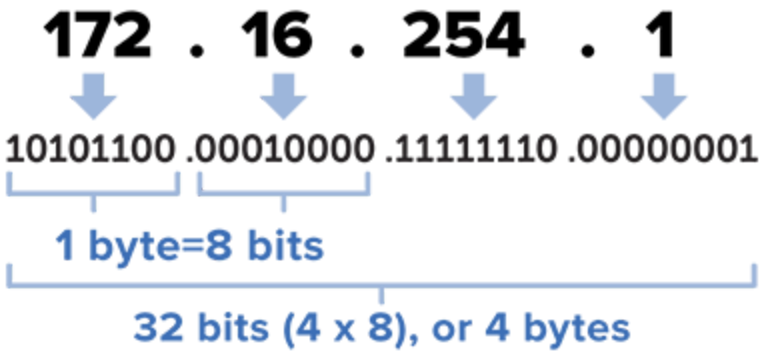
NETWHAAAAAAAAAAAAAT?

BY LNIEHUES

◦ What is an IP address

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. O IP, na versão 4 do IP (**IPv4**), **é um número de 32 bits** oficialmente escrito 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 endereço **127.0.0.1** 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.**

Each IP address must be unique on its own network. Networks can be isolated from one another, and they can be bridged and translated to provide access between distinct networks. A system called **Network Address Translation (NAT)**, allows the addresses to be rewritten when packets traverse network borders to allow them to continue on to their correct destination. This allows the same IP address to be used on multiple, isolated networks while still allowing these to communicate with each other if configured correctly.

◦ What is a Netmask

A subnet mask is a 32- or 128-bit number that segments an existing IP address in a TCP/IP network. It is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network. **Subnet mask divides the IP address into a network address and host address, hence to identify which part of IP address is reserved for the network and which part is available for host use.** Once given the IP address and its subnet mask, the network address (subnet) of a host can be determined. Usually, subnet calculators are readily available online that help divide an IP network into subnets.

EXAMPLE:

In the picture below, the first three parts of the IP address belongs to the IP network (42 bits selected to create networks), which is determined by the subnet mask. 0 is the lowest address that is available in the fourth part of the IP address. The computer thus

belongs to the IP network 101.102.103.0. The fourth part (.5) of the IP address shows which host address that the computer is using on the IP network (8 bits to create hosts).

◦ What is the subnet of an IP with Netmask

Subnetting is the process to divide the larger network into smaller sub-networks (subnets). We always reserve an IP address to identify the subnet and another one to identify the broadcast address within the subnet. Subnetting breaks up larger networks into small parts, which **is more efficient and would conserve a great amount of addresses.** The smaller networks, therefore, created smaller broadcasts that generate less broadcast traffic. Besides, subnet also simplifies fault troubleshooting by isolating network problems down to their specific existence.

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 hospedeiro ou rede específicos.

◦ What is the broadcast address of a subnet

A broadcast address is an IP address that is used to target all systems on a specific subnet network instead of single hosts. In other words broadcast address allows information to be sent to all machines on a given subnet rather than to a specific machine. The broadcast address of any IP address can be calculated by taking the bit compliment of the subnet mask, sometimes referred to as the reverse mask and then applying it with a bitwise OR calculation to the IP address in question. The last IP address after filtering through netmask.

EXAMPLE:

If the IP address is 192.168.12.220 and subnet mask is 255.255.255.128 then the broadcast address can be deduced in the following manner.

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

◦ What are the different ways to represent an IP address with the Netmask

- Dotted decimal :- It is represented by decimal number in which 32 Bit IP address is divided in four octets separated by '.'.

  Ex.: 128.0.0.0 | 127.0.0.0/8 | 192.0.2.0/24

- 2) Binary representation:- In this IP address is represented by binary numbers 0 or 1 with octets separated by '.'.

  Ex.: 11000000.10101000.00001100.11011100

- 3) Hexadecimal representation:- It is represented by hexadecimal.

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

◦ What are the differences between public and private IPs

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).

