**Resumo Fundamentos de Rede**

**IP**

O termo IP (Internet Protocol) é um número binário identificador dado ao seu computador, ou roteador, ao conectar-se à rede. É através desse número que seu computador pode enviar e receber dados na internet.

* **IP Público**

Um endereço IP *público* é aquele que pode ser acessado diretamente pela Internet e é atribuído ao roteador de rede pelo provedor de serviços de Internet. Seu dispositivo pessoal também tem um IP *privado* que fica oculto quando você se conecta à Internet por meio do IP público do seu roteador.

* **IP Privado**

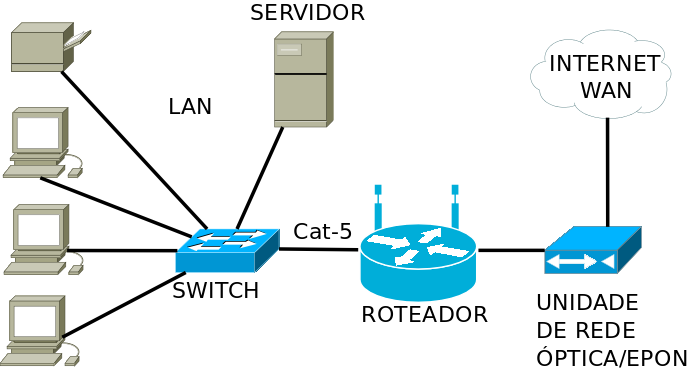
Um endereço IP privado é aquele que o roteador de rede atribui ao seu dispositivo. Cada dispositivo na mesma rede recebe um endereço IP privado exclusivo (às vezes chamado de endereço de rede privada). Assim os dispositivos na mesma rede interna se comunicam entre si.



**Redes**

* **LAN**

LAN é Local Area Network. Este termo geralmente se refere a redes de computadores restritas a um local físico definido como uma casa, escritório ou empresa em um mesmo prédio. Uma rede sem fio de uma empresa também faz parte da LAN. O que realmente limita a rede LAN é uma faixa de IP privada à mesma, com uma máscara de rede comum.



* **WAN**

WAN é Wide Area Network. Significa uma rede que cobre uma área física maior, como o campus de uma universidade, uma cidade, um estado ou mesmo um país. É usado frequentemente nas configurações dos roteadores para se referir à rede externa à empresa, que não é considerada parte da LAN, como foi dito acima. WAN também é usado para se referir à rede da internet em geral, apesar desta ser uma designação genérica demais.

**Tráfego de redes**

* **Unicast**

Tipo de comunicação na qual um quadro é enviado de um host e endereçado a um destino específico. Existe apenas um remetente e um receptor. Sendo uma forma predominante de transmissão em redes locais e na Internet.

* **Multicast**

É uma comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes. Os clientes da transmissão multicast devem ser membros de um grupo multicast lógico para receber as informações.

* **Broadcast**

Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de broadcast é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local.

**Sub-rede**

Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de broadcast é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local.

**ARP**

##### O que é e como funciona o protocolo ARP

Recentemente um leitor enviou-me um e-mail com a seguinte questão: “Numa rede ethernet, como é que os PC’s se descobrem uns aos outros?”. Quem trabalha com redes a resposta seria directa: o protocolo ARP (*Address Resolution Protocol* – RFC 826) permite que um PC obtenha o endereço físico de uma máquina, usando o endereço IP (da máquina de destino).

Percebido? hum…confuso. Então vamos a três questões essenciais:

1) Quando pretendemos comunicar com outra máquina, o que precisamos de saber?

Endereço IP (ou o nome que depois é traduzido num endereço IP).

2) Qual a informação que é inserida numa frame relativamente ao destinatário?

O MAC Address do PC de destino (endereço físico) é incluído na frame (PDU da camada 2, saber mais [aqui](https://pplware.sapo.pt/networking/redes-sabe-o-que-e-o-modelo-osi/)).

3) Mas se eu só sei o IP, como descobrir o MAC do PC de destino?

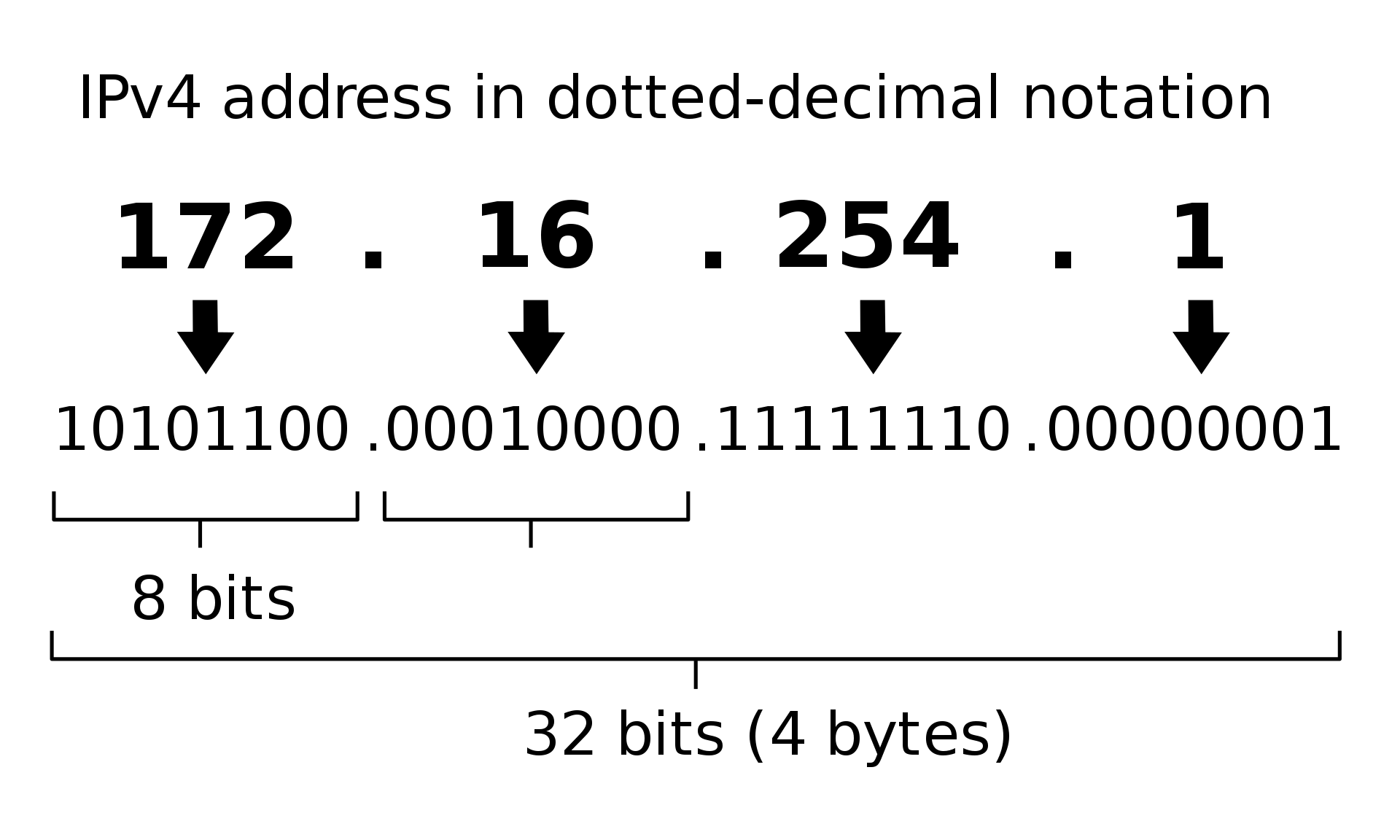
Recorrendo ao protocolo ARP, que permite obter o endereço MAC (do PC de destino) usando o endereço IP (do PC de destino).

