

ROTEIRO 1

1) Qual a topologia da sua rede? Quais outras topologias existem?

Primeiramente, tem-se que a topologia de uma rede está relacionada com a forma de como os elementos de uma rede de comunicação estão organizados. Assim, as topologias de rede são essenciais para ter mais organização, performance e usabilidade, que atualmente são características necessárias ao implementar uma rede de computadores.

E esse conceito é aplicado tanto de uma maneira física como de maneira lógica. Dessa forma, existem dois tipos de topologias: a física e a lógica. A primeira – física – representa como as redes são conectadas fisicamente com os cabos, e o meio de conexão dos dispositivos das redes como os nós (switches), logo, é por meio das estratégias de organização, cabeamento e disposição das máquinas que a topologia física pode ser definida. Por sua vez, a topologia lógica diz respeito ao modo que os sinais agem sobre os meios de rede, ou seja, como os dados são transmitidos através da rede a partir de um dispositivo para outro, mas sem levar em consideração a interligação física dos dispositivos, considerando mais os ajustes que dependem de uma interface como softwares, recursos de nuvem, roteadores, entre outros, com o objetivo de conectar os nós a rede com um tráfego menor e mais eficiente.

Dentro da categoria de topologia física, temos as seguintes opções: estrela, anel, árvore, barramento, híbrida, malha e ponto a ponto. A mais comum dentre essas é a topologia estrela, que utiliza cabos de par trançado e um concentrador que é um ponto central da rede, sendo que esse ponto retransmite todos os dados para todas as estações, tendo a vantagem de tornar a localização de problemas mais fácil, já que caso um dos cabos, ou uma das portas do concentrador ou placa de rede estiver com problemas, apenas o nó ligado ao componente defeituoso será afetado.

2) Quais casos uma rede ter mais de 1 gateway?

Antes de pensar nesses casos, primeiro precisamos entender o que é um gateway e como duas redes diferentes podem ser conectadas. Assim, um gateway é um conceito usado para descrever uma máquina que faz conexão entre duas ou mais redes e que oferece a conversão necessária em termos de hardware e software. Sendo que, há diferentes tipos de gateways, que são distinguidos através da camada em que estão operando na hierarquia de protocolos.

De maneira geral, a vantagem de ter uma rede interligada é a possibilidade de conectar computadores pelas redes, assim não queremos um gateway em muito baixo nível, caso contrário não poderemos fazer conexões entre diferentes tipos de redes. Além disso, também não queremos usar um gateway em um nível muito alto, pois senão a conexão só vai funcionar para determinadas aplicações. Logo, o nível do meio é o mais apropriado – camada de rede – e um roteador é um gateway que comuta pacotes nessa camada. Assim, para ter uma rede interligada, é preciso uma rede que tem roteadores (que tem gateways). Nesse caso a quantidade de gateways irá depender de quantos intermediários são necessários para

estabelecer uma conexão entre duas redes diferentes. Por exemplo, se quero estabelecer uma conexão com o “Blackboard” precisarei de quantos roteadores para estarmos conectados na mesma rede? Exato, pro BB precisa ter alguns roteadores a mais para evitar que caso aconteçam falhas tenha um backup. Pensa no e-commerce, quando a gente tem vários servidores para serviços replicados para manter o backup, aí a gente pode ter diferentes gateways e roteadores de diferentes redes, para não ficar a mercê de instabilidade (principalmente quando o número de requisições é maior: dia das mães): claro, vivo, gvt.

Liga uma rede interna à internet.

OBS: pense em redes como andares, hosts como apartamentos e gateways como escadas/elevadores.

Tipos de máscaras que são as regrinhas para saber se estamos em um mesmo andar, etc.

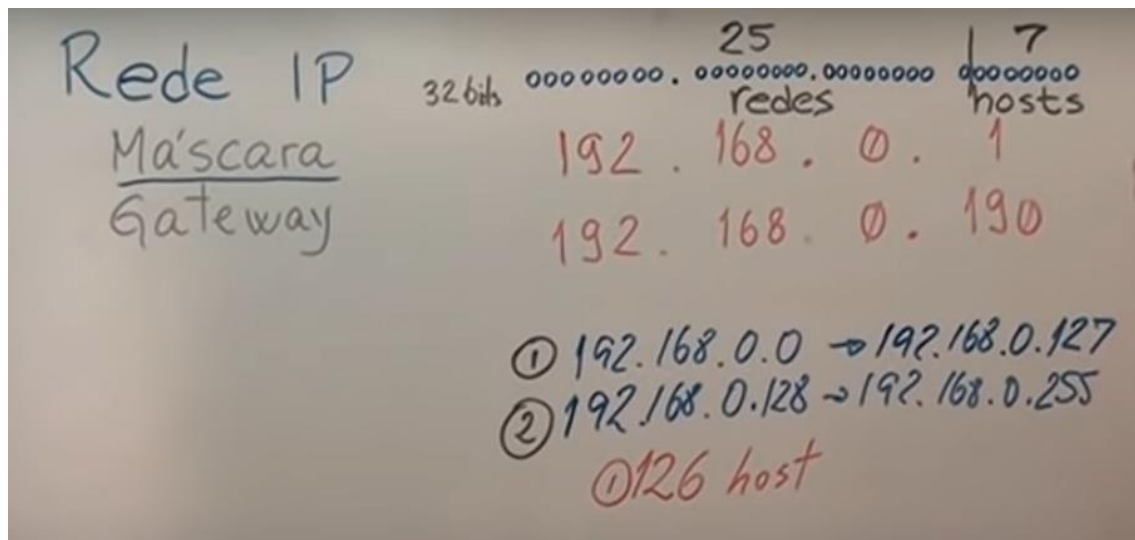
Usando máscara para 24 bits de redes e 8 para hosts, o intervalo de ips possíveis seria de: 192.168.0.0 – 192.168.0.255

Nem o primeiro e nem o último ip são usados (o último é o broadcast). O broadcast serve para quando uma máquina quer mandar uma informação para todas as outras dessa mesma rede recebam essa informação. Então se contarmos, dá 256 ips possíveis, mas nem o ip 0 (ip da rede) e o último (broadcast) serão usados, logo apenas 254 hosts em uma rede.

