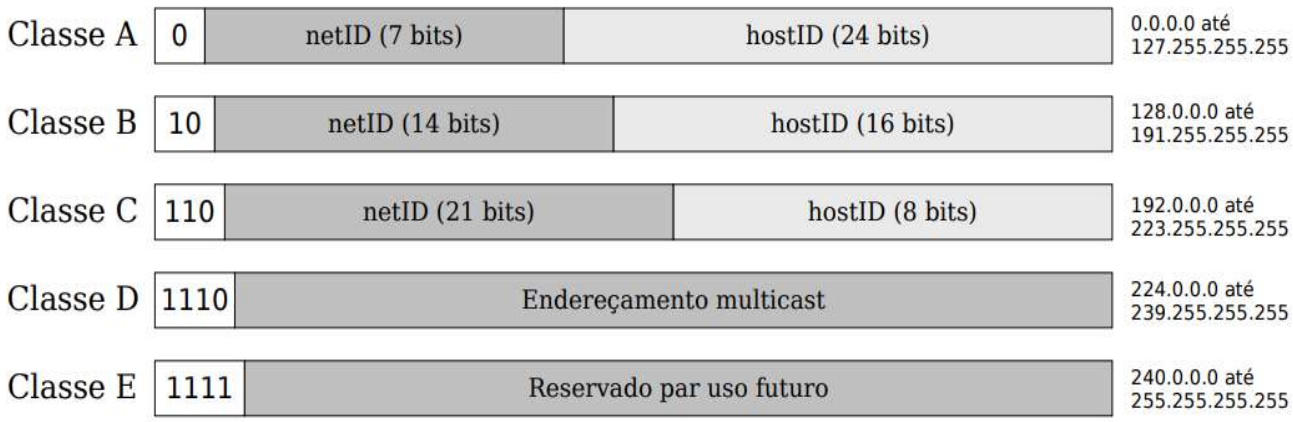
Na Internet, cada host e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host. A combinação é exclusiva: em princípio, duas máquinas na Internet nunca têm o mesmo endereço IP. É importante observar que um endereço IP não se refere realmente a um host. Na verdade, ele 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.

2.3 Classes

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 autoidentificável, 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.

Classes de endereço IP



- Classe A - apenas o primeiro octecto identifica a rede e os últimos três octectos identificam os hosts;
- Classe B - os dois primeiros octectos identificam a rede e os outros dois identificam os hosts;
- Classe C - os três primeiros octectos identificam as redes possíveis e apenas o último octecto identifica os hosts.

Observe que o que diferencia uma classe de endereços de outra é o valor do primeiro octecto, logo:

Classe A	Classe B	Classe C
1 a 126	128 a 191	192 a 224

Ao instalar uma rede TCP/IP é necessário analisar qual classe de endereços é mais adequada, baseado no número de nós da rede. Por exemplo, com um endereço classe C, é possível endereçar apenas 254 nós de rede; com um endereço B já é possível endereçar até 65.534 nós e com endereços de classe A é possível endereçar até 16.777.214.

2.4 Endereço de loopback

Um endereço de *loopback* é uma interface de rede virtual que permite que um cliente e um servidor no mesmo host se comuniquem entre si usando a pilha de protocolos TCP/IP. Neste caso, é reservado todo o bloco de endereços IP classe A com identificação de rede 127.0.0.0, e por convenção, a maioria dos sistemas atribuem o endereço IP 127.0.0.1 a esta interface, além de usar o nome *localhost* para identificá-la.

Um datagrama IP enviado à interface de *loopback* não deve aparecer em nenhuma rede, nem ser roteado para nenhum dispositivo de roteamento, devendo ser processado inteiramente dentro do próprio host que o originou. Se um pacote com destino a uma interface de loopback for recebido sem que tenha sido originado no mesmo host, deve ser descartado, pois pode se tratar de um pacote malicioso. Além disso, qualquer pacote enviado para um endereço IP do próprio host é enviado automaticamente para a interface de *loopback*. As principais aplicações de uma interface de *loopback* são:

- Diagnóstico de problemas;
- Testes de software e conectividade;
- Conexão a servidores que rodam na própria máquina;
- Configuração de serviços.

