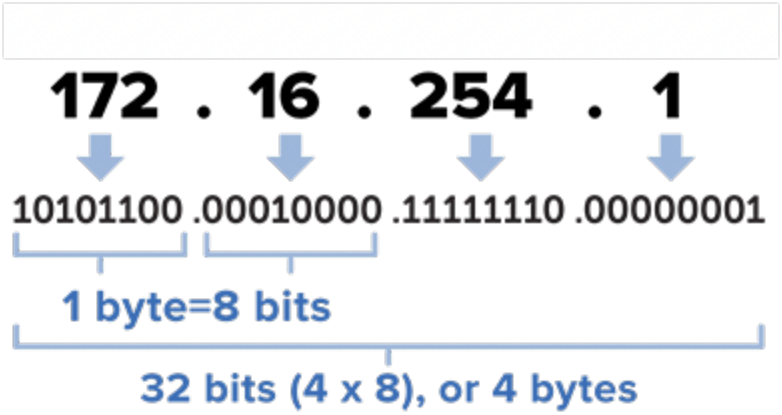
NETWHAAAAAAAAAAAAT?

BY LNIEHUES

◦ O que é um endereço de IP?

Um Endereço de Protocolo da Internet (Endereço IP), do inglês Internet Protocol address (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação. Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e endereçamento de localização.OIP,naversão4doIP(IPv4),éumnúmerode32bitsoficialmenteescrito com quatro octetos (bits) representados no formato decimal como, por exemplo, "192.168.1.2". Nele é possível mais de 4,3 bilhões de possibilidades e devido ao crescimento imenso da internet e dispositivos conectados à internet, os endereços de IPv4 estão esgotados.



O endereço127.0.0.1 é reservado para teste (loopback) e comunicação entre processos da mesma máquina (localhost). Existe uma outra versão do IP,a versão 6 **(IPv6) que utiliza um número de 128 bits**, o que torna possível utilizar 256^{16} endereços diferentes.

Cada endereço IP deve ser único em sua própria rede. As redes podem ser isoladas umas das outras e podem ser interligadas e convertidas para fornecer acesso entre redes distintas. Um sistema denominado **Network Address Translation (NAT)** permite que os endereços sejam reescritos quando os pacotes atravessam as fronteiras da rede para permitir que eles continuem até o destino correto. Isso permite que o mesmo endereço IP seja usado em várias redes isoladas e, ao mesmo tempo, permite que elas se comuniquem entre si, se configuradas corretamente.

◦ O que é NetmasK (mascara de rede)?

Uma máscara de sub-rede é um número de 32 ou 128 bits que segmenta um endereço IP existente em uma rede TCP / IP. É usado pelo protocolo TCP / IP para determinar se um host está na sub-rede local ou em uma rede remota. A máscara de sub-rede divide o endereço IP em um endereço de rede e um endereço de host, portanto, para identificar qual parte do endereço IP está reservada para a rede e qual parte está disponível para uso do host. Uma vez fornecido o endereço IP e sua máscara de sub-rede, o endereço de rede (sub-rede) de um host pode ser determinado. Normalmente, calculadoras de sub-rede estão prontamente disponíveis online que ajudam a dividir uma rede IP em sub-redes.

EXEMPLO:

Na figura abaixo, as três primeiras partes do endereço IP pertencem à rede IP (42 bits selecionados para criar redes), que é determinada pela máscara de sub-rede. 0 é o endereço mais baixo disponível na quarta parte do endereço IP. O computador, portanto, pertence à rede IP 101.102.103.0. A quarta parte (.5) do endereço IP mostra qual endereço de host o computador está usando na rede IP (8 bits para criar hosts).

IP: 101. 102. 103. 5

Subnet Mask: 255. 255. 255. 0

◦ Qual é a sub-rede de um IP com máscara de rede?

Sub-redes é o processo de dividir a rede maior em sub-redes menores (sub-redes). Sempre reservamos um endereço IP para identificar a sub-rede e outro para identificar o endereço de transmissão dentro da sub-rede. A sub-rede divide redes maiores em pequenas partes, o que é mais eficiente e conservaria uma grande quantidade de endereços. As redes menores, portanto, criaram transmissões menores que geram menos tráfego de transmissão. Além disso, a sub-rede também simplifica a solução de problemas, isolando os problemas de rede até sua existência específica.

Uma sub-rede é uma subdivisão lógica de uma rede IP. A subdivisão de uma rede grande em redes menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede.

Dispositivos que pertencem a uma sub-rede são endereçados com um grupo de bit mais significativo comum (rede que pertence) e idêntico em seus endereços IP. Isto resulta na divisão lógica de um endereço IP em dois campos, um número de rede ou prefixo de roteamento e o restante do campo ou identificador de host. O campo restante é um identificador para uma interface de h ospedeiro ou rede específicos.

◦ Qual é o endereço de broadcast de uma sub-rede?

Um endereço de broadcast é um endereço IP usado para direcionar todos os sistemas em uma rede de sub-rede específica, em vez de hosts únicos. Em outras palavras, o endereço de broadcast permite que as informações sejam enviadas para todas as máquinas em uma determinada sub-rede, em vez de para uma máquina específica. O endereço de broadcast de qualquer endereço IP pode ser calculado pegando o complemento de bits da máscara de sub-rede, às vezes referido como a máscara reversa e, em seguida, aplicando-o com um cálculo OR bit a bit ao endereço IP em questão. O último endereço IP após a filtragem pela máscara de rede.

EXEMPLO:

Se o endereço IP for 192.168.12.220 e a máscara de sub-rede for 255.255.255.128, o endereço de broadcast pode ser deduzido da seguinte maneira.