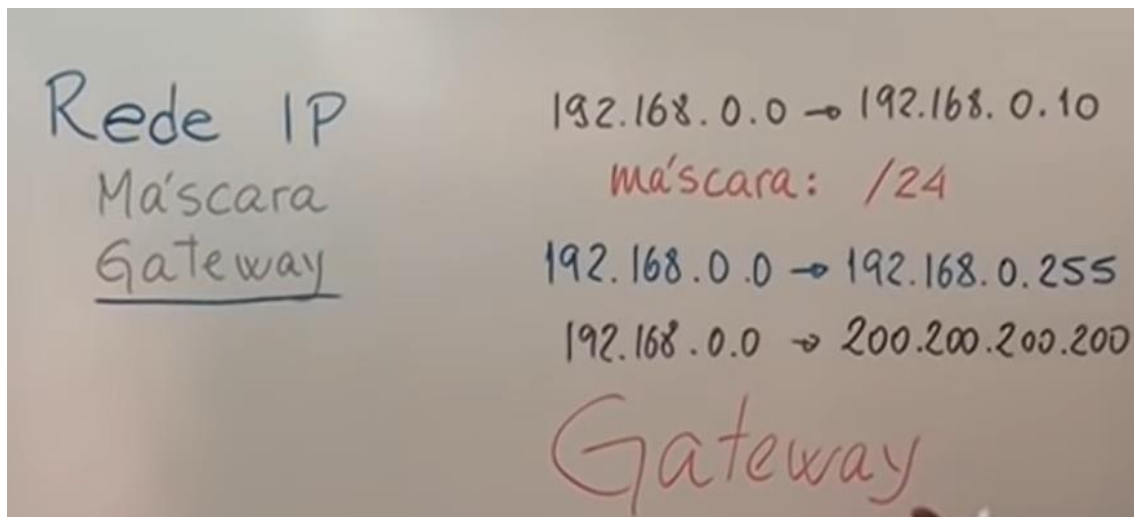
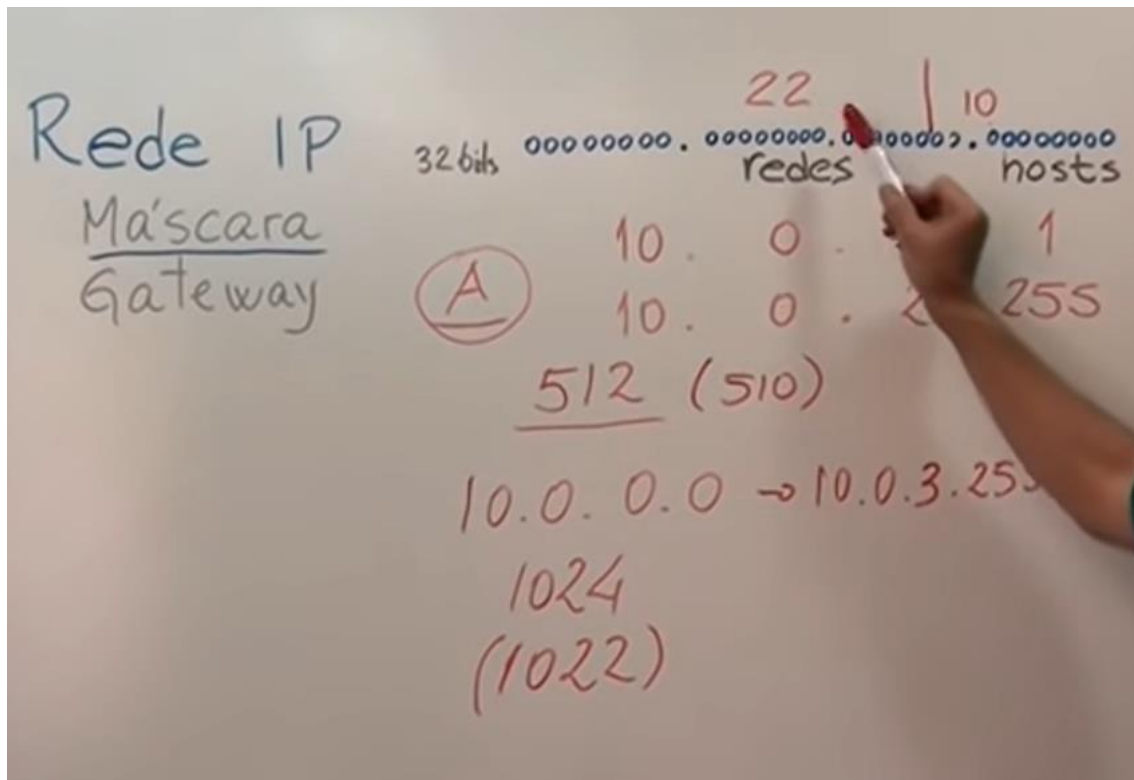
Outro exemplo, rede menor: usar apenas 7 bits para hosts e 25 bits para representar redes.