A interface de *loopback* aparece como se fosse uma camada de enlace para a camada de rede do TCP/IP, de modo que a camada de rede envia um datagrama IP para a interface de *loopback* como se estivesse enviando à camada de enlace normal, e a interface de *loopback* retorna o datagrama à fila de entrada da camada de rede.

2.5 Endereços não válidos

Os endereços não válidos, também chamados de endereços privados constituem-se de determinados intervalos que não são tratados externamente pelos roteadores da Internet.

As redes privadas são empregadas onde não há a necessidade de que todos os computadores de uma organização possuam um IP universalmente endereçável. Outra razão que torna importante os endereços privados é o número limitado de endereços públicos. O protocolo IPv6 (comentado posteriormente) foi criado para resolver este último problema.

Aplicam-se também os endereços privados na criação de redes locais onde os dispositivos se comunicam entre si, mas que não precisam de comunicação com uma rede externa, como por exemplo, impressoras ou servidores internos em uma organização.

Os intervalos de endereçamento IP destinados às redes privadas são:

Classe	Início	Fim
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

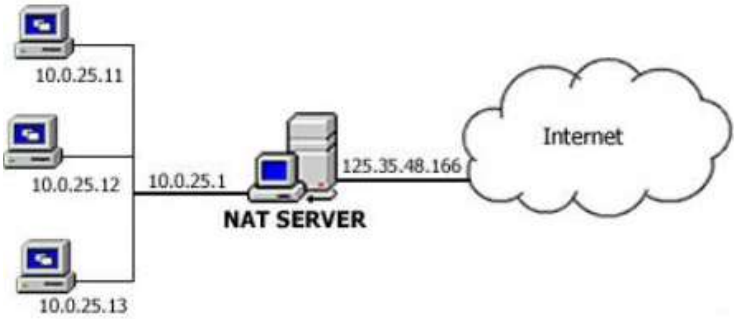
Os roteadores são configurados para descartar qualquer tráfego que use um IP privado. Este isolamento garante que uma rede privada tenha uma maior segurança, pois não é possível, em geral, ao mundo externo criar uma conexão direta a uma máquina que use um IP privado. Como as conexões não podem ser feitas entre diferentes redes privadas por meio da internet, diferentes organizações podem usar a mesma faixa de IP sem que haja conflitos, ou seja, que uma comunicação chegue acidentalmente a um elemento que não deveria.

2.6 NAT

Como vimos, os roteadores da Internet são incapazes de encaminhar pacotes cujos endereços de destino sejam um IP privado. A fim de permitir que hosts com IP privados tenham acesso a Internet, é necessário utilizar um tradutor de endereços. Esses tradutores são denominados de NAT (*Network Address Translation*).

O NAT é um mecanismo que permite traduzir endereços privados em endereços públicos registrados. As funções de NAT estão bastante relacionadas às funções de roteamento, e por isso são implementadas pelas camadas de rede dos sistemas operacionais de roteadores ou mesmo de desktops, como o Linux ou o Windows. Por estar relacionada ao roteamento, a função de NAT é normalmente implementada em roteadores ou firewalls. A função de NAT também é bastante comum em roteadores ADSL e WiFi.

NAT – *Network Address Translation*



O mapeamento feito pelo NAT pode ser também estático ou dinâmico. No mapeamento estático, as regras de mapeamento são configuradas previamente, de maneira que um dado endereço IP privado está sempre mapeado em um mesmo IP público. No mapeamento dinâmico, as regras de mapeamento são configuradas dinamicamente, criando mapeamentos temporários que são automaticamente desfeitos quando o IP privado deixa de ser utilizado por muito tempo.