◦ What is a class of IP addresses

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 128 bits, 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.**

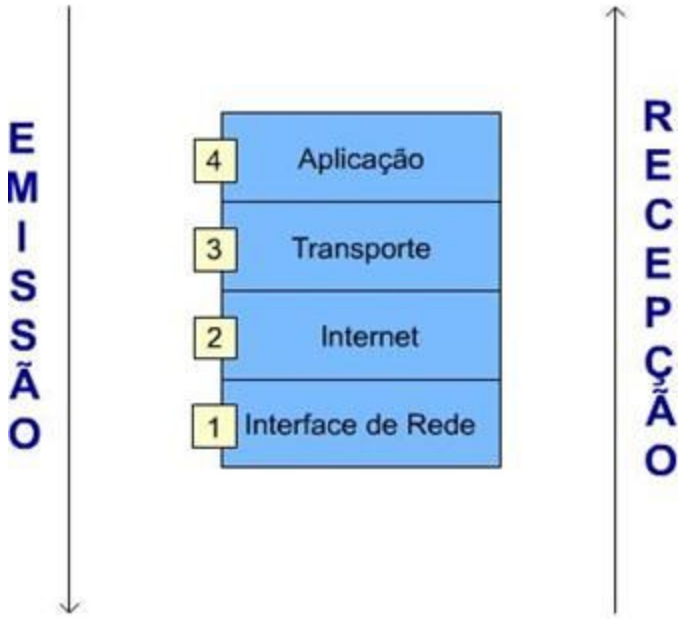
◦ What is TCP

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.) ...																															

It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite.

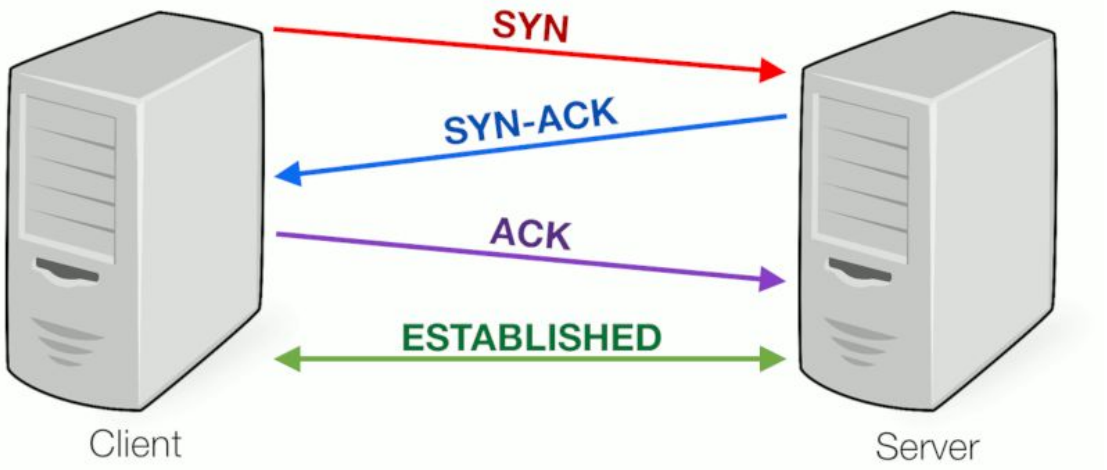


- Aplicação – usada pelos programas para comunicação em rede, alguns protocolos pertencentes a camadas são: HTTP (*HyperText Transfer Protocol Secure*, protocolo de transferência de hipertexto), FTP, SMTP (*Simple Mail*

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 *bits*, 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).

TCP is connection-oriented, and a connection between client and server is established (passive open) before data can be sent. Three-way handshake (active open), retransmission, and error-detection adds to reliability but lengthens latency. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that prioritizes time over reliability.



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;

◦ What is UDP

UDP(User Datagram Protocol) uses a simple connectionless communication model with a minimum of protocol mechanisms. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network; there is no guarantee of delivery, ordering, or duplicate protection.

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.

◦ What are the network layers

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.

◦ What is the OSI model

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. (e.g. 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. (e.g. 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. (e.g. 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. (e.g. 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) em endereços físicos ou MAC. Dentro da mesma, a camada 3 (*layer 3*) do modelo OSI, é onde trabalham os roteadores, promovendo serviços relacionados ao processo de encaminhamento. (e.g. 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. (e.g. 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. (e.g. 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.

◦ What is a DHCP server and the DHCP protocol

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.

A router or a residential gateway can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.

Como ele faz isso?