O primeiro da rede seria: 192.168.0.0 – 192.168.0.127. Tira os dois ips, fica com 126 ips.

Posso criar também subredes:



Cada classe tem uma máscara padrão. Então por exemplo, tem a classe A com 8 bits para redes e 24 bits para hosts, ou seja, para uma rede grande, que precisa de muitos hosts/equipamentos.



3) Quais as consequências de utilizar um DNS externo (por exemplo: 8.8.8.8) em uma rede privada?

Mais rápido, porém mais instável

O DNS (Domain Name System) é um sistema de nomes de domínios que foi criado em 1983. Assim como existem diversas maneiras de comunicar algo, como por exemplo na música, em que temos partituras que são como textos de notas musicais para serem tocadas, o computador também funciona de maneira diferente por dentro. Bem no fundo tudo é um conjunto de números, principalmente os uns e zeros. Mas então, por que quando queremos acessar sites nós digitamos nomes ao invés de números? Isso porque existe o que é chamado

de DNS, Domain Name System em inglês ou Sistema de Nomes de Domínio em português, que localiza e traduz para números IP os endereços que digitamos nos navegadores. Assim como no caso das ruas, uma forma de representá-las é através do CEP, que também é um conjunto de números, mas já pensou se para todas as ruas que você quisesse ir tivesse que chamá-las por números ao invés dos nomes? Pois é, seria uma confusão. E é por isso que o DNS foi criado, continuamos com os nomes, e esse trabalho de tradução para a máquina entender o que queremos, é feito por esse sistema - um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos

Existem diferentes tipos de DNS (agenda telefônica/ conversor de nomes legíveis em endereços ip), os públicos e os privados. No caso de um DNS público significa que está disponível para a população em geral que normalmente vem do seu provedor de serviços de internet ou de um provedor DNS dedicado. Já um DNS privado é normalmente usado por empresas para fornecer aos funcionários acesso mais fácil a sites ou endereços IP internos.

Quando existem problemas relacionados ao carregamento de sites (mesmo em boas velocidades de conexão) é possível que isso esteja relacionado ao DNS utilizado. Problemas assim são mais comuns em servidores públicos, pois estes acabam sendo mais vulneráveis a ataques e instabilidades.

Isso se dá por esses servidores serem compartilhados por um número muito grande de usuários, logo existem mais riscos. É partindo deste princípio que começam as diferenças entre servidores públicos e privados.

Quando uma rede de internet é instalada, é comum que sua rede DNS padrão seja pública e naturalmente, também seja a de sua provedora. Porém, usuários podem optar por [alterar o canal de conexão DNS](#) dos seus dispositivos para outro que seja mais conveniente.

4) O Switch estava originalmente em qual rede? Quantos IPs tem essa rede?

Cada computador troca informações usando o protocolo Ethernet e se conecta a um dispositivo de rede chamado switch, com um enlace ponto a ponto. Daí o nome. Um switch tem várias portas, cada qual podendo se conectar a um computador. A função do switch é repassar os pacotes entre os computadores que estão conectados a ela, usando o endereço em cada pacote para determinar para qual computador enviá-lo. Para montar LANs maiores, os switches podem ser conectados uns aos outros usando suas portas. O que acontece se você os conectar em um loop? A rede ainda funcionará? Felizmente, os projetistas pensaram nesse caso. É função do protocolo descobrir que caminhos os pacotes devem atravessar para alcançar o computador pretendido com segurança.

5) Quando acessou o roteador pela primeira vez ele estava na classe C. Quantas classes existem e qual é classe da rede do main?

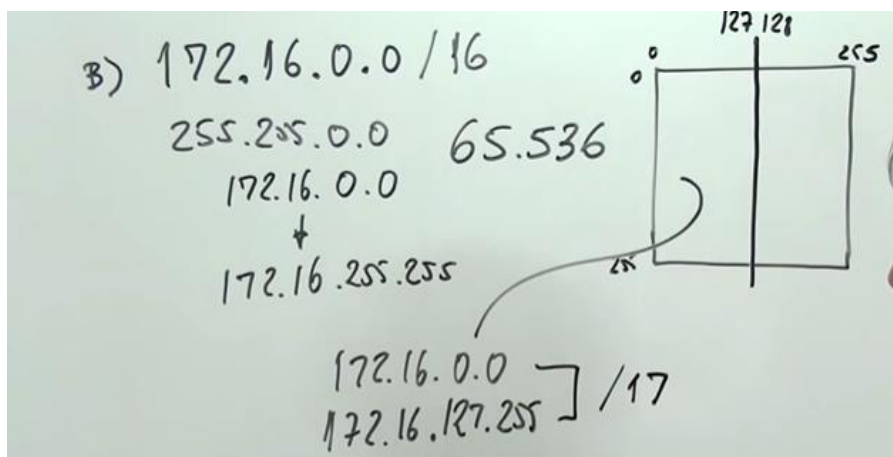
Foram criadas para dar suporte a números específicos de redes e hosts, contemplando capacidades diferentes entre eles e dividindo o espaço dos endereços IP. Temos três classes

principais: A, B e C. Há ainda a D, porém, é reservada somente para endereços Multicast, e a classe E, voltada para pesquisas. Os endereços reservados para classe A para uso interno são diferentes das B e C.