2.7 Protocolos

Na camada de rede do TCP/IP, além do protocolo IP utilizado para endereçamento, existem outros protocolos que possuem funções específicas, comentadas a seguir:

- ARP (*Address Resolution Protocol*) - O ARP é um protocolo de pergunta e resposta utilizado para mapear dinamicamente endereços da camada de rede com a camada de enlace. Tipicamente, ele é utilizado para mapear endereços IPs em endereços MAC, ou seja, busca por um endereço MAC. Para controlar esse mapeamento, o protocolo ARP mantém uma tabela chamada *ARP Table*. Sempre que um novo pacote com endereços MAC ou IP aparece e ainda não estão na tabela ARP ou precisam se atualizar, o protocolo modifica a tabela com os novos dados.
- RARP (*Reverse Address Resolution Protocol*) - O RARP associa um endereço MAC conhecido a um endereço IP. Essa associação permite que os dispositivos de rede encapsulem os dados antes de enviá-los à rede. Um dispositivo de rede, como uma estação de trabalho sem disco, por exemplo, pode conhecer seu endereço MAC, mas não seu endereço IP. O RARP permite que o dispositivo faça uma solicitação para saber o seu endereço IP. Os dispositivos que usam o RARP exigem que haja um servidor RARP presente na rede para responder às solicitações RARP. O RARP usa o mesmo formato de

pacote do ARP, contudo, em uma solicitação RARP, os cabeçalhos MAC e o código de operação (*operation code*) são diferentes. O formato do pacote RARP contém espaços para os endereços MAC dos dispositivos de destino e de origem. O campo de endereço IP de origem é vazio.

- ICMP (*Internet Control Message Protocol*) – Trata-se de um protocolo que comunica mensagens de erro e outras condições que requeiram atenção em uma rede. O protocolo IP, que fornece o mecanismo para entrega de datagramas entre dispositivos, carece dessa funcionalidade, e por isso o ICMP foi criado, sendo um protocolo extremamente importante por conta dessas capacidades. O ICMP é usado para coletar o tempo de resposta, a disponibilidade dos serviços e as informações de perda de pacotes de dispositivos de rede, como roteadores, em uma rede IP. O comando **ping** é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos, estando disponível praticamente em todos os sistemas operacionais. Seu funcionamento consiste no envio de pacotes para o equipamento de destino e na "escuta" das respostas. Se o equipamento de destino estiver ativo, uma "resposta" é devolvida ao computador solicitante. O comando **traceroute** é uma ferramenta de diagnóstico que rastreia a rota de um pacote através de uma rede de computadores que utiliza os protocolos IP e o ICMP. Seu funcionamento está baseado no uso do campo *Time to Live* (TTL), destinado a limitar o tempo de vida dele. Este valor é decrementado a cada vez que o pacote é encaminhado por um roteador. Ao atingir o valor zero o pacote é descartado e o originador é alertado.

2.8 Atribuição de endereços IP

Após determinado o esquema de endereçamento para uma rede, faz-se necessário escolher o método para atribuir endereços aos hosts. Essencialmente, existem dois métodos para atribuir endereços IP - endereçamento estático e endereçamento dinâmico.

- Atribuição estática de endereços - com uma atribuição estática, o administrador da rede deve configurar manualmente as informações da rede para um host. No mínimo, isso inclui digitar o endereço IP do host, a máscara de sub-rede e o gateway padrão (falaremos sobre sub-redes no tópico 2.11). Os endereços estáticos têm algumas vantagens sobre os endereços dinâmicos. Por exemplo, são úteis para impressoras, servidores e outros dispositivos de rede que precisam ser acessíveis aos clientes na rede. Se os hosts normalmente acessam um servidor em um determinado endereço IP, haveria problemas