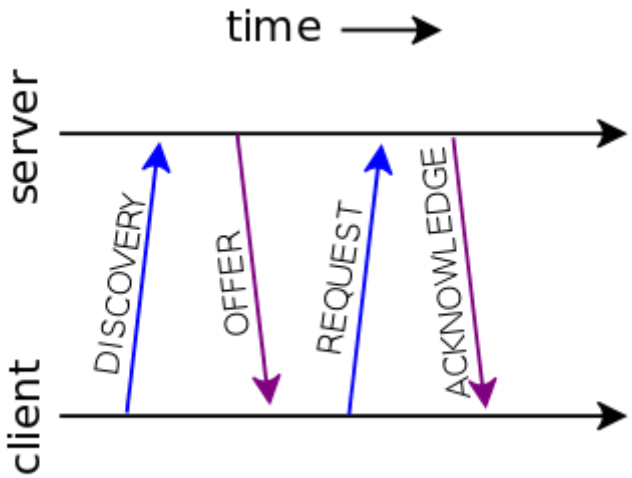
Resumidamente, utilizando um modelo cliente-servidor, o DHCP faz o seguinte:

● 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.

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the bootstrap protocol (BOOTP). **UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client.**

DHCP operations fall into four phases: server discovery, IP lease offer, IP lease request, and IP lease acknowledgement. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgement.



DHCP cannot use TCP as the transport protocol because TCP requires both end-points to have unique IP addresses. At the time a host is required to use DHCP, it does not have an IP address it can source the packets from, nor does it have the IP address of the DHCP server. So it uses `0.0.0.0` as the source IP address and `255.255.255.255` (broadcast) as the destination IP address (this is for DHCP - similar behaviour is present for DHCPv6). These IP addresses are not valid host IP addresses and can be used by multiple clients at any time. So a TCP connection wouldn't be "unique" for lack of a better term. **Important: DHCP works for both IPv4 and IPv6.**

◦ What is a DNS server and the DNS protocol

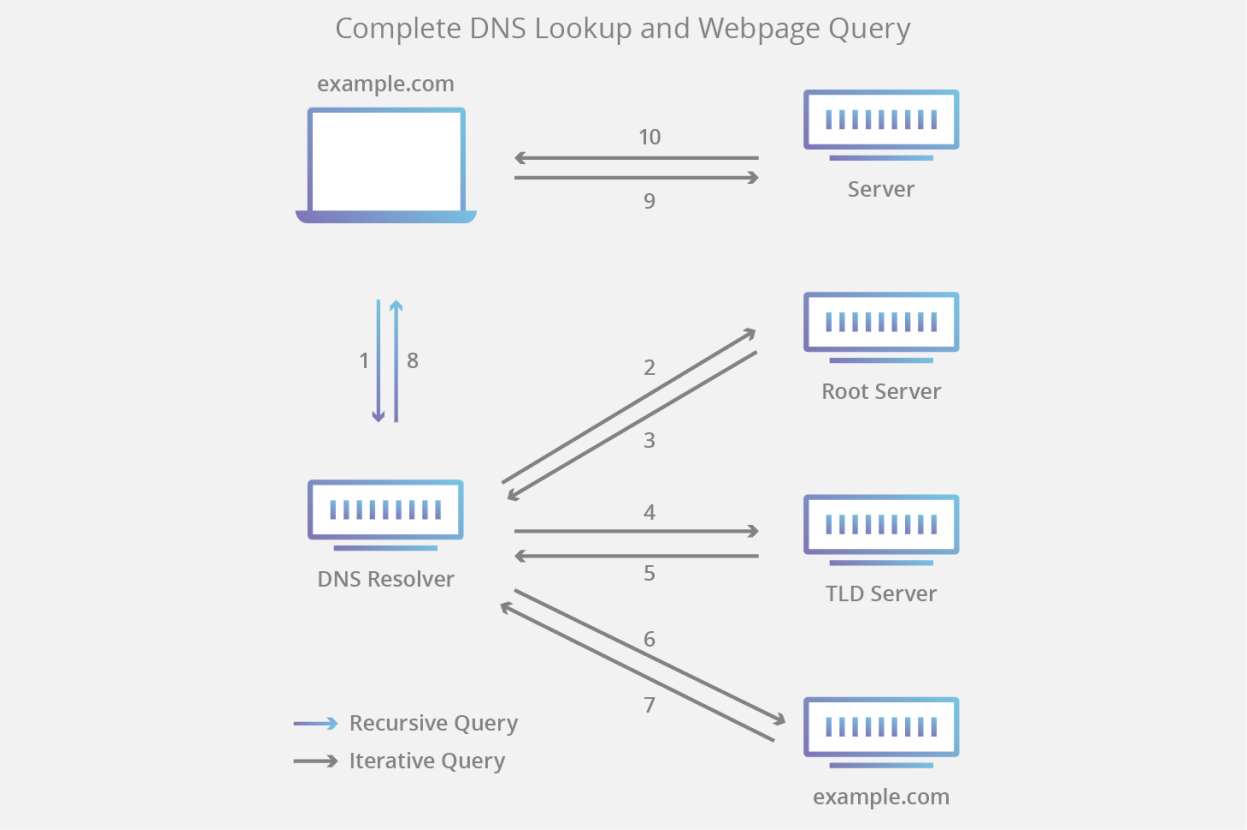
De forma clara e objetiva, um servidor DNS (Domain Name System) é um computador que contém um banco de dados com endereços de IP públicos e os seus respectivos domínios associados.