Vamos a um exemplo de funcionamento do protocolo ARP

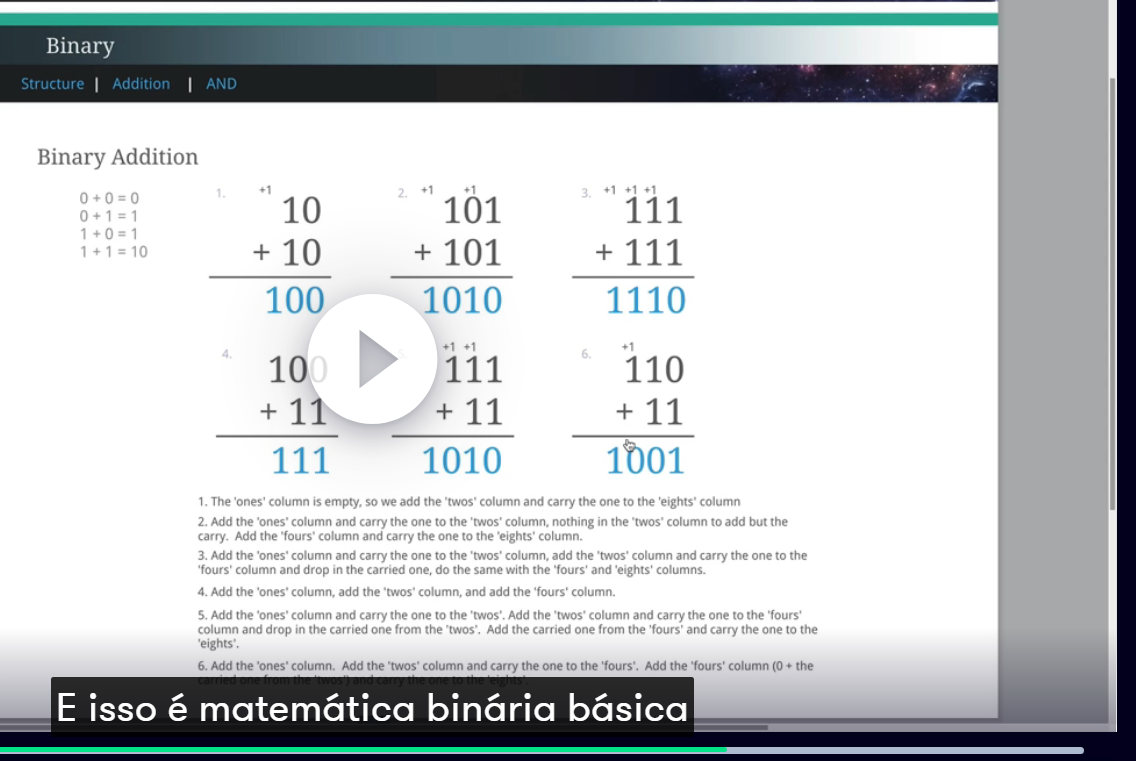
* Vamos considerar que o PC-A com o endereço IP: 192.168.0.1 quer comunicar com o PC-B que tem o endereço IP: 192.168.0.3 (os PCs estão na mesma rede).
* O PC-A verifica a sua tabela ARP (podem ver esta informação através do comando arp –a) para saber se já existe alguma informação relativamente ao endereço físico do PC-B. Caso exista, esse endereço é usado.
* Caso o PC-A não tenha qualquer informação na tabela ARP do PC-B, o protocolo ARP envia uma mensagem de *broadcast* (para o endereço FF:FF:FF:FF:FF:FF) a “questionar” (ARP Request) a quem pertence o endereço IP (neste caso o endereço IP do PC-B).
* O PC-B responderá à mensagem ARP enviada pelo PC-A, enviando o seu endereço físico.O PC-A guardará essa informação na sua tabela ARP (que fica guardada na memória RAM do PC)

**IPV4**

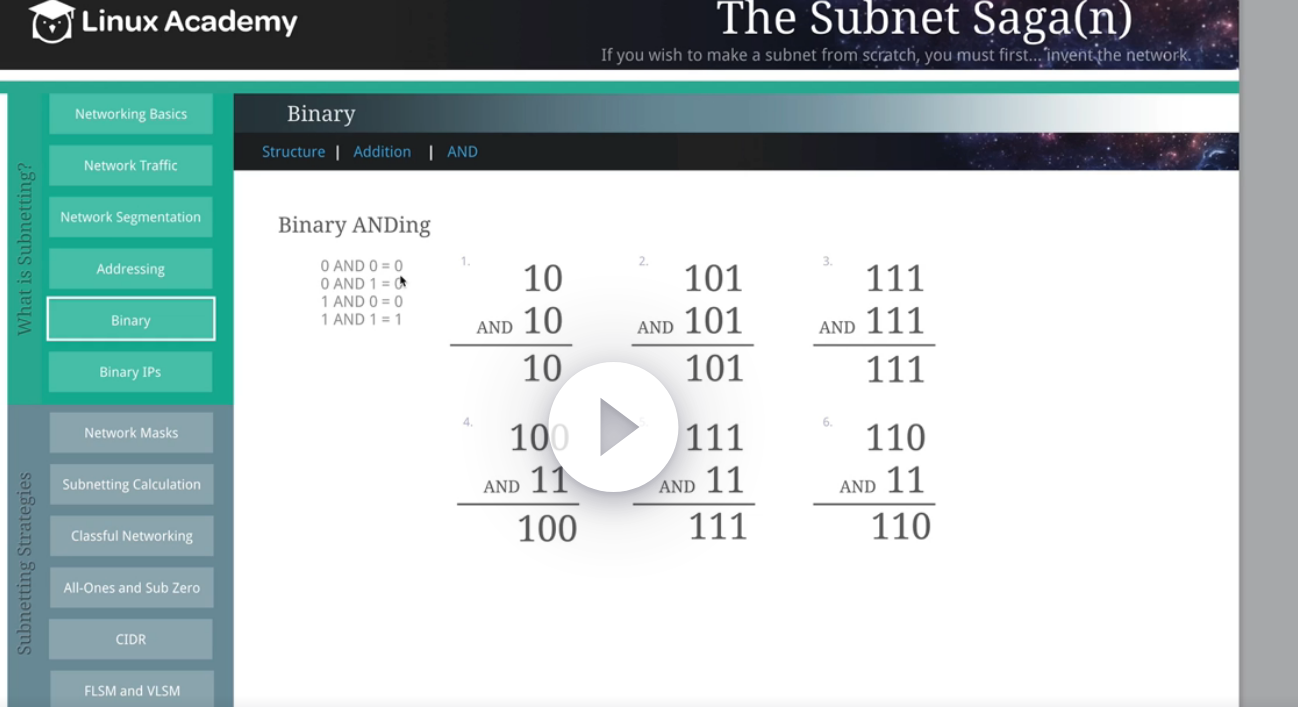
O IPv4 utiliza endereços de 32 bits, o que limita o [espaço de endereço](https://pt.wikipedia.org/wiki/Espa%C3%A7o_de_endere%C3%A7amento) para 4294967296 (232) endereços.