IP Address: 11000000.10101000.00001100.11011100
Reverse Mask: 00000000.00000000.00000000.01111111
Bitwise OR ----------
Broadcast Address:11000000.10101000.00001100.11111111

◦ Quais são as diferentes maneiras de representar um endereço IP com a máscara de rede?

- 1)Decimal pontilhada: - É representado pelo número decimal em que endereço IP de 32 bits é dividido em quatro octetos separados por '.'.

  Ex .: 1 28.0.0.0 | 127.0.0.0/8 | 192.0.2.0/24

- 2) Representação binária: - Neste endereço IP é representado por números binários 0 ou 1 com octetos separados por '.'.

  Ex .: 1 1000000.10101000.00001100.11011100

- 3) Representação hexadecimal: - É representado por hexadecimal.

  Ex .: IPv4 - c0.a8.0c.dc | IPv6 - 2001: 0db8: 85a3: 08d3: 1319: 8a2e: 0370: 7344

◦ Quais são as diferenças entre IPs públicos e privados?

Dos mais de 4 mil milhões de endereços disponíveis, três faixas são reservadas para redes privadas. Os endereços IP contidos nestas faixas não podem ser roteadas para fora da rede privada e não são roteáveis nas redes públicas. Dentro das classes A, B e C foram reservadas redes que são conhecidas como endereços de rede privada.

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

A maioria dos endereços IP são públicos, permitindo assim que as nossas redes (ou pelo menos o nosso router que faz fronteira entre a nossa rede e a Internet) estejam acessíveis publicamente através da Internet, a partir de qualquer lado. Quanto a endereços privados, estes não nos permitem acesso directo à Internet, no entanto esse acesso é possível mas é necessário recorrer a mecanismos de NAT (Network Address Translation) que traduzem o nosso endereço privado num endereço público. Os endereços públicos são geridos por uma entidade reguladora, muita das vezes são pagos e permitem identificar univocamente uma máquina (PC, routers,etc) na Internet. O organismo que gere o espaço de endereçamento público (endereços IP “encaminháveis”) é a Internet Assigned Number Authority (IANA).

◦ O que é uma classe de endereços IP?

O IP utiliza três classes (A, B e C - classful) diferentes de endereços. A definição de tipo de endereço classes de endereços deve-se ao fato do tamanho das redes que compõem a Internet variar muito, indo desde redes locais de computadores de pequeno porte, até redes públicas interligando milhares de hosts. Existe uma outra versão do IP, a versão 6(IPv6) que utiliza um número de 128bits, o que torna possível utilizar 256^{16} endereços diferentes.

Classe	**Gama de Endereços**	**Bits parte rede (N) e host (H)**	**Nº de redes**	**Nº de Endereços por Rede (apenas Hosts)**
A	0.0.0.1 até 126.255.255.255	N.H.H.H	126 (2^7 - 2)	16 777 214 (2^24 - 2)
B	128.0.0.0 até 191.255.255.255	N.N.H.H	16 382 (2^14 - 2)	65 534 (2^16 - 2)
C	192.0.0.0 até 223.255.255.255	N.N.N.H	2 097 150 (2^21 - 2)	254 (2^8 - 2)
D	224.0.0.0 até 239.255.255.255	N.A.	N.A.	Multicast
E	240.0.0.0 até 255.255.255.254	N.A.	N.A.	*Uso futuro; atualmente reservada a testes pela IETF*

*** A subtração por 2 no Nº de redes e Hosts é porque o primeiro IP é o IP de rede e o último IP é o IP Broadcast.**

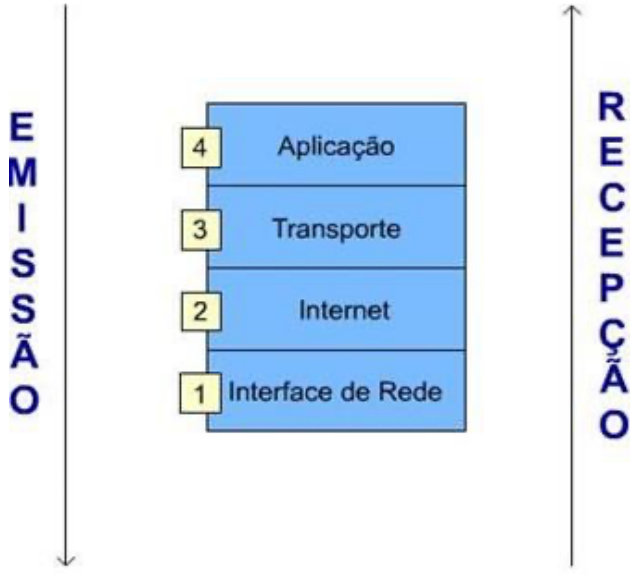
◦ O que é TCP ?

O TCP/IP (também chamado de pilha de protocolos TCP/IP ou Transmission Control Protocol) é um conjunto de protocolos de comunicação entre computadores em rede. O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI),onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas, estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.

TCP segment header

Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Originou-se na implementação inicial da rede em que complementou o Protocolo de Internet (IP). Portanto, todo o conjunto é comumente referido como TCP / IP. O TCP fornece entrega confiável, ordenada e com verificação de erros de um fluxo de octetos (bytes) entre aplicativos em execução em hosts que se comunicam por meio de uma rede IP. Os principais aplicativos da Internet, como a World Wide Web, e-mail, administração remota e transferência de arquivos, dependem do TCP, que faz parte da camada de transporte do conjunto TCP / IP.