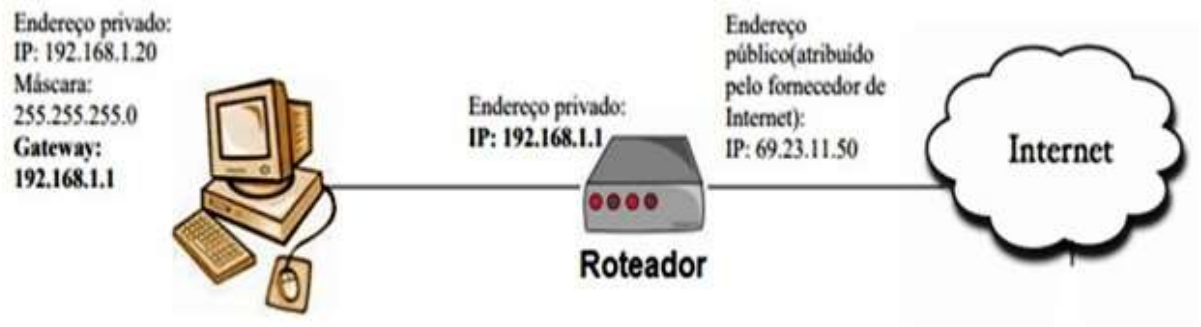
se esse endereço mudasse. Além disso, a atribuição estática de informações de endereçamento pode fornecer maior controle dos recursos da rede. Contudo, pode consumir muito tempo digitar as informações em cada host. Ao usar o endereçamento IP estático, é necessário manter uma lista exata de atribuição de endereços IP para cada dispositivo. Esses são endereços permanentes e normalmente não são reutilizados.

- Atribuição dinâmica de endereços - devido aos desafios associados ao gerenciamento de endereços estáticos, os dispositivos dos usuários finais em geral têm endereços dinamicamente atribuídos, usando o protocolo DHCP. Este protocolo ativa a atribuição automática de informações de endereçamento, como endereço IP, máscara de sub-rede, gateway padrão e outras informações de configuração. A configuração do servidor DHCP requer que um intervalo de endereços, chamado de conjunto de endereços, seja definido para ser atribuído aos clientes DHCP em uma rede. Os endereços atribuídos a esse intervalo devem ser planejados para excluir quaisquer endereços usados para os outros tipos de dispositivos. O DHCP em geral é o método preferido de atribuição de endereços IP para hosts em redes grandes porque reduz a carga sobre a equipe de suporte de rede e praticamente elimina erros de entrada. Outro benefício do DHCP é que o endereço não é permanentemente atribuído a um host, mas é só "alugado" por um período. Se o host for desligado ou removido da rede, o endereço retorna ao grupo para ser reutilizado. Essa característica é especialmente útil para usuários móveis que entram e saem da rede.

2.9 Gateway

É um dispositivo destinado a interligar redes ou mesmo traduzir protocolos. Exemplos de gateway podem ser os roteadores, uma vez que servem de intermediários entre o utilizador e a rede.

Exemplo de Gateway



Assume-se que o gateway tenha acesso ao exterior (ligação à Internet, por exemplo). Poderá ter também medidas de segurança contra invasões externas. Cabe igualmente ao gateway traduzir e adaptar os pacotes originários da rede local para que estes possam atingir o destinatário, mas também traduzir as respostas e devolvê-las à origem da comunicação. Um protocolo de utilização frequente é o NAT — que é uma das implementações de gateway mais simples.

2.10 DNS

O *Domain Name System* (Sistema de Nomes de Domínios) é um sistema de gestão de nomes que tem a função de traduzir os endereços escritos “por palavras” em endereços IP escritos em números. Ou seja, os servidores DNS, contêm listas de endereços onde os nomes estão relacionados com endereços IP. Funcionam como uma espécie de páginas amarelas gigante, com os endereços de todos os servidores existentes (ou, então, estão ligados a outros servidores com outras listas).

Por exemplo, ao escrevermos www.google.com no navegador, o pedido vai para um servidor DNS, que procura na sua lista o IP correspondente (por exemplo, 64.68.92.29) e o devolve ao navegador. A partir daí, o navegador automaticamente se liga a esse endereço.

Normalmente, ao configurar uma rede/host é necessário definir o endereço IP do servidor DNS. Se este não for automaticamente atribuído por DHCP, então, teremos de saber esse endereço.