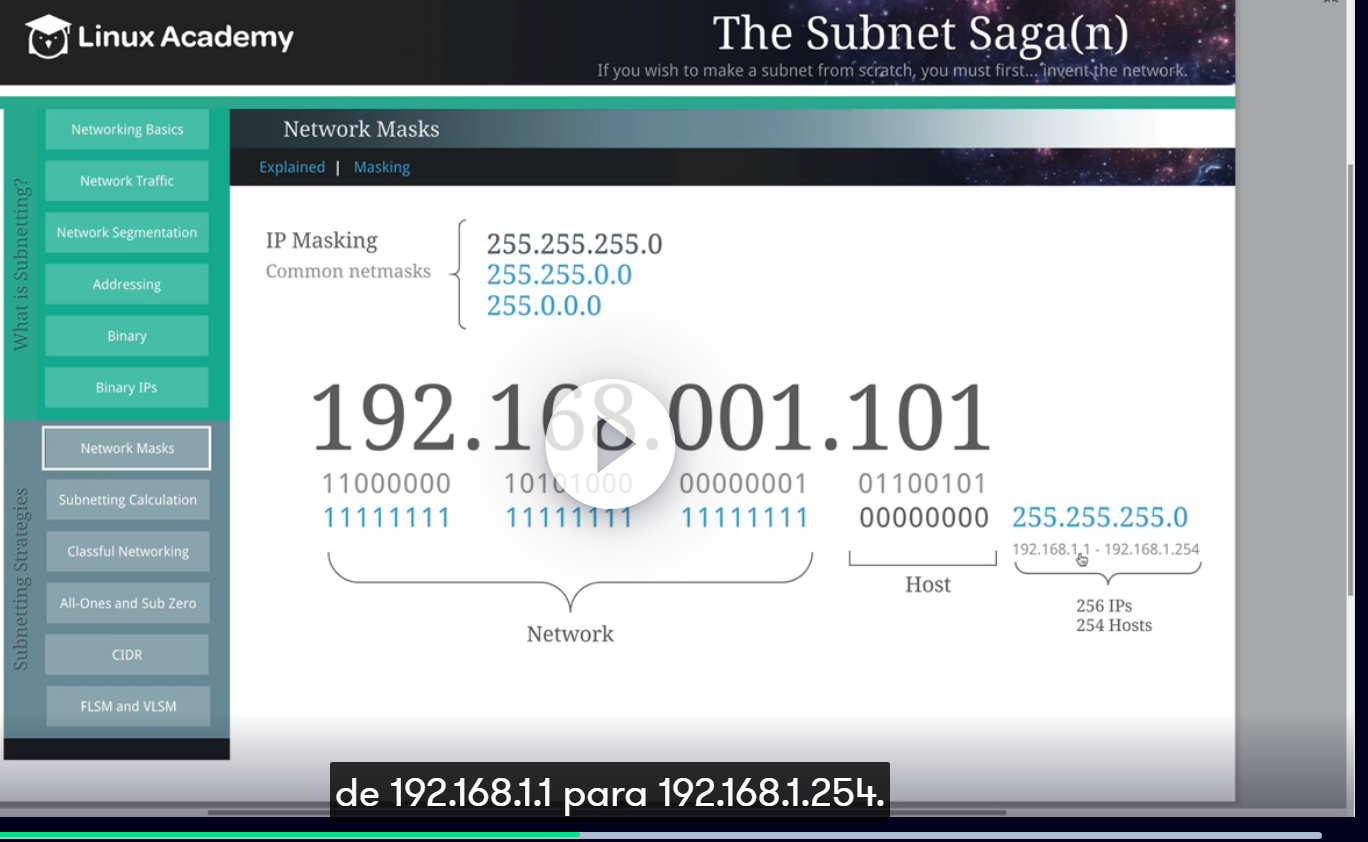
**Adição Binária:**

****

**Subtração Binária:**

****

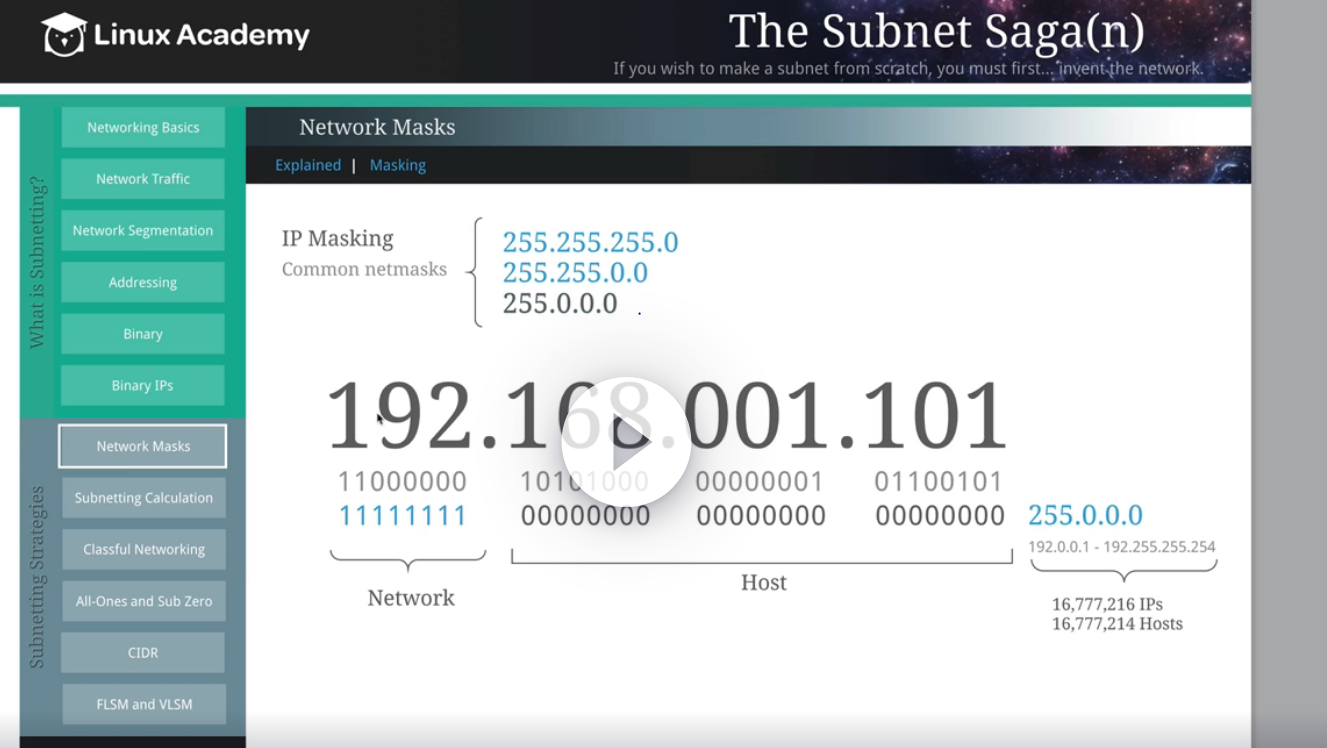
**Máscara IP 255.255.255.0:**

****

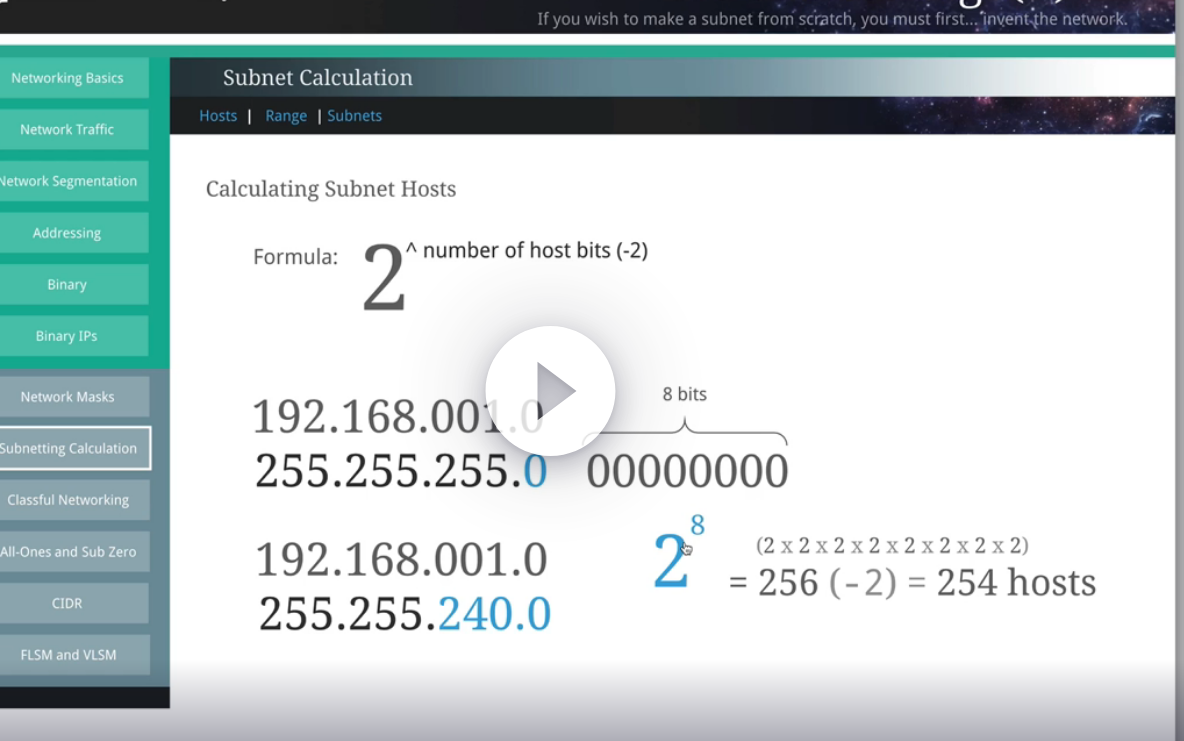
**Máscara IP 255.255.0.0:**

****

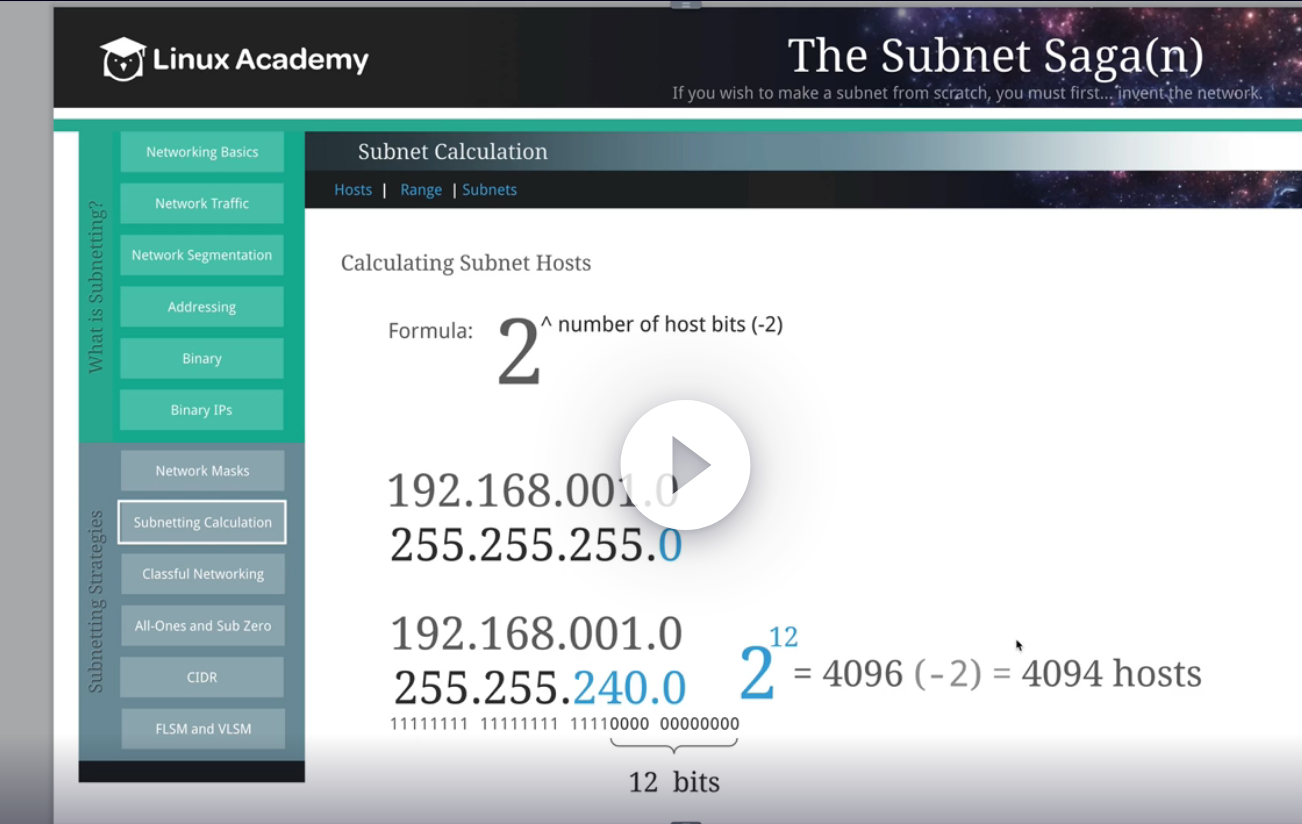