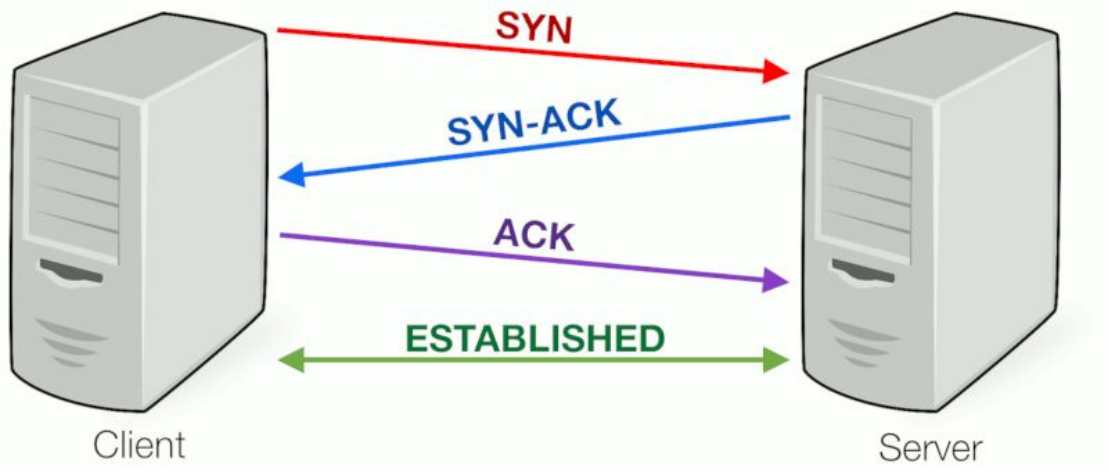
● Aplicação – usada pelos programas para comunicação em rede, alguns protocolos pertencentes a camadas são: HTTP (HyperText Transfer Protocol Secure, protocolo de transferência de hipertexto), FTP, SMTP (*Simple Mail Transfer Protocol* protocolo de transferência de mensagens eletrônicas – *e-mail*), e outros.

● Transporte – cria e faz manutenções de conexões realizando o controle de erros e fluxo de dados. A transmissão dos dados é feita através dos protocolos TCP e UDP.

● Internet – responsável por entregar, endereçar e reconstruir os pacotes. Tendo o protocolo IP (Internet Protocol) como referência. Todo host (dispositivo conectado em uma rede)recebe um endereço lógico de 32 b its, ou seja, um IP.

● Interface de rede – interliga as camadas superiores com a rede. As principais funções executadas dentro desta camada são encapsulamento (proteção dos dados na rede), mapeamento, e endereçamento de endereços IP aos endereços físicos (endereços MAC, ex.: 0080.77d0.cd65).

O TCP é orientado à conexão e uma conexão entre o cliente e o servidor é estabelecida (aberta passiva) antes que os dados possam ser enviados. O handshake triplo (aberto ativo), retransmissão e detecção de erros aumenta a confiabilidade, mas aumenta a latência. Os aplicativos que não exigem serviço de fluxo de dados confiável podem usar o protocolo UDP (User Datagram Protocol), que fornece um serviço de datagrama sem conexão que prioriza o tempo em relação à confiabilidade.



Principais características:

- - Mais lenta que o protocolo UDP;
- - Faz checagem de erros;
- - Garante a entrega dos dados ao destino;
- - É um protocolo orientado à conexão;
- - Não permite Broadcasting, pois é unicast;
- - Faz a entrega ordenada dos bytes;

◦ O que é UDP ?

UDP (User Datagram Protocol) usa um modelo de comunicação simples sem conexão com um mínimo de mecanismos de protocolo. O UDP fornece somas de verificação para integridade de dados e números de porta para endereçar funções diferentes na origem e destino do datagrama. Ele não tem diálogos de handshake e, portanto, expõe o programa do usuário a qualquer falta de confiabilidade da rede subjacente; não há garantia de entrega, pedido ou proteção duplicada.

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

Principais características:

- É um protocolo simples e rápido;
- Faz checagem simples de erros (checksums);
- Não garante a entrega íntegra dos dados ao destino;
- É um protocolo connectionless;
- Permite Broadcasting (multiplex);
- Transmite mensagens em datagramas;
- Não verifica conexão antes de enviar a mensagem;
- Não reagrupa as mensagens de entrada e não fornece controle de fluxo.

◦ O que são camadas de rede?

Nas últimas duas décadas houve um grande aumento na quantidade e no tamanho das redes. Várias redes foram criadas, onde possuíam diferentes hardwares e softwares, tornando redes incompatíveis. Para tratar desse problema, a ISO (International Organization for Standardization, organização internacional de padronização e normas) realizou uma pesquisa sobre vários esquemas de rede. A ISO reconheceu a necessidade de se criar um modelo de rede para ajudar os desenvolvedores a implementar redes que poderiam comunicar-se e trabalhar juntas. Assim, a ISO lançou em 1984 o modelo de referência OSI.

O modelo de referência OSI permite a visualização das funções de rede que acontece em cada camada. Sobretudo, o modelo de referência OSI que é uma estrutura usada para entendermos como as informações trafegam através de uma rede. Além disso, você pode usar o modelo de referência OSI para visualizar como as informações, ou pacotes de dados, trafegam desde os programas aplicativos (por exemplo: planilhas, documentos, etc.), através de um meio de rede (cabos, etc.), até outros programas aplicativos localizados em outro computador de uma rede, mesmo se o remetente e o destinatário tiverem tipos diferentes de rede.

◦ O que é o modelo OSI ?

No modelo de referência OSI, existem sete camadas numeradas e cada uma ilustra uma função particular da rede . Essa separação das funções da rede é chamada divisão em camadas. Dividir a rede nessas sete camadas oferece as seguintes vantagens:

● Divide as comunicações de rede em partes menores e mais simples, facilitando sua compreensão.