Na classe A, há possibilidade de cerca de 16 milhões de endereços IPs por rede, mas com somente 126 sub-redes. Na B, são 65.000 endereços IP e 16.000 sub-redes. Na C, há 254 endereços IP, porém, são praticamente 3 milhões de sub-redes. Para saber em qual delas pertence um endereço, é preciso examinar os bits iniciais. A = 0, B = 10 e C = 110. As gamas de endereço de cada classe: A = de 1.0.0.0 até 127.0.0.0, B = de 128.0.0.0 até 191.255.0.0 e C = de 192.0.0.0 até 223.255.255.0. Em geral, a classe A é utilizada por grandes empresas e instituições, a B para empresas de médio porte e a C, que pode ser mais numerosa, são as mais prováveis de serem encontradas atualmente.

| Classe | Primeiro Octeto | Parte da rede (N) e parte para hosts (H) | Máscara | Nº Redes | Endereços por rede |
|--------|-----------------|--|---------------|--------------------------|---------------------------|
| A | 1-127 | N.H.H.H | 255.0.0.0 | 126 (2^7-2) | 16,777,214 ($2^{24}-2$) |
| B | 128-191 | N.N.H.H | 255.255.0.0 | 16,382 ($2^{14}-2$) | 65,534 ($2^{16}-2$) |
| C | 192-223 | N.N.N.H | 255.255.255.0 | 2,097,150 ($2^{21}-2$) | 254 (2^8-2) |
| D | 224-239 | Multicast | NA | NA | NA |
| E | 240-255 | experimental | NA | NA | NA |

- 1) Quantos IPs utilizáveis estão disponíveis na subrede 192.168.0.0/20? Todos os IPs são utilizáveis?



A rede 192.168.0.0 usa máscara /20 , logo temos 20 bits para as redes e 12 bits para os hosts.

00000000 00000000 0000|0000 00000000

11111111 11111111 1111 0000 00000000

-----rede----- subrede----- host

255 255 240 0 essa seria a máscara

Então temos: $2^{12} = 4096$ hosts possíveis. Porém nem todos os IPS são utilizáveis, exatamente porque temos o primeiro que é o ip da rede e o último que é o ip do broadcast. Em resumo, 4094 hosts possíveis.

O padrão é 192.168.0.0 / 24, ou seja, 24 bits para redes e 8 bits para hosts. O que faria com que o endereçamento fosse de 192.168.0.0 até 192.168.0.255 -> 254 possíveis endereços de ip. Masss, estamos fazendo uma subrede, onde dentro disso nós pegamos mais 4 bits.

192.168.0.0

192.168.15.255

$16 * 256 = 4096$

Mas aí tira os endereços de ip da rede e do broadcast, exemplo: 192.168.0.0, 192.168.0.255, 192.168.1.0, 192.168.1.255

4 - (CAP) - Um computador "A" de uma subrede possui a seguinte configuração TCP/IP:

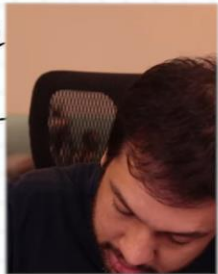
Endereço IP: 192.168.40.18
Máscara: 255.255.255.240
Gateway: 192.168.40.1

Sabendo que o computador "A" está funcionando corretamente, e desejando instalar um segundo computador nesta mesma subrede, pode-se configurar este segundo computador com o seguinte endereço IP:

a) 192.168.40.0
b) 192.168.40.17
c) 192.168.40.18
d) 192.168.40.30
e) 192.168.40.33

Handwritten notes and calculations:

- $256 - 240 = 16$ - SALTO
- 192.168.40.18
- 255.255.255.240
- 192.168.40.0
- 192.168.40.16
- 192.168.40.32
- 192.168.0.1
- 192.168.0.255
- 256



2) Qual a diferença entre um IP público e um IP privado?

A principal diferença entre endereços IP públicos e privados é o alcance e a que estão conectados. Um **endereço IP público** te identifica na Internet, para que todas as informações que procura possam chegar a você. Um **endereço IP privado** é usado em uma rede privada para se conectar com segurança a outros dispositivos nessa mesma rede.



<https://www.avast.com/pt-br/c-ip-address-public-vs-private#:~:text=Um%20endereço%20p%C3%A7%C3%B3blico%20e,um%20endereço%20privado%20exclusivo.>

- 3) Qual a classe utilizada na rede interna do Insper? E na sua rede? Quantas classes existem?

Insper: 10.102.0.71

-
- 1) Por que desabilitar o do roteador?

- 2) Descreva o processo PXE Boot? Qual a sua grande vantagem em um datacenter real?

O PXE (Preboot Execution Environment, ou Ambiente de Pré-execução) é um padrão de boot remoto, desenvolvido pela Intel, que consiste em um pequeno software gravado na ROM da placa de rede que permite que o computador inicialize através da rede, carregando todo o software necessário a partir de um servidor previamente configurado para esse fim. Graças ao PXE é possível ter estações de trabalho sem HD, CD-ROM e nem mesmo drive de disquete. O PXE é derivado do protocolo Dynamic Host Configuration Protocol (DHCP), que deriva por sua vez do BootP, sendo diretamente implementado na placa de rede. Após a inicialização do sistema, um servidor DHCP instalado no servidor LTSP é configurado para responder ao chamado, enviando a configuração de rede juntamente com informações do Kernel que o cliente deve carregar via TFTP e a pasta do servidor com a instalação do LTSP, que deve se acessada via NFS.