**Máscara IP 255.0.0.0:**

****

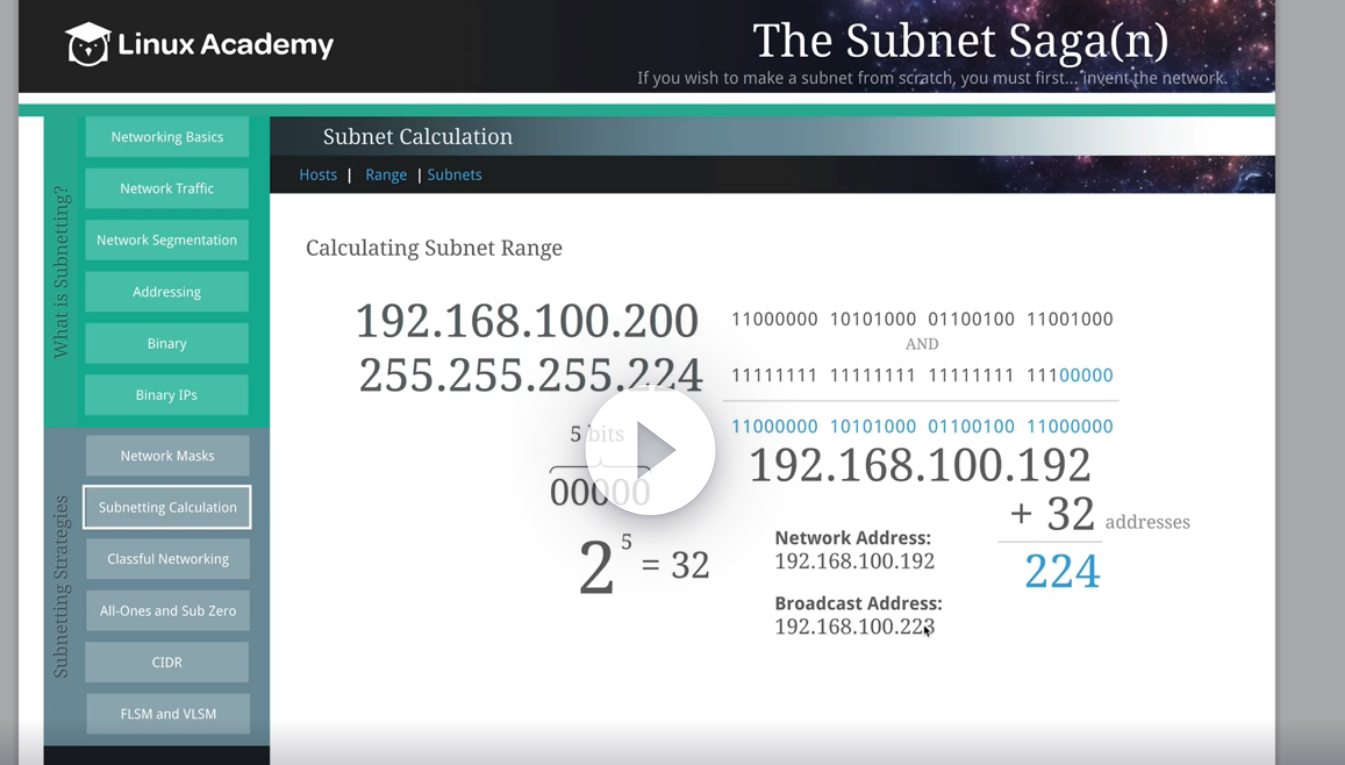
**Calculando hosts:**

****

**Calculando hosts:**

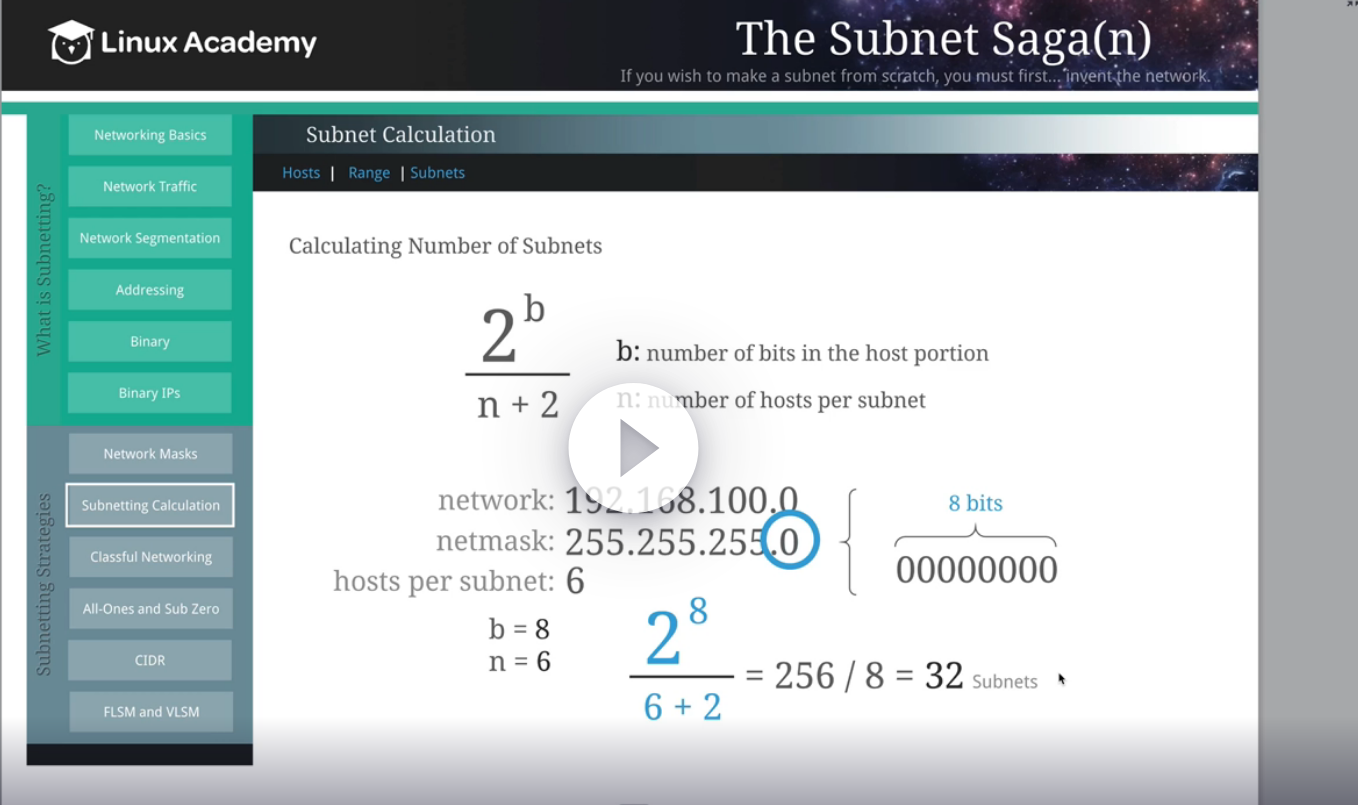
****

**Calculando sub-redes ranged:**

****

Endereço de broadcast tem que ser ímpar.