● Padroniza os componentes de rede, permitindo o desenvolvimento e o suporte por parte de vários fabricantes.

● Possibilita a comunicação entre tipos diferentes de hardware e de software de rede.

● Evita que as modificações em uma camada afetem as outras, possibilitando maior rapidez no seu desenvolvimento.

Camada de aplicação

A camada de aplicação é a camada do modelo OSI mais próxima do usuário. Esta camada é a porta de entrada para a rede ou o sistema de comunicação, da forma como é vista pelos aplicativos que usam este sistema, ou seja, fornece um conjunto de funções para serem usadas pelos aplicativos que operam sobre o modelo OSI.
(ex. SNMP, HTTP, FTP).

Camada de apresentação

A camada de apresentação garante que a informação seja divulgada pela camada de aplicação legivelmente para outro sistema, sendo assim, codifica e converte dados com o propósito de fazer com que os sistemas falem a mesma língua.
(ex. encryption, ASCII, PNG, MIDI)

Suas principais funcionalidades são:

- Formatação de dados;
- Criptografia de dados;
- Compactação de dados.

Antes de receber e enviar os dados, a camada 6 (apresentação) do modelo OSI executa uma ou todas suas funcionalidades sobre os dados antes de encaminhá-los a próxima camada (camada de sessão).

Camada de sessão

A camada de sessão é responsável pela inicialização, gerenciamento e finalização de sessões entre o transmissor e receptor. Suas funcionalidades são fornecer seus serviços à camada de apresentação, manter os dados de diferentes aplicações separados uns dos outros, ou seja, oferecer recursos e serviços eficientes nos diálogos e conversações sobre a camada de sessão. (ex. Syn/Ack)

Camada de transporte

Está camada segmenta os dados e reconstruí os fluxos de dados provenientes de camadas superiores. Também provêm de comunicação ponto a ponto, onde estabelece uma conexão lógica entre aplicações origem e destino em uma rede.

A camada de transporte estabelece, mantém e termina corretamente os circuitos virtuais, e controle de fluxo de informação, detecção e recuperação de erros de transporte, garantindo qualidade nos serviços e confiabilidade. Ela oculta os detalhes das informações relacionadas às camadas superiores de rede, oferecendo transparência na transmissão dos dados. (ex. TCP, UDP, port numbers)

Dentro desta camada contém um conjunto de protocolos, mais conhecidos como pilha de protocolos ou TCP/IP(*Transmission Control Protocol / Internet Protocol*, é um conjunto de protocolos de comunicação). Os protocolos de referência dentro da pilha de protocolos são:

- TCP (Transmission Control Protocol) –responsável por verificar se os dados estão sendo enviados corretamente, ou seja, sem erros e na sequência certa, é o protocolo de controle de transmissão que fornece um circuito virtual entre as aplicações e o usuário final.

- UDP (User Datagram Protocol) – é o protocolo de datagramas (ou pacotes) que transporta dados sem confiabilidade entre receptor e transmissor.

Camada de rede

A camada de rede é responsável pelo encaminhamento dos dados através da interligação de redes, endereçamento de pacotes de dados, e conversão de endereços lógicos(IP)emendereçosfísicosouMAC.Dentrodamesma,acamada3(layer3)do modelo OSI, é onde trabalham os roteadores, promovendo serviços relacionados ao processo de encaminhamento. (ex. IP, routers)

Quando os pacotes são recebidos pelo roteador o dispositivo verifica o endereço IP de destino, caso o pacote não for destinado ao roteador citado, o roteador verifica em sua tabela de encaminhamento (base de dados armazenada em sua memória RAM).

As principais funções da camada de rede são:

- Não orientada a conexão;
- Sem garantia de entrega;
- Endereçamento lógico (IP) de pacotes;
- Escolha do melhor caminhamento através do encaminhamento.

Camada de enlace:

Está camada oferece aos dados segurança, conversão em bits dos pacotes vindos da camada de rede, realizando em seguida a transmissão através de um link físico (cabeamento). Os serviços prestados pela camada de enlace são dependentes dos protocolos que provêm entrega garantida entre enlaces, ou seja, desde o transmissor, passando por um único enlace, até chegar ao receptor. (ex. MAC, switches)

Os protocolos que trabalham dentro da camada de enlace possuem características importantes, como:

- Encapsular datagramas da camada superior (camada de rede);
- Enviar e receber quadros (unidades de dados);
- Detectar erros;
- Retransmissão dos dados;
- Controle de fluxo.

Camada de física

Nesta camada são definidas especificações elétricas, mecânicas, funcionais e de procedimentos. Onde é definida a transmissão de bits por um canal de comunicação, nível de voltagem, taxas de dados físicos, distância máxima de transmissão, conectores físicos. (ex. cable, RJ45)

A camada física do modelo OSI é a única que possui acesso físico ao meio de transmissão da rede, tendo como principal função adaptar o sinal lógico ao meio de transmissão.

Outras características importantes da camada física são:

- Estabelecimento e encerramento de conexões: ativa e desativa conexões físicas de acordo com as solicitações feitas pela camada de enlace
- Transferência de dados: a transmissão dos dados é realizada em bits de acordo com a ordem de chegada dos dados vindos da camada de enlace, e são devolvidos a camada de enlace na mesma ordem que chegaram.
- Gerenciamento de conexões: verifica o nível de qualidade das conexões físicas estabelecidas, monitorando taxas de erro, disponibilidade de serviço, taxa de transmissão, etc.

◦ O que é um servidor DHCP e o protocolo DHCP ?