O PXE é um padrão do setor criado pela Intel que fornece serviços de pré-inicialização no firmware de dispositivos que permite que os dispositivos baixem programas de inicialização de rede para computadores cliente.

A grande vantagem é a **possibilidade de se utilizar equipamentos de baixo custo**. Os equipamentos não precisam ter disco rígido, apenas uma placa de rede com suporte a Preboot Execution Environment (PXE), recurso utilizado em muitas placas de rede on-board para inicializar o carregamento do sistema.

Preboot Execution Environment(PXE) is a client-server interface that allows computers in a network to be booted from the server before deploying the obtained [PC image](#) in local and remote offices, for PXE enabled clients. PXE network boot is performed using client-server protocols like DHCP(Dynamic Host Configuration Protocol) and TFTP(Trivial File Transfer Protocol). PXE will be enabled by default on all computers.

- 3) Analisando em um aspecto mais amplo, quais outras funcionalidades do Maas podem ser úteis no gerenciamento de bare metal?

1) O que é e como funciona o NAT?

É um mecanismo que vai trabalhar na camada de rede onde sa princiáis infos são IP de origem e destino.

A tradução de endereços de rede (NAT) é um processo que permite que um endereço IP exclusivo represente um grupo inteiro de computadores. Na tradução de endereços de rede, um dispositivo de rede, geralmente um roteador ou firewall NAT, atribui um endereço público a um computador ou computadores dentro de uma rede privada. Desta forma, a tradução de endereços de rede permite que o único dispositivo atue como intermediário ou agente entre a rede local privada e a rede pública que é a internet. O principal objetivo do NAT é conservar o número de endereços IP públicos em uso, tanto para fins de segurança quanto econômicos.

<https://www.geeksforgeeks.org/types-of-network-address-translation-nat>

2) O que é e como funciona a VPN?

VPN significa “Virtual Private Network” (rede virtual privada): um serviço que protege a sua conexão de Internet e privacidade online. Ela cria um túnel criptografado para os seus dados, protege a sua identidade online, oculta o seu endereço de IP e permite que você use pontos de acesso de Wi-Fi públicos com segurança.

3) O que deveria ser feito para você conseguir acessar o Maas da sua casa sem VPN?

4) O que significa LTS? Por que isso importa para uma empresa?

Dentro do universo do software livre e de projetos de código aberto, como distribuições Linux, frameworks e IDEs de desenvolvimento, existe a demanda por programas com estabilidade garantida por meses ou até anos. Tal exigência gerou mudanças no ciclo de vida útil de algumas aplicações, que lançaram “versões LTS” de seus próprios programas para este público específico; mas o que são essas distribuições LTS?

Sigla para *Long-term support* (ou suporte de longo prazo, em português), LTS é uma variação de um software cujo principal objetivo é proporcionar estabilidade por longos períodos aos usuários. É um conceito presente em alguns programas que normalmente atuam nos “bastidores” do mundo digital — sistemas operacionais ou ferramentas de criação, por exemplo — e que demandam maior confidencialidade, integridade e disponibilidade no cotidiano.

5) O que é IPv6? Qual a importância da migração?

Alguns dos protocolos mais conhecidos são: IPv4, IPv6 e HTTP. Começando pelo IPv4 e o IPv6, estes são protocolos da camada de rede que irão identificar computadores e garantir que as informações cheguem nos destinos corretos, assim, os arquivos empacotados em uma camada anterior vão ser recebidos e anexados ao IP da máquina que enviará e receberá arquivos. E a partir disso serão enviados pela internet e irão para outra camada. É como se fosse um

entregador, mas a diferença é que o IPv4 consegue entregar menos que o IPv6, enquanto o primeiro transfere endereços de protocolos de 32 bits, o IPv6 transfere endereços com 128 bits. E a necessidade do IPv6 ter sido criado deve-se ao fato do IPv4 suportar 4,29 bilhões de IPs pelo mundo, mas não mais que isso, enquanto o IPv6 suporta um número de cerca de 340 undecilhões de endereços, ou seja, com ele o crescimento da demanda de internet é facilmente suportado por muitos anos.

6) A literatura preconiza que o Modelo de Rede Internet possui 5 camadas, quais são elas e quais camadas foram envolvidas nesse capítulo?

O modelo de rede de internet que possui 5 camadas é chamado de TCP/IP e possui 5 camadas: a camada física, a camada de enlace, a de internet, a de transporte e a de aplicação.

A camada física trata da transmissão de bits por um canal de comunicação, de maneira a garantir que quando um lado manda um bit 1, esse bit deve ser recebido do outro lado como um bit 1, além de se preocupar com o tempo que um bit deve durar, se a transmissão é simultânea nos dois sentidos, como a comunicação será iniciada, estabelecida e finalizada, etc. Ou seja, é mais sobre interfaces mecânicas, elétricas e de sincronização.

Já a camada de enlace irá descrever o que os enlaces como as linhas seriais e a ethernet precisam fazer para cumprir com os requisitos da camada de interconexão com o serviço não orientado a conexões.

Por sua vez a camada de internet vem para manter toda a arquitetura unida, como se correspondesse a camada de rede do modelo OSI. E sua tarefa é permitir que hosts coloquem pacotes em qualquer rede e garantir que esses pacotes irão trafegar de maneira independente até o destino – podendo ser até em uma rede diferente. É como se fosse um sistema de correio, em que uma pessoa pode deixar várias cartas internacionais em uma caixa de correio em um país e irá esperar que essas cartas serão entregues no endereço correto no país de destino. Por conta disso as cartas provavelmente vão passar por centros de triagem ao longo do caminho e isso será transparente para os usuários, também sendo orientado pelo padrão de cada país em relação aos selos, tamanhos de envelope, regras de entrega, etc.