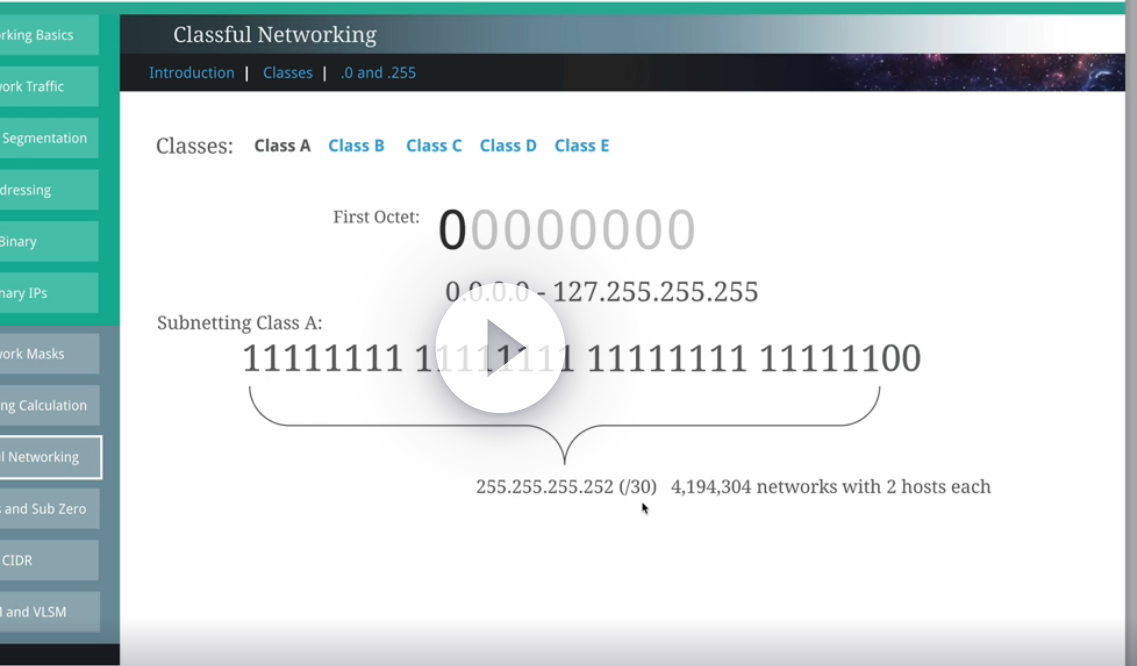
**Calculando número de Sub-redes:**

****

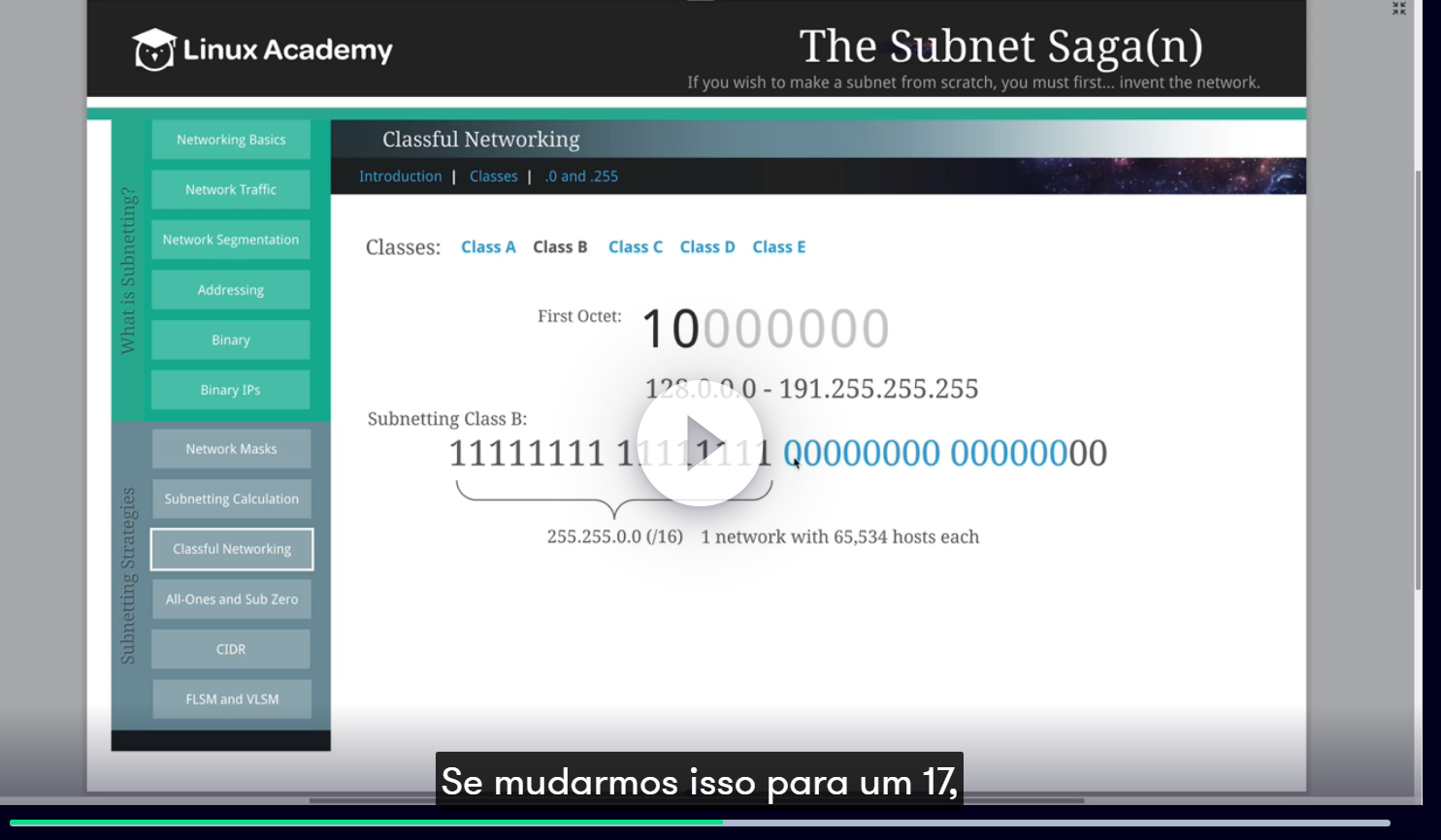
Cada uma dessas sub-redes têm 6 ips de host e 8 ips totais, cada uma terá seu ip de rede e ip de broadcast.