O protocolo de configuração dinâmica de hosts (DHCP) é um protocolo de gerenciamento de rede usado em redes de protocolo de Internet por meio do qual um servidor DHCP atribui dinamicamente um endereço IP e outros parâmetros de configuração de rede a cada dispositivo em uma rede para que possam se comunicar com outras redes IP. Um servidor DHCP permite que os computadores solicitem endereços IP e parâmetros de rede automaticamente do provedor de serviços de Internet (ISP), reduzindo a necessidade de um administrador de rede ou um usuário atribuir manualmente endereços IP a todos os dispositivos de rede.

Um roteador ou gateway residencial pode ser habilitado para atuar como um servidor DHCP. A maioria dos roteadores de rede residencial recebe um endereço IP exclusivo globalmente dentro da rede ISP. Em uma rede local, um servidor DHCP atribui um endereço IP local a cada dispositivo conectado à rede.

Como ele faz isso?

Resumidamente, utilizando um modelo cliente-servidor, o DHCP faz o seguinte:

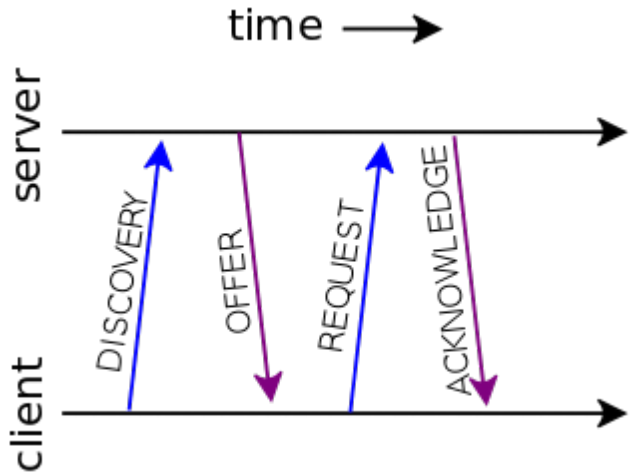
● Quando um computador (ou outro dispositivo) se conecta a uma rede, o host/cliente DHCP envia um pacote UDP em broadcast (destinado a todas as máquinas) com uma requisição DHCP (para a porta 68);

● Qualquer servidor DHCP na rede pode responder a requisição. O servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede e informações sobre os parâmetros de configuração dos clientes como gateway padrão, nome do domínio, servidor de nomes e servidor de horário. Os servidores DHCP que capturarem este pacote responderão (se o cliente se enquadrar numa série de critérios) para a porta 68 do host solicitante com um pacote com configurações onde constará, pelo menos, um endereço IP e uma máscara de rede, além de dados opcionais, como o gateway, servidores de DNS, etc.

O DHCP emprega um modelo de serviço sem conexão, usando o User Datagram Protocol (UDP). Ele é implementado com dois números de porta UDP para

suas operações, que são iguais ao protocolo de inicialização (BOOTP). **O número da porta UDP67 é a porta de destino de um servidor e o número de porta UDP 68 é usado pelo cliente.**

As operações DHCP se dividem em quatro fases: descoberta do servidor, oferta de aluguel de IP, solicitação de aluguel de IP e confirmação de aluguel de IP. Esses estágios são geralmente abreviados como DORA para descoberta, oferta, solicitação e confirmação.



O DHCP não pode usar TCP como protocolo de transporte porque o TCP requer que ambos os terminais tenham endereços IP exclusivos. No momento em que um host precisa usar o DHCP, ele não tem um endereço IP de onde possa originar os pacotes, nem tem o endereço IP do servidor DHCP. Portanto, ele usa 0.0.0.0 como o endereço IP de origem e 255.255.255.255 (transmissão) como o endereço IP de destino (isso é para DHCP - comportamento semelhante está presente para DHCPv6). Esses endereços IP não são endereços IP de host válidos e podem ser usados por vários clientes a qualquer momento. Portanto, uma conexão TCP não seria "única" por falta de um termo melhor. **Importante: o DHCP funciona para IPv4 e IPv6.**

◦ O que é um servidor DNS e o protocolo DNS ?