Em relação à camada de transporte, tem-se que essa camada irá permitir que as entidades pares dos hosts de origem e destino mantenham uma conversação, e para isso conta com o auxílio de dois protocolos: o TCP e o UDP. O TCP é o protocolo de controle de transmissão e é orientado a conexões confiáveis permitindo a entrega de um fluxo de bytes sem erros – e para isso fragmenta o fluxo de bytes de entrada em mensagens discretas e passa cada uma delas para a camada de internet, sendo que é no destino que o processo TCP receptor volta a montar as mensagens recebidas. Por sua vez o protocolo UDP é um protocolo sem conexões, não confiável e para aplicações que não desejam a sequência ou o controle de fluxo do TCP. Ele é usado mais para consultas isoladas com solicitação e resposta (tipo cliente-servidor), e em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como na transmissão de voz ou vídeo.

Por fim, a camada de apresentação contém todos os protocolos de nível mais alto, dentre eles temos: o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP). Além desses, outros foram incluídos com o decorrer dos anos como o DNS – que mapeia os nomes de hosts para seus respectivos endereços da camada de internet -, o HTTP (protocolo usado para buscar páginas na World Wide Web, e o RTP (protocolo para entregar mídia em tempo real como voz ou vídeo).

7) A literatura mais antiga discorre sobre o Modelo de Rede OSI de 7 camadas. Explique a diferença entre os dois modelos.

O modelo de rede OSI possui 7 camadas: a camada física, de enlace, de rede, de transporte, de sessão, de apresentação e de aplicação. Sendo que dessas camadas, as camadas de aplicação, apresentação, sessão e transporte estão representando uma comunicação dentro de um próprio computador. E é a partir da camada de transporte que há uma separação dessas aplicações do usuário, para entrar na camada de rede – onde já não está mais dentro do computador do usuário e onde há de fato comunicação com a rede, com pacotes e informações sendo encaminhadas pela rede.

Agora, já no modelo TCP/IP essas camadas de aplicação, apresentação, e sessão foram juntadas em uma única: a camada de aplicação. Já a camada de rede se tornou a camada de internet, e as outras camadas de transporte, enlace e física se mantém. Detalhe que no modelo TCP/IP original as camadas de enlace e física eram juntadas em uma única: acesso aos meios, mas depois da atualização desse modelo, as camadas de enlace e física se mantiveram separadas para uma melhor compreensão.

O modelo de referência OSI foi concebido antes de os protocolos correspondentes terem sido criados. Isso significa que o modelo não teve influência de um determinado conjunto de protocolos, o que o deixou bastante genérico. A desvantagem dessa ordenação foi que os projetistas não tinham muita experiência no assunto nem muita noção sobre a funcionalidade que deveria ser incluída em cada camada. Com o TCP/IP, ocorreu exatamente o contrário: como os protocolos vieram primeiro, o modelo realmente foi criado como uma descrição dos protocolos existentes. Não houve problemas para os protocolos serem adaptados ao modelo. Eles se encaixaram perfeitamente. O único problema foi o fato de o modelo não se adaptar a outras pilhas de protocolos. Consequentemente, ele não tinha muita utilidade para descrever outras redes que não faziam uso do protocolo TCP/IP

| Comparação entre as Camadas OSI e TCP/IP | | | | |
|--|-----------------|-------------------|----------|-------|
| OSI | TCP/IP Original | TCP/IP Atualizado | Serviços | PDU's |
| 7 APLIC | | | | |
| 6 APRES. | | | | |
| 5 SESSÃO | | | | |
| 4 TRANSP | TRANSPORTE | TRANSP(4) | | |
| 3 REDE | INTERNET | INTERNET(3) | | |
| 2 ENLACE | ACESSO AOS | ENLACE(2) | | |
| 1 FÍSICA | MEIOS | FÍSICO(1) | | |



8) O que é e para que serve um gerenciador de Bare Metal?

9) O que é um MAC address?

O endereço MAC (Media Access Control ou Controle de Acesso de Mídia) é um endereço físico e único, que é associado às interfaces de comunicação utilizadas em dispositivos de rede. A identificação é gravada em hardware por fabricantes de placa de rede, tornando-se posteriormente, parte de equipamentos como computadores, roteadores, smartphones, tablets, impressoras de rede e diversos outros equipamentos que usam comunicação em rede.

Como a identificação é única, ela é usada para fazer o “controle de acesso” em diversos tipos de redes de computadores, como o próprio nome já diz. Mas, apesar de ser único e gravado em hardware, é possível alterar o endereço MAC com técnicas específicas. Também é importante destacar que, embora não seja algo visível, sempre que a rede utiliza uma identificação baseada em software como o protocolo TCP/IP, o endereço MAC está sendo utilizado.

10) O que é um IP address? Como ele difere do MAC address?

Endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local. IP vem do inglês "Internet Protocol" (protocolo de rede) que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local.

Basicamente, o endereço IP é o identificador que permite que as informações sejam enviadas entre dispositivos em uma rede: ele contém as informações de localização e torna o dispositivo acessível para comunicação. A Internet precisa de um meio de distinguir diferentes computadores, roteadores e sites. O endereço IP providencia isso, além de ser uma parte essencial do funcionamento da Internet.