**Classes de redes**

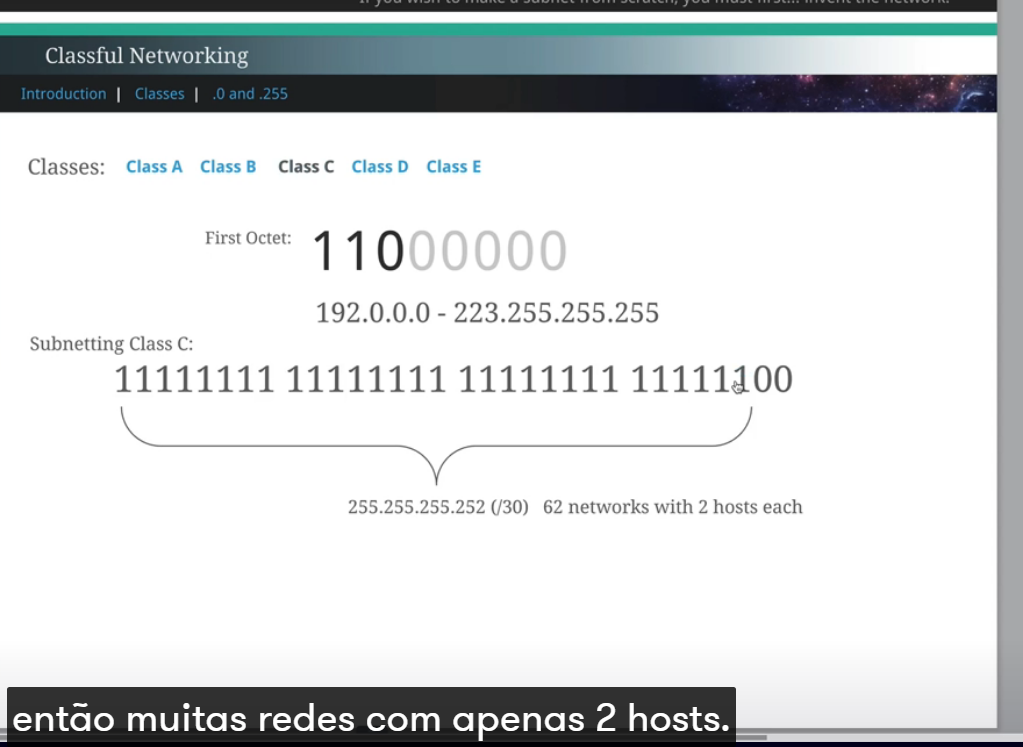
**Classe A:**

****

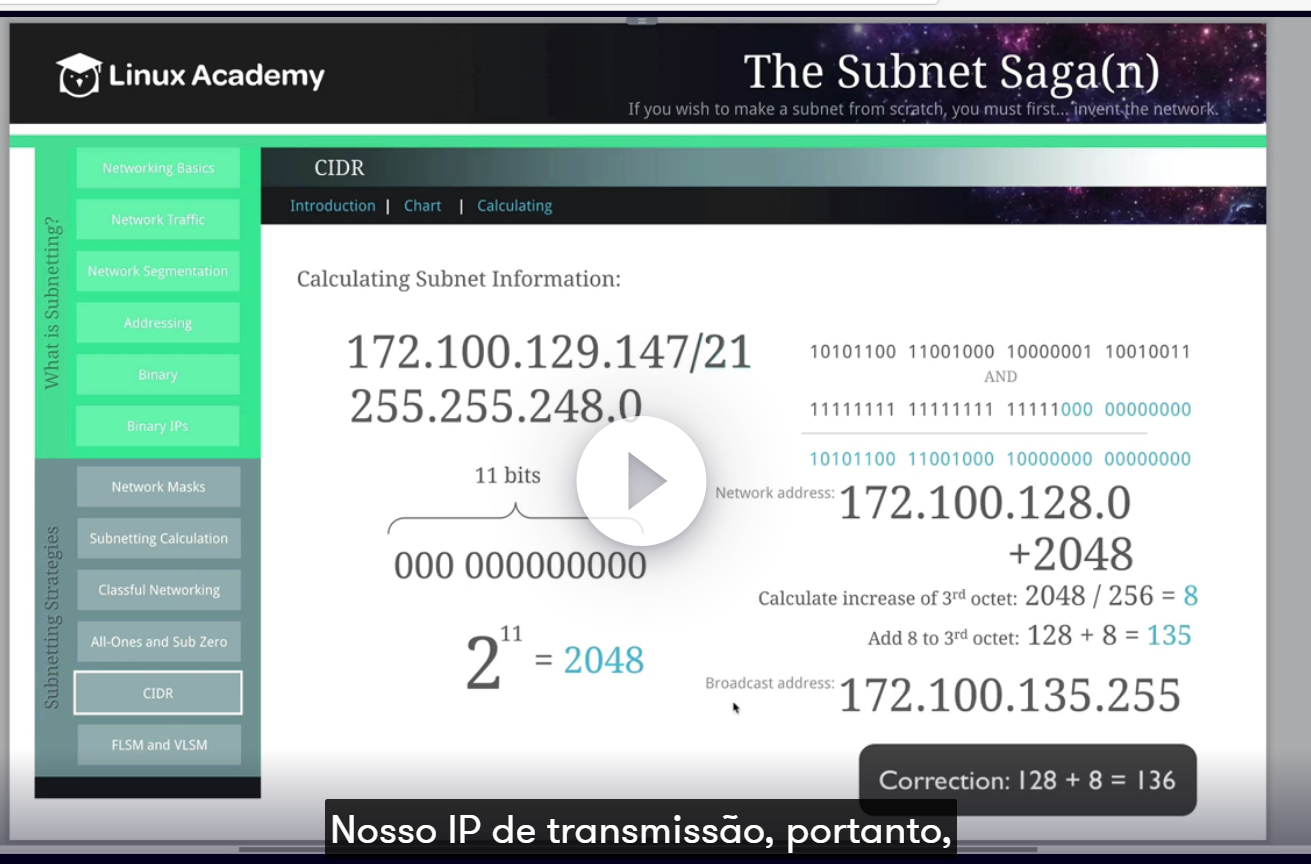
**Classe B**

****

**Classe c:**

****

**Calculando Sub-Rede informações :**

****

**Aprofundar→ CIDR, FLSM E VLSM**

**DHCP**

O serviço DHCP, associado com outros protocolos do TCP/IP, permite atribuir endereços IP únicos e exclusivos para nossos dispositivos cada vez que nos conectamos a uma rede.

Os dispositivos clientes configurados para utilizarem IP dinâmico transmitem uma solicitação ao servidor DHCP, requisitando informações de configuração da rede, local ou remota, para os quais estão conectados.

Dispositivos clientes que dependem de [servidores](https://www.controle.net/faq/o-que-sao-servidores), como celulares e computadores conectados a redes como a internet, normalmente transmitem uma consulta por essas informações imediatamente após sua inicialização

**Network Address Translation (NAT)**

um host com uma solicitação para internet, essa solicitação é destinada para o ip privado do roteador e ele envia a solicitação para internet, essa solicitação retorna para o ip público do roteador e ele encaminha ela para o ip privado do host que solicitou.