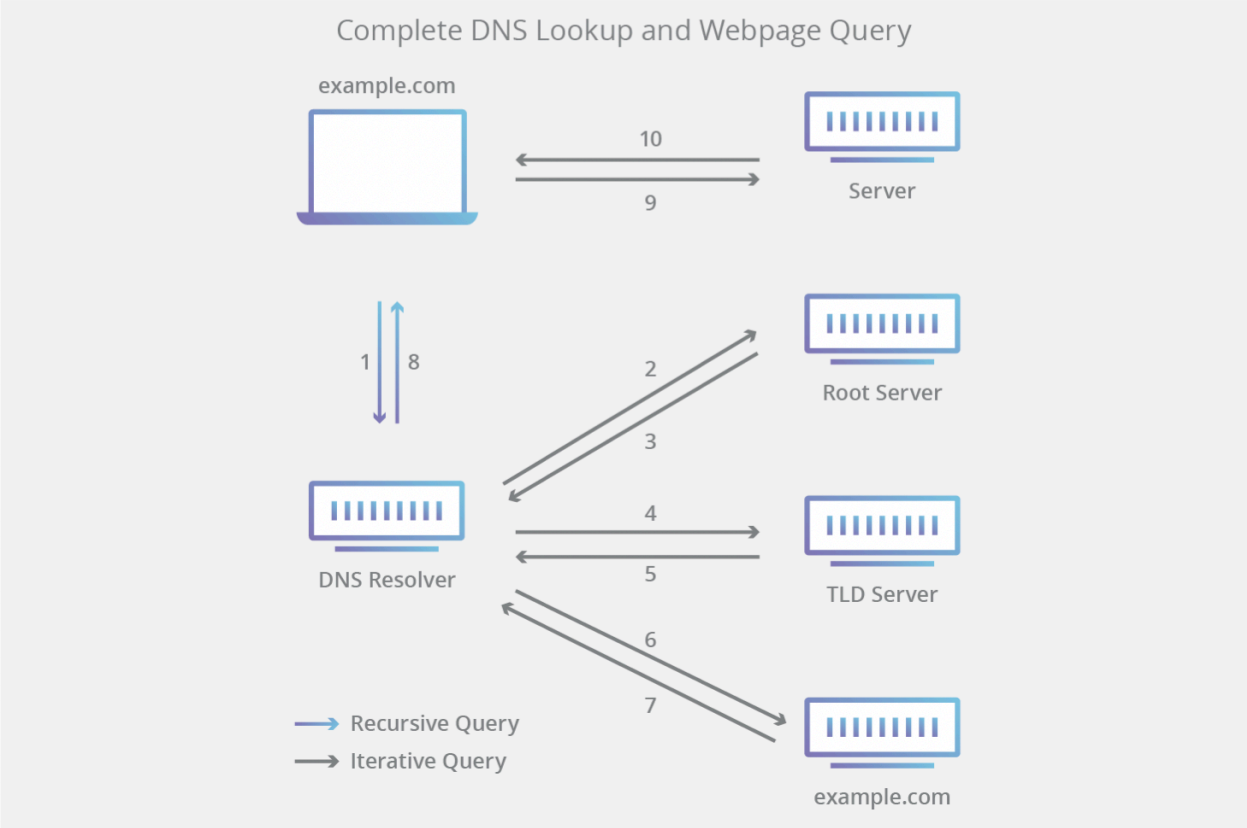
De forma clara e objetiva, um servidor DNS (Domain Name System) é um computador que contém um banco de dados com endereços de IP públicos e os seus respectivos domínios associados.

Vale ressaltar que existem diversos deles por aí: eles executam softwares específicos e se comunicam entre si com base em protocolos especiais. Em termos práticos, eles fazem a ligação entre um domínio e um número de IP, que nada mais é do que a identificação do servidor para o qual o domínio está apontado.

Para facilitar ainda mais, um servidor DNS é o sistema que traduz o “site.com.br” para um endereço de IP, por exemplo, 151.101.129.121. Isso ocorre quando o domínio é digitado nos navegadores.

Sem esse sistema, você teria que gravar os IPs e digitá-los no navegador. Imagine ter que digitar “179.184.115.223” para acessar o Google e “31.13.85.36” para o Facebook. Para contextualizar, podemos dizer que o DNS desempenha uma função bastante similar a uma lista telefônica. Porém, em vez de associar pessoas/empresas aos seus telefones, ele relaciona os nomes aos seus endereços de IP.

O recursor DNS (também conhecido como resolvedor DNS) é um servidor que recebe a consulta do cliente DNS e, em seguida, interage com outros servidores DNS para localizar o IP correto. Depois que o resolvedor recebe a solicitação do cliente, ele se comporta realmente como um cliente, consultando os outros três tipos de servidores DNS em busca do IP correto.



Primeiro, o resolvedor consulta o nome servidor raiz. O servidor raiz é a primeira etapa na tradução (resolução) de nomes de domínio legíveis por humanos em endereços IP. O servidor raiz então responde ao resolvedor com o endereço de um servidor DNS de domínio de nível superior (TLD) (como .com ou .net) que armazena as informações de seus domínios.

Em seguida, o resolvedor consulta o servidor TLD. O servidor TLD responde com o endereço IP do servidor de nomes autorizado do domínio. O recursor então consulta o servidor de nomes autorizado, que responderá com o endereço IP do servidor de origem.

O resolvedor finalmente passará o endereço IP do servidor de origem de volta ao cliente. Usando esse endereço IP, o cliente pode então iniciar uma consulta diretamente ao servidor de origem, e o servidor de origem responderá enviando dados do site que podem ser interpretados e exibidos pelo navegador da web.

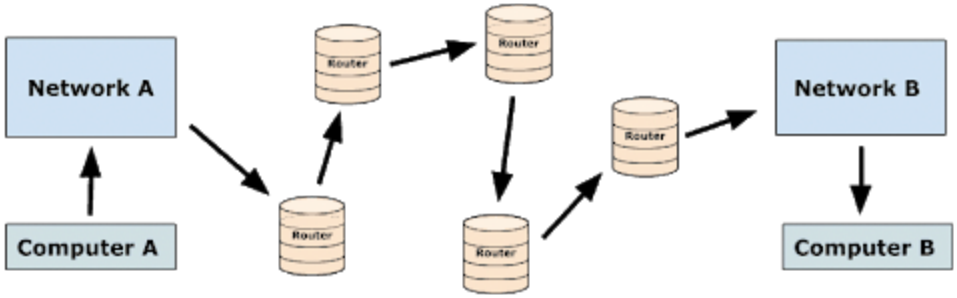
Além do processo descrito acima, os resolvedores recursivos também podem resolver consultas DNS usando dados em cache. Depois de recuperar o endereço IP correto para um determinado site da Web, o resolvedor armazenará essas informações em seu cache por um período limitado de tempo. Durante esse período, se qualquer outro cliente enviar solicitações para esse nome de domínio, o resolvedor pode pular o processo de pesquisa DNS típico e simplesmente responder ao cliente com o endereço IP salvo no cache.

◦ Quais são as regras para fazer 2 dispositivos se comunicarem usando endereços IP ?