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.

The DNS recursor (also referred to as the DNS resolver) is a server that receives the query from the DNS client, and then interacts with other DNS servers to hunt down the correct IP. Once the resolver receives the request from the client, the resolver then actually behaves as a client itself, querying the other three types of DNS servers in search of the right IP.



First the resolver queries the root nameserver. The root server is the first step in translating (resolving) human-readable domain names into IP addresses. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net) that stores the information for its domains.

Next the resolver queries the TLD server. The TLD server responds with the IP address of the domain's authoritative nameserver. The recursor then queries the authoritative nameserver, which will respond with the IP address of the origin server.

The resolver will finally pass the origin server IP address back to the client. Using this IP address, the client can then initiate a query directly to the origin server, and the origin server will respond by sending website data that can be interpreted and displayed by the web browser.

In addition to the process outlined above, recursive resolvers can also resolve DNS queries using cached data. After retrieving the correct IP address for a given website, the resolver will then store that information in its cache for a limited amount of time. During this time period, if any other clients send requests for that domain name, the resolver can skip the typical DNS lookup process and simply respond to the client with the IP address saved in the cache.

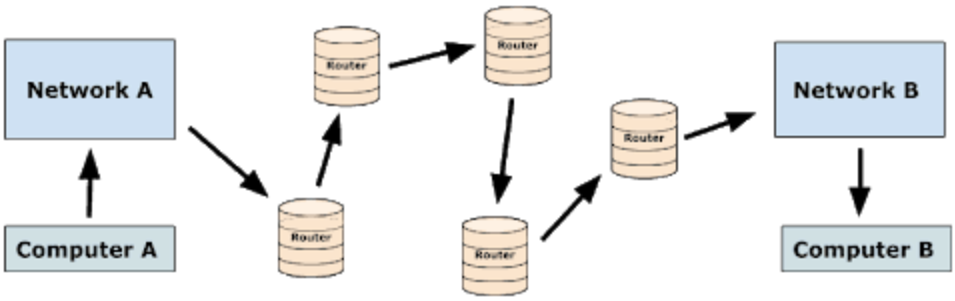
◦ What are the rules to make 2 devices communicate using IP addresses

If they are in the same network (local network) then it's easy peasy. They communicate directly to each other. Otherwise, if they are on different networks use valid IP addresses for hosts (if they are not public IP addresses you will need to translate them to public with NAT), the rest is story (Routers, transportation protocols, network layers, a lot of stages and validations, ...) rs ;)

◦ How does routing work with IP

IP Routing describes the process of determining the path for data to follow in order to navigate from one computer or server to another. A packet of data traverses from its source router through a web of routers across many networks until it finally reaches its destination router using a routing algorithm. The routing algorithm takes into account factors such as the size of a packet and its header to determine the most efficient route to the destination. When a packet has reached a router, the source and destination address of the packet are used in conjunction with a routing table (list that

contains the routes to a certain network) to determine the next hop address. This process is repeated for the next router using its own routing table until the packet has reached its destination. Because the data is divided into packets, each packet travels independently from each other and is treated as such. As a result, each packet can be sent through a different route to the destination if necessary.



The host has several network interfaces. *eth0* is the interface name of the network interface card representing an Ethernet port. *ppp0* is a PPPoE interface, which is configured as the default route in this example.