O IP é uma identificação que a rede atribui a cada aparelho conectado a ela (ou seja o IP pode mudar) já o mac address é um endereço único de cada aparelho que nunca muda e que a rede utiliza além de outras coisas para manter um registro de todos os aparelhos que já se conectaram a ela.

11) O que é CIDR? Qual o papel da subrede?

O CIDR é uma sigla para Classes Inter-Domain Routing, e ele é considerado um método para repartir os endereços IP e para rotear. Foi em 1993 que o CIDR foi introduzido pela Internet Engineering Task Force, e desde então esse método tem sido utilizado para substituir a arquitetura anterior que endereçava as redes.

Sua principal função era de desacelerar o crescimento das tabelas que continham os roteamentos dos roteadores na rede. Desta forma, foi possível auxiliar a desacelerar a rapidez com que os endereços IPv4 estava alcançando.

O CIDR possui uma notação que é extremamente compacta e que identifica o endereço IP e qual o seu prefixo de roteamento que está associado. Sua notação é construída através de um endereço IP, uma barra (/) e, por último, um número decimal. O número final será composto pela contagem dos bits 1 iniciais que está na máscara de roteamento, e esse número normalmente é conhecido como a máscara de rede.

A notação sempre representa o endereço IP de acordo com as normas e com os padrões definidos para o IPv4 e o IPv6.

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.^[1]

Dispositivos que pertencem a uma sub-rede são endereçados com um grupo de bit mais significativo comum 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.

O prefixo de roteamento pode ser expressado em notação de Classless Inter-Domain Routing (CIDR) escrito como o primeiro endereço de uma rede, seguido por um "caractere barra" (/), e finalizando com o comprimento de bit do prefixo. Por exemplo, 192.168.1.0/24 é o prefixo da rede IPv4 começando no endereço fornecido, possuindo 24 *bits* aplicados para o prefixo de rede; e os 8 *bits* restantes reservados para endereçamento de hospedeiro. A especificação de endereço IPv6 2001:db8::/32 é um bloco de endereço amplo com 2⁹⁶ endereços, possuindo um prefixo de roteamento de 32 *bits*.

12) O que são DHCP, DNS e gateway?

Quando falamos em redes, existem alguns recursos que são utilizados e facilitam muito a nossa vida, mas nem os percebemos. Um deles é o protocolo DHCP. Do inglês Dynamic Host Configuration Protocol (que ficaria, em português, algo como Protocolo de Configuração Dinâmica de Endereços de Rede), é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.

Este protocolo começou a ganhar terreno aproximadamente em Outubro de 1993, sendo o sucessor do BOOTP que, embora seja mais simples, tornou-se muito limitado para as exigências atuais.

Por que ele é importante?

Digamos que você seja o administrador de uma rede. Se fosse uma rede doméstica com 3 computadores, não seria trabalhoso atribuir um número de IP e todos os parâmetros necessários para cada um deles. Agora, se fossem 100, 200 ou mais, certamente a história seria outra.

O protocolo DHCP faz exatamente isto, por meio dele um servidor é capaz de distribuir automaticamente endereços de IP diferentes a todos os computadores à medida que eles fazem a solicitação de conexão com a rede. Essa distribuição dos IPs é feita em um intervalo

pré-definido configurado no servidor. Sempre que uma das máquinas for desconectada o IP ficará livre para o uso em outra.

Aqui é importante ressaltar que as funções de gateway não são desempenhadas exclusivamente por um equipamento ou aparelho. Na verdade, por se tratar mais de um conceito do que de uma ferramenta em si, existem diferentes tipos de gateways, que realizam uma ou mais funções de intermediação nas conexões que estabelecemos.

TANNENBAUM e guria da <https://portaldeplanos.com.br/artigos/gateway/>

Quais as consequências de utilizar um DNS externo (Por exemplo: 8.8.8.8) em uma rede privada?

Para resolver esses problemas, foi criado o sistema de nomes de domínios, ou DNS (Domain Name System), em 1983. Ele tem sido uma parte fundamental da Internet desde então. A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos. O DNS é definido nas RFCs 1034, 1035, 2181 e elaborado com mais detalhes em muitas outras. Em resumo, o DNS é utilizado da forma descrita a seguir. Para mapear um nome em um endereço IP, um programa aplicativo chama um procedimento de biblioteca denominado resolvidor e repassa a ele o nome como um parâmetro. Vimos um exemplo de resolvidor, gethostbyname, na Figura 6.6. O resolvidor envia uma consulta contendo o nome para um servidor DNS local, que procura o nome e retorna uma resposta contendo o endereço IP ao resolvidor. Este, em seguida, retorna o endereço IP ao programa aplicativo que fez a chamada. As mensagens de consulta e resposta são enviadas como pacotes UDP. Munido do endereço IP, o programa pode então estabelecer uma conexão TCP com o host ou enviar pacotes UDP até ele.

- **DNS público vs. DNS privado** - Um DNS público está disponível para a população em geral, e normalmente vem

do seu provedor de serviços de Internet ou de um provedor DNS dedicado. Já um DNS privado é normalmente usado por empresas para fornecer aos funcionários acesso mais fácil a sites ou endereços IP internos. Normalmente, você pode usar um DNS público em casa e em um DNS público ou privado no trabalho.

Topologia Barramento

Todos os computadores são ligados em um mesmo barramento físico de dados. Apesar de os dados não passarem por dentro de cada um dos nós, apenas uma máquina pode "escrever" no barramento num dado momento. Todas as outras "escutam" e recolhem para si os dados destinados a elas. Quando um computador estiver a transmitir um sinal, toda a rede fica ocupada e se outro computador tentar enviar outro sinal ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

- **Vantagens:**

- Uso de cabo é econômico;
- Mídia é barrata, fácil de trabalhar e instalar;
- Simples e relativamente confiável;
- Fácil expansão.