Se eles estiverem na mesma rede (rede local), é fácil. Eles se comunicam diretamente um com o outro. Caso contrário, se eles estiverem em redes diferentes, use endereços IP válidos para hosts (se eles não forem endereços IP públicos, você precisará traduzi-los para públicos com NAT), o resto é história (roteadores, protocolos de transporte, camadas de rede, muitos etapas e validações, ...) rs;)

◦ Como funciona o roteamento com IP ?

O roteamento IP descreve o processo de determinação do caminho para os dados seguirem em para navegar de um computador ou servidor para outro. Um pacote de dados passa de seu roteador de origem por uma teia de roteadores em muitas redes até que finalmente chega ao roteador de destino usando um algoritmo de roteamento. O algoritmo de roteamento leva em consideração fatores como o tamanho de um pacote e seu cabeçalho para determinar a rota mais eficiente para o destino. Quando um pacote chega a um roteador, os endereços de origem e destino do pacote são usados em conjunto com uma tabela de roteamento (liste que contém as rotas para uma determinada rede) para determinar o endereço do próximo salto. Esse processo é repetido para o próximo roteador usando sua própria tabela de roteamento até que o pacote alcance seu destino. Como os dados são divididos em pacotes, cada pacote viaja independentemente um do outro e é tratado como tal. Como resultado, cada pacote pode ser enviado por uma rota diferente ao destino, se necessário.



O host possui várias interfaces de rede. *eth0* é o nome da interface da placa de interface de rede que representa uma porta Ethernet. *ppp0* é uma interface *PPPoE*, que é configurada como rota padrão neste exemplo.

Uma rota padrão é reconhecida pelo destino *0.0.0.0* e o sinalizador *G*. Um roteador de rede é identificado pela máscara de rede *255.255.255.255* e o sinalizador *H.*

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         71.46.14.1      0.0.0.0         UG    0      0        0 ppp0
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 eth0
71.46.14.1      0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
192.168.1.0     192.168.96.1    255.255.255.0   UG    0      0        0 eth0
192.168.96.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Link

https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ip-routing-explained

◦ O que é um gateway padrão para roteamento ?

Um gateway padrão é o nó em uma rede de computadores que usa o protocolo de Internet adequado que atende ao host de encaminhamento (roteador) para outras redes quando nenhuma outra especificação de rota corresponde ao endereço IP de destino de um pacote.

Um gateway é um nó de rede que serve como ponto de acesso a outra rede, geralmente envolvendo não apenas uma mudança de endereçamento, mas também uma tecnologia de rede diferente. Definido de forma mais restrita, um roteador apenas encaminha pacotes entre redes com diferentes prefixos de rede. A pilha de software de rede de cada computador contém uma tabela de roteamento que especifica qual interface é usada para transmissão e qual roteador na rede é responsável por encaminhar para um conjunto específico de endereços. Se nenhuma dessas regras de encaminhamento for apropriada para um determinado endereço de destino, o gateway padrão será escolhido como o roteador de último recurso. O gateway padrão pode ser especificado pelo comando r oute para configurar a tabela de roteamento do nó e a rota padrão.

◦ O que é uma porta do ponto de vista do IP e para que ela é usada ao se conectar a outro dispositivo ?

s portas são identificadas para cada combinação de protocolo e endereço por números não assinados de 16 bits, comumente conhecidos como o número da porta. Os protocolos mais comuns que usam números de porta são o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

Um número de porta está sempre associado a um endereço IP de um host e ao tipo de protocolo de comunicação. Ele completa o destino ou endereço de rede de origem de uma mensagem. Números de porta específicos são comumente reservados para identificar serviços específicos, de modo que um pacote que chega possa ser facilmente encaminhado para um aplicativo em execução.

Uma conexão entre dois computadores usa um soquete. Um soquete é a combinação de endereço IP e porta.

Imagine-se sentado em seu PC em casa, e você tem duas janelas do navegador abertas.

A conexão com o Google seria:

Seu PC - IP1 + porta 60200 ——— Google IP2 + porta 80 (porta padrão)

A combinação IP1 + 60200 = soquete no computador cliente e IP2 + porta 80 = soquete de destino no servidor Google.

◦ EXTRAS - Apenas para “diversão” :) PING

Ping é um utilitário de software de administração de rede de computadores usado para testar a acessibilidade de um host em uma rede de protocolo da Internet (IP). Ele está disponível para praticamente todos os sistemas operacionais com capacidade de rede, incluindo a maioria dos softwares de administração de rede incorporados.

Ping mede o tempo de viagem final para mensagens enviadas do host de origem para um computador de destino que é ecoado de volta para a origem. O nome vem de terminologia de sonar ativo que envia um pulso de som e ouve o eco para detectar [1] objetos debaixo d'água.

O ping opera enviando pacotes de solicitação de eco do protocolo ICMP (Internet Control Message Protocol) para o host de destino e aguardando uma resposta de eco ICMP. O programa relata erros, perda de pacote e um resumo estatístico dos resultados, normalmente incluindo o mínimo, o máximo, os tempos médios de ida e volta e o desvio padrão da média.

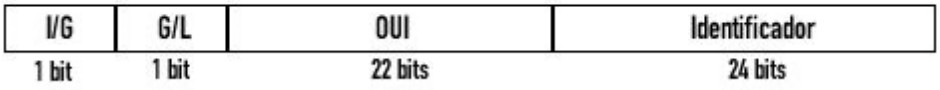
Pacote ICMP

IPv4 Datagram

	Bits 0–7	**Bits 8–15**	**Bits 16–23**	**Bits 24–31**
Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Header Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

◦ Endereço MAC

Um endereço de controle de acesso à mídia (endereço MAC) de um dispositivo é um identificador único atribuído a uma interface de rede (ou Network Interface Controller - NIC). Para comunicações dentro de um segmento de rede, é usado como endereço de rede para a maioria das tecnologias de rede IEEE 802, incluindo Ethernet, Wi-Fi e Bluetooth. No modelo Open Systems Interconnection (OSI), os endereços MAC são usados na subcamada de protocolo do controle de acesso ao meio da camada de enlace de dados. Como normalmente representado, os endereços MAC são reconhecíveis como seis grupos de dois dígitos hexadecimais, separados por hífens, dois pontos ou nenhum separador.(48 bits, 12 caracteres hexadecimais).