O conceito de NAT pode ser descrito como a própria sigla já diz (Network AddressTranslation), ou tradução de endereço de rede, confuso, vou tentar explicar melhor.Todos que tem uma conexão com a internet tem um modem, ai já podemos ter uma ideia do que é, pois existe o ip privado e o ip publico, ou seja, o ip privado é a sua rede interna e o ip publico é a internet, digamos assim, ai para fazer esta conexão para que possa acessar os sites em outro servidores precisamos fazer esta tradução e o responsável por esta tradução e o NAT.

Um outro exemplo que podemos usar é caso tenha que acessar um endereço dentro da sua rede mas você não esta nela, claro da para utilizar um VPN, mas pode também acessar pelo navegador é o caso dos sites ou sistemas como [GLPI](https://falati.com.br/glpi-9-4-disponivel/) que é criado para fazer chamados pela web.

Explicando melhor, tenho o GLPI e quero deixar ele aberto para que os clientes possam abrir os chamados de qualquer lugar, então configuro no meu roteador ou firewall uma NAT dizendo que tudo que vier da web será enviado para o meu servidor interno onde está o sistema, a imagem abaixo explica melhor isso.

**Rotas Estáticas**

Rotas estáticas são comumente usadas nos seguintes cenários:

* Como uma rota padrão, encaminhamento de pacotes para um provedor de serviços
* Para rotas fora do domínio de roteamento e não aprendidas pelo protocolo de roteamento dinâmico
* Quando o administrador da rede deseja definir explicitamente o caminho para uma rede específica
* Para roteamento entre redes stub

As rotas estáticas são úteis para redes menores com apenas um caminho para uma rede externa. Eles também fornecem segurança em uma rede maior para certos tipos de tráfego ou links para outras redes que precisam de mais controle.

**Rotas Dinâmicas**

Os protocolos de roteamento dinâmico ajudam o administrador da rede a gerenciar o processo demorado e preciso de configuração e manutenção de rotas estáticas. Os protocolos de roteamento dinâmico são implementados em qualquer tipo de rede que consiste em mais do que apenas alguns roteadores. Os protocolos de roteamento dinâmico são escalonáveis ​​e determinam automaticamente as melhores rotas se houver uma alteração na topologia.

Os protocolos de roteamento dinâmico são comumente usados ​​nos seguintes

cenários:

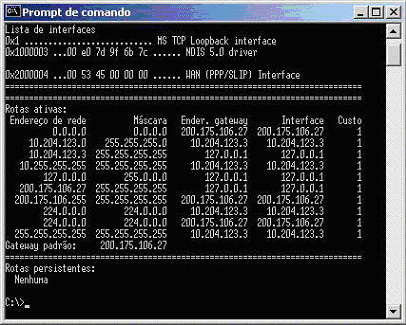
* Em redes que consistem em mais do que apenas alguns roteadores
* Quando uma mudança na topologia da rede exige que a rede determine automaticamente outro caminho
* Para escalabilidade. Conforme a rede cresce, o protocolo de roteamento dinâmico aprende automaticamente sobre quaisquer novas redes.

A tabela mostra uma comparação de algumas diferenças entre o roteamento dinâmico e estático

Tabelas de roteamento

Falei na Parte 5 que toda a funcionalidade do Roteador é baseada em tabelas de roteamento. Quando um pacote chega em uma das interfaces do roteador, ele analisa a sua tabela de roteamento, para verificar se contém uma rota para a rede de destino. Pode ser uma rota direta ou então para qual roteador o pacote deve ser enviado. Este processo continua até que o pacote seja entregue na rede de destino, ou até que o limite de 16 hopes tenha sido atingido.

Na Figura a seguir apresento um exemplo de uma "mini-tabela" de roteamento:



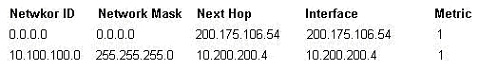
Cada linha é uma entrada da tabela. Por exemplo, a linha a seguir é que define o Default Gateway da ser utilizado:

0.0.0.0 0.0.0.0 200.175.106.54 200.175.106.54 1

Neste tópico você aprenderá sobre os campos que compõem uma entrada da tabela de roteamento e o significado de cada campo. Também aprenderá a interpretar a tabela de roteamento que existe em um computador com o Windows 2000, Windows XP ou Windows Server 2003.

Entenda os campos que compõem as entradas de uma tabela de roteamento:

Uma entrada da tabela de roteamento possui os campos indicados no esquema a seguir e explicados logo em seguida:



Network ID: Este é o endereço de destino. Pode ser o endereço de uma rede (por exemplo: 10.10.10.0), o endereço de um equipamento da rede, o endereço de uma sub-rede (veja detalhes sobre sub-rede mais adiante) ou o endereço da rota padrão (0.0.0.0). A rota padrão significa: "a rota que será utilizada, caso não tenha sido encontrada uma rota específica para o destino". Por exemplo, se for definida que a rota padrão deve ser envida pela interface com IP 10.10.5.2 de um determinado roteador, sempre que chegar um pacote, para o qual não existe uma rota específica para o destino do pacote, este será enviado pela roda padrão, que no exemplo seria a interface 10.10.5.2. Falando de um jeito mais simples: Se não souber para onde mandar, manda para a rota padrão.

Network Mask: A máscara de sub-rede utilizada para a rede de destino.

Next Hop: Endereço IP da interface para a qual o pacote deve ser enviado. Considere o exemplo a seguir, como sendo uma entrada de um roteador, com uma interface de WAN configurada com o IP número 10.200.200.4:



Esta entrada indica que pacotes enviados para a rede definida pelos parâmetros 10.100.100.0/255.255.255.0, deve ser enviada para o gateway 10.200.200.1 e para chegar a este gateway, os pacotes de informação devem ser enviados pela interface 10.200.200.120. Neste exemplo, esta entrada está contida na tabela interna de roteamento de um computador com o Windows Server 2003, cujo número IP é 10.200.200.120 e o default gateway configurado é 10.200.200.1. Neste caso, quando este computador quiser se comunicar com um computador da rede 10.100.100.0, será usada a entrada de roteamento descrita neste item. Nesta entrada está especificado que pacotes para a rede 10.100.100.0, com máscara 255.255.255.0, devem ser enviados para o default gateway 10.200.200.1 e que este envio deve ser feito através da interface de rede 10.200.200.120, que no nosso exemplo é a placa de rede do computador. Uma vez que o pacote chegou no default gateway (na interface de LAN do roteador), o processo de roteamento, até a rede de destino (rede 10.100.100.0) é o processo descrito nas análises anteriores.

Interface: É a interface através da qual o pacote deve ser enviado. Por exemplo, se você estiver analisando a tabela de roteamento interna, de um computador com o Windows Server 2003, o número IP do campo interface, será sempre o número IP da placa de rede, a não ser que você tenha mais de uma placa de rede instalada.

Metric: A métrica é um indicativo da distância da rota, entre destino e origem, em termos de hopes. Conforme descrito anteriormente, pode haver mais de um roteador entre origem e destino. Também pode haver mais de um caminho entre origem e destino. Se for encontrada duas rotas para um mesmo destino, o roteamento será feito pela rota de menor valor no campo Metric. Um valor menor indica, normalmente, um número menor de hopes (roteadores) entre origem e destino.

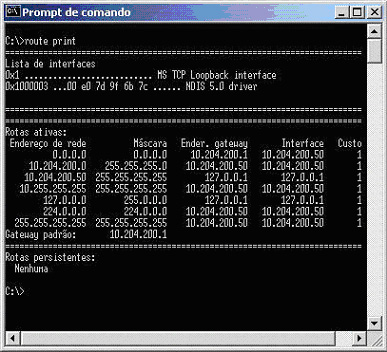
Analisando a tabela de roteamento de um computador com o Windows (2000, 2003 ou XP):

Agora que você já conhece os conceitos de tabelas de roteamento e também conhece os campos que formam uma entrada em uma tabela de roteamento, é hora de analisar as entradas de uma tabela de roteamento em um computador com o Windows Server 2003 instalado. No Windows Server 2003, o protocolo TCP/IP é instalado automaticamente e não pode ser desinstalado (esta é uma das novidades do Windows Server 2003). Ao instalar e configurar o protocolo TCP/IP, o Windows Server 2003 cria, na memória do servidor, uma tabela de roteamento. Esta tabela é criada, dinamicamente, toda vez que o servidor é inicializado. Ao desligar o servidor o conteúdo desta tabela será descartado, para ser novamente recriado durante a próxima inicialização. A tabela de roteamento é criada com base nas configurações do protocolo TCP/IP. Existem também a possibilidade de adicionar entradas estáticas. Uma entrada estática fica gravada em disco e será adicionada a tabela de roteamento durante a inicialização do sistema. Ou seja, além das entradas criadas automaticamente, com base nas configurações do TCP/IP, também podem ser acrescentadas rotas estáticas, criadas com o comando route, o qual descreverei mais adiante.