A default route is recognized by the destination *0.0.0.0* and the flag *G*. A network router is identified by the network mask *255.255.255.255* and the flag *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

◦ What is a default gateway for routing

A default gateway is the node in a computer network using the internet protocol suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.

A gateway is a network node that serves as an access point to another network, often involving not only a change of addressing, but also a different networking technology. More narrowly defined, a router merely forwards packets between networks with different network prefixes. The networking software stack of each computer contains a routing table that specifies which interface is used for transmission and which router on the network is responsible for forwarding to a specific set of addresses. If none of these forwarding rules is appropriate for a given destination address, the default gateway is chosen as the router of last resort. The default gateway can be specified by the route command to configure the node's routing table and default route.

◦ What is a port from an IP point of view and what is it used for when connecting to another device

Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number. The most common protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

A port number is always associated with an IP address of a host and the protocol type of the communication. It completes the destination or origination network address of a message. Specific port numbers are commonly reserved to identify specific services, so that an arriving packet can be easily forwarded to a running application.

A connection between two computers uses a **socket.** *A socket is the combination of **IP address plus port.***

Imagine sitting on your PC at home, and you have two browser windows open.

The connection to Google would be:

Your PC – **IP1**+port 60200 ——– Google IP2 +port **80** (standard port)

The combination IP1+60200 = the socket on the client computer and **IP2 + port 80** = destination socket on the Google server.

EXTRASSSSSSSS - JUST FOR "FUN" :)

◦ PING

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.[1]

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including

the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

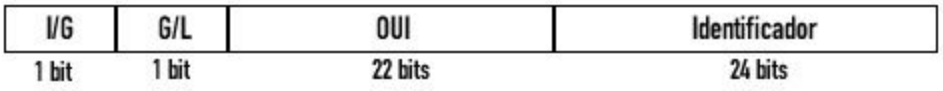
ICMP packet

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			

◦ MAC ADDRESS

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.

◦ PORTS

Applications can use datagram sockets to establish host-to-host communications. An application binds a socket to its endpoint of data transmission, which is a combination of an IP address and a port. In this way, UDP provides application multiplexing. A port is a software structure that is identified by the port

number, a 16 bit integer value, allowing for port numbers between 0 and 65535. Port 0 is reserved, but is a permissible source port value if the sending process does not expect messages in response.

The Internet Assigned Numbers Authority (IANA) has divided port numbers into three ranges.[4] Port numbers 0 through 1023 are used for common, well-known services. On Unix-like operating systems, using one of these ports requires superuser operating permission. Port numbers 1024 through 49151 are the registered ports used for IANA-registered services. Ports 49152 through 65535 are dynamic ports that are not officially designated for any specific service, and may be used for any purpose. These may also be used as ephemeral ports, which software running on the host may use to dynamically create communications endpoints as needed.

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.

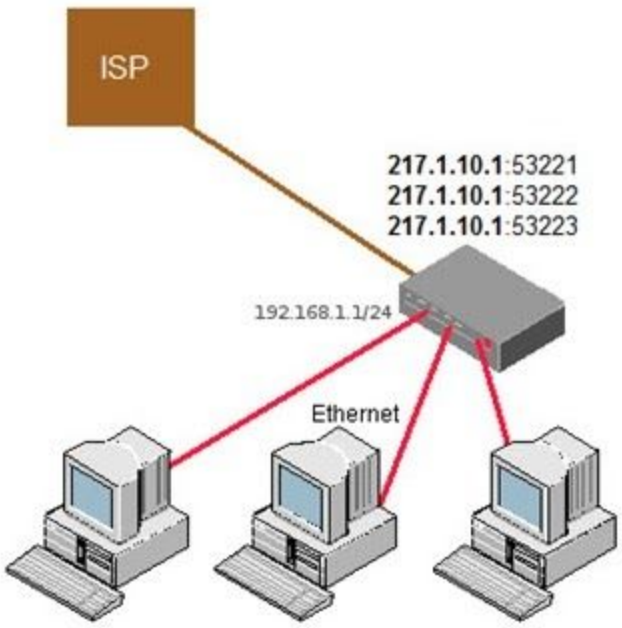
Os endereços públicos são geridos por uma entidade reguladora, são pagos, e permitem identificar univocamente uma máquina (PC, routers,etc) na Internet.

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.
- NAT Dinâmico – Existe um conjunto de endereços públicos (*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).