● I/G (Individual/Group) – corresponde ao bit que indica que se trata de um endereço MAC individual, se o valor for 0, ou a um endereço broadcast ou multicast se o valor for 1.

● G/L (Global/Local) – corresponde ao bit que indica que se trata de um endereço MAC de âmbito global (ex. administrado pelo IEEE) ou localmente (ex. DECnet);

● OUI – Identificador unívoco, atribuído pelo IEEE a cada fabricante.

● Identificador – identificador da interface em si.

◦ PORTAS

Os aplicativos podem usar soquetes de datagrama para estabelecer comunicações host-a-host. Um aplicativo liga um soquete ao seu ponto final de transmissão de dados, que é uma combinação de um endereço IP e uma porta. Dessa forma, o UDP fornece multiplexação de aplicativos. Uma porta é uma estrutura de software que é identificada pelo número da porta, um valor inteiro de 16 bits, permitindo números de porta entre 0 e 65535. A porta 0 é reservada, mas é um valor de porta de origem permitido se o processo de envio não esperar mensagens em resposta.
A Internet Assigned Numbers Authority (IANA) dividiu os números das portas em [4] três intervalos. Os números de porta de 0 a 1023 são usados para comum, bem conhecidos serviços. Em sistemas operacionais do tipo Unix, o uso de uma dessas portas requer permissão de operação do superusuário. Os números de porta de 1024 a 49151 são as portas registradas usadas para serviços registrados da IANA. As portas 49152 a 65535 são portas dinâmicas que não são oficialmente designadas para nenhum serviço específico e podem ser usadas para qualquer finalidade. Eles também podem ser usados como portas efêmeras, que o software em execução no host pode usar para criar pontos de extremidade de comunicação dinamicamente conforme

necessário. Esse canal virtual garante que uma aplicação que iniciou uma chamada pela porta 80, como por exemplo, o uso de um navegador para abrir uma página HTTP no computador A, encontre, no destino, o servidor web que fornecerá a página HTTP solicitada também por uma porta 80. Assim se evita que a informação seja direcionada erroneamente para outra aplicação, como por exemplo, um servidor FTP (porta 21).

Port number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

◦ NAT (Network Address Translation)

Sabendo que os IPs públicos (IPv4) são um recurso limitado e actualmente escasso, o NAT tem como objectivo poupar o espaço de endereçamento público, recorrendo à IPs privados.

Os endereços públicos são geridos por uma entidade reguladora, são pagos, e permitem identificar univocamente uma máquina (PC, routers,etc) na Internet.

Por outro lado os endereços privados apenas fazem sentido num domínio local e não são conhecidos (encaminháveis) na Internet, sendo que uma máquina configurada com um IP privado terá de sair para a Internet através de um IP público.

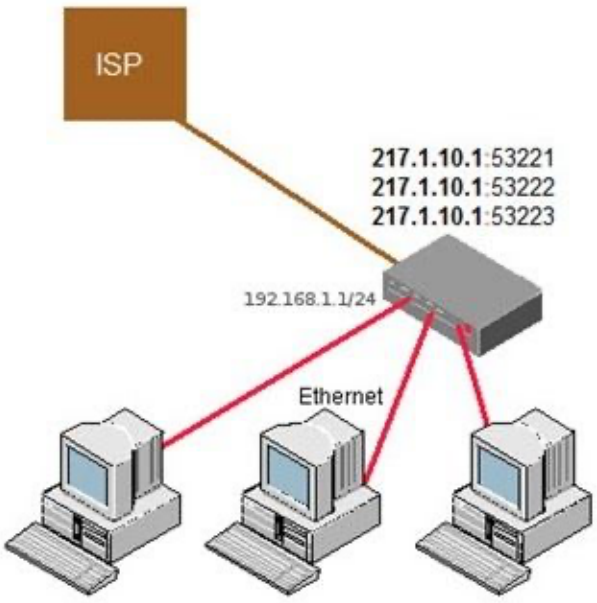
A tradução de um endereço privado num endereço público é então definido como NAT e está definido no RFC 1631.

Existem 3 tipos de NAT:

- NAT Estático – Um endereço privado é traduzido num endereço público.

- NATDinâmico–Existeumconjuntodeendereçospúblicos(pool),que as máquinas que usam endereços privados podem usar.

- NAT Overload (PAT) – Esta é certamente a técnica mais usada. Um exemplo de PAT é quando temos 1 único endereço público e por ele conseguimos fazer sair várias máquinas (1:N). Este processo é conseguido, uma vez que o equipamento que faz PAT utiliza portas que identificam univocamente cada pedido das máquinas locais (ex: 217.1.10.1:53221, 217.1.10.1:53220, etc) para o exterior.



O PAT é a técnica presente na maioria dos equipamentos de rede que usamos. Considerando por exemplo um router WiFi. É possível ligarmos/associarmos vários clientes a esse equipamento e estes são configurados (ou adquirem) um endereço privado.

No entanto todos eles podem ter acesso à Internet através de um único endereço público. Como já referido, tal é possível porque a técnica de NAT, recorre às portas para distinguir os pedidos das máquinas internas. Na prática existem 65536 portas, no entanto por norma apenas são usadas as portas dinâmicas (de 49152 a 65535).