- **Desvantagens:**

- Rede pode ficar extremamente lenta em situações de tráfego pesado;
- Problemas são difíceis de isolar;
- Falha no cabo paralisa a rede inteira.

Topologia Anel

Na topologia em anel os dispositivos são conectados em série, formando um circuito fechado (anel). Os dados são transmitidos unidirecionalmente de nó em nó até atingir o seu destino. Uma mensagem enviada por uma estação passa por outras estações,

através das retransmissões, até ser retirada pela estação destino ou pela estação fonte.

- **Vantagens:**

- Todos os computadores acessam a rede igualmente;
- Performance não é impactada com o aumento de usuários.

- **Desvantagens:**

- Falha de um computador pode afetar o restante da rede;
- Problemas são difíceis de isolar.

Topologia Malha

Esta topologia é muito utilizada em várias configurações, pois facilita a instalação e configuração de dispositivos em redes mais simples. Todos os nós estão atados a todos os outros nós, como se estivessem entrelaçados. Já que são vários os caminhos possíveis por onde a informação pode fluir da origem até o destino.

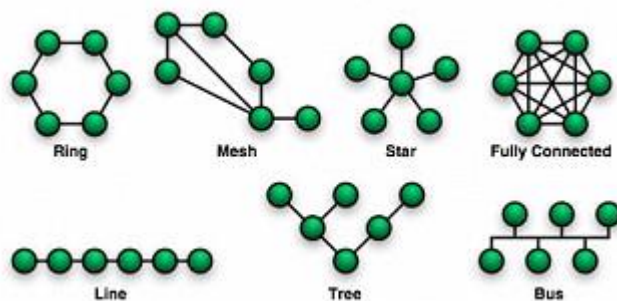
- **Vantagens:**

- Maior redundância e confiabilidade;
- Facilidade de diagnóstico.

- **Desvantagem:**

- Instalação dispendiosa.

Espero que tenham compreendido uma matéria simples que mostra apenas as principais vantagens e desvantagens. Abraço!



<https://anlix.io/topologia-de-rede-o-que-e-tipos-e-qual-e-melhor/>

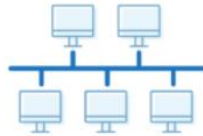
[https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens#:~:text=Topologia%20de%20Redes%3F-,A%20topologia%20de%20rede%20%C3%A9%20o%20padr%C3%A3o%20no%20qual%20o,n%C3%B3s%20\(computadores\)%20da%20rede.](https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens#:~:text=Topologia%20de%20Redes%3F-,A%20topologia%20de%20rede%20%C3%A9%20o%20padr%C3%A3o%20no%20qual%20o,n%C3%B3s%20(computadores)%20da%20rede.)

Network Topology Types

1 Point to point



2 Bus



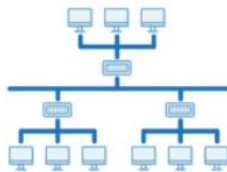
3 Ring



4 Star



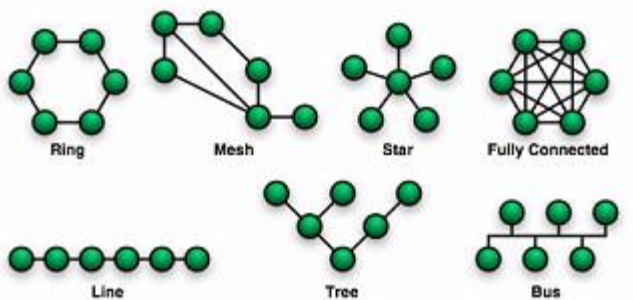
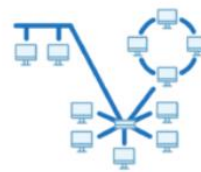
5 Tree



6 Mesh



7 Hybrid



[https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens#:~:text=Topologia%20de%20Redes%3F-A%20topologia%20de%20rede%20C3%A9%20o%20padr%C3%A3o%20no%20qual%20o,n%C3%B3s%20\(computadores\)%20da%20rede.](https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens#:~:text=Topologia%20de%20Redes%3F-A%20topologia%20de%20rede%20C3%A9%20o%20padr%C3%A3o%20no%20qual%20o,n%C3%B3s%20(computadores)%20da%20rede.)

<https://www.dnsstuff.com/what-is-network-topology>

2. Quais casos uma rede ter mais de 1 gateway?

Máquina só conversa com outras que estão na mesma rede, caso wueria acessar por exemplo o BB dentro do Insper, precisamos de gateway ou router. Uma rede muito interconectada que precisa sempre de uma rede livre.

Quando você tem mais de um gateway, a máquina tenta utilizar o próximo sempre que o primeiro está fora, ou seja, o gateway não é escolhido de acordo com o destino. Para que isso aconteça você precisa criar rotas estáticas informando quais faixas de ip devem sair pelo roteador que está ligado às filiais. Os demais endereços de destino saem pelo gateway padrão, que fica sendo o roteador da Internet.

3. Quais as consequências de utilizar um DNS externo (Por exemplo: 8.8.8.8) em uma rede privada?

1. O que é e como funciona o NAT?

2. O que é e como funciona a VPN?

3. O que deveria ser feito para você conseguir acessar o Maas da sua casa sem VPN?