Para exibir a tabela de roteamento de um computador com o Windows Server 2003 (ou com o Windows 2000, ou Windows XP), abra um Prompt de comando, digite o comando indicado a seguir e pressione Enter:

route print

Será exibida uma tabela de roteamento, semelhante a indicada na Figura a seguir, onde é exibida a tabela de roteamento para um servidor com o número IP: 10.204.200.50:



Vamos analisar cada uma destas entradas e explicar a função de cada entrada, para que você possa entender melhor os conceitos de roteamento. Rota padrão:



Esta rota é indicada por uma identificação de rede 0.0.0.0 com uma máscara de sub-rede 0.0.0.0. Quando o TCP/IP tenta encontrar uma rota para um determinado destino, ele percorre todas as entradas da tabela de roteamento em busca de uma rota específica para a rede de destino. Caso não seja encontrada uma rota para a rede de destino, será utilizada a rota padrão. Em outras palavras, se não houver uma rota específica, mande para a rota padrão. Observe que a rota padrão é justamente o default gateway da rede (10.204.200.1), ou seja, a interface de LAN do roteador da rede. O parâmetro Interface (10.204.200.50) é o número IP da placa de rede do próprio servidor. Em outras palavras: Se não houver uma rota específica manda para a rota padrão, onde o próximo hope da rede é o 10.204.200.1 e o envio para este hope é feito através da interface 10.204.200.50 (ou seja, a próprio placa de rede do servidor).

Endereço da rede local:



Esta rota é conhecida como Rota da Rede Local. Ele basicamente diz o seguinte: "Quando o endereço IP de destino for um endereço da minha rede local, envia as informações através da minha placa de rede através da minha placa de rede (observe que tanto o parâmetro Gateway como o parâmetro Interface estão configurados com o número IP do próprio servidor). Ou seja, se for para uma das máquinas da minha rede local, manda através da placa de rede, não precisa enviar para o roteador.

Local host (endereço local):



Este endereço faz referência ao próprio computador. Observe que 10.204.200.50 é o número IP do servidor que está sendo analisado (no qual executei o comando route print). Esta rota diz que os programas do próprio computador, que enviarem pacotes para o destino 10.204.200.50 (ou seja, enviarem pacotes para si mesmo, como no exemplo de dois serviços trocando informações entre si), devem usar como Gateway o endereço de loopback 127.0.0.1, através da interface de loopback 127.0.0.1. Esta rota é utilizada para agilizar as comunicações que ocorrem entre os componentes do próprio Windows Server 2003, dentro do mesmo servidor. Ao usar a interface de loopback, toda a comunicação ocorre a nível de software, ou seja, não é necessário enviar o pacote através das diversas camadas do protocolo TCP/IP, até que o pacote chege na camada de enlace (ou seja, a placa de rede), para depois voltar. Ao invés disso é utilizada a interface de loopback para direcionar os pacotes corretamente. Observe que esta entrada tem como máscara de sub-rede o número 255.255.255.255. Esta máscara indica que a entrada é uma rota para um endereço IP específico (no caso o próprio IP do servidor) e não uma rota para um endereço de rede.

Network broadcast (Broadcast de rede):

 Esta rota define o endereço de broadcast da rede. Broadcast significa enviar para todos os computadores da rede. Quando é utilizado o endereço de broadcast, todos os computadores da rede recebem o pacote e processam o pacote. O broadcast é utilizado por uma série de serviços, como por exemplo o WINS, para fazer verificações periódicas de nomes, para enviar uma mensagem para todos os computadores da rede, para obter informações de todos os computadores e assim por diante. Observe que o gateway é o número IP da placa de rede do servidor e a Interface é este mesmo número, ou seja, para enviar um broadcast para a rede, envie através da placa de rede do servidor, não há necessidade de utilizar o roteador. Um detalhe interessante é que, por padrão, a maioria dos roteadores bloqueia o tráfego de broadcast, para evitar congestionamentos nos links de WAN.

Rede/endereço de loopback:



Comentei anteriormente que os endereços da rede 127.0.0.0 são endereços especiais, reservados para fazer referência a si mesmo. Ou seja, quando faço uma referência a 127.0.0.1 estou me referindo ao servidor no qual estou trabalhando. Esta roda indica, em palavras simples, que para se comunicar com a rede de loopback (127.0.0.0/255.0.0.0), utilize "eu mesmo" (127.0.0.1).

Multicast address (endereço de Multicast):



O tráfego IP, de uma maneira simples, pode ser de três tipos: Unicast é o tráfego direcionado para um número IP definido, ou seja, com um destinatário. Broadcast é o tráfego dirigido para todos os computadores de uma ou mais redes. E tráfego Multicast é um tráfego direcionado para um grupo de computadores, os quais estão configurados e "inscritos" para receber o tráfego multicast. Um exemplo prático de utilização do multicast é para uma transmissão de vídeo através da rede. Vamos supor que de uma rede de 1000 computadores, apenas 30 devem receber um determinado arquivo de vídeo com um treinamento específico. Se for usado tráfego unicast, serão transmitidas 30 cópias do arquivo de vídeo (o qual já é um arquivo grande), uma cópia para cada destinatário. Com o uso do Multicast, uma única cópia é transmitida através do link de WAN e o tráfego multicast (com base no protocolo IGMP), entrega uma cópia do arquivo apenas para os 30 computadores devidamente configurados para receber o tráfego multicast. Esta rota define que o tráfego multicast deve ser enviado através da interface de rede, que é o número IP da placa de rede do servidor.Lembrando do Capítulo 2, quando falei sobre classes de endereços, a classe D é reservada para tráfego multicast, com IPs iniciando (o primeiro número) a partir de 224.

Limited Broadcast (Broadcast Limitado):



Esta é a rota utilizada para o envio de broadcast limitado. O endereço de broadcast limitado é formato por todos os 32 bits do endereço IP sendo iguais a 1 (255.255.255.255). Este endereço é utilizado quando o computador tem que fazer o envio de um broadcast na rede local (envio do tipo um para todos na rede), porém o computador não conhece a número da rede local (network ID). Você pode perguntar: Mas em que situação o computador não conhecerá a identificação da rede local? Por exemplo, quando você inicializa um computador, configurado para obter as configurações do TCP/IP a partir de um servidor DHCP, a primeira coisa que este computador precisa fazer é localizar um servidor DHCP na rede e requisitar as configurações do TCP/IP. Ou seja, antes de receber as configurações do DHCP, o computador ainda não tem endereço IP e nem máscara de sub-rede, mas tem que se comunicar com um servidor DHCP. Esta comunicação é feita via broadcast limitado, onde o computador envia um pacote de formato específico (chamado de DHCP Discover), para tentar descobrir um servidor DHCP na rede. Este pacote é enviado para todos os computadores. Aquele que for um servidor DHCP irá responder a requisição do cliente. Aí o processo de configuração do DHCP continua (conforme descreverei na seção sobre DHCP), até que o computador esteja com as configurações do TCP/IP definidas, configurações estas obtidas a partir do servidor DHCP.

Em termos de roteamento, estes são os conceitos necessários ao que será visto neste tutorial. Agora é hora de tratar sobre a divisão de uma rede em sub-redes, assunto mais conhecido como: subnetting. Mas este é assunto para as próximas partes deste tutorial.

**ICMP**

Teste de conectividade

**Load Balance**

O balanceamento de carga refere-se à distribuição eficiente do tráfego de rede de entrada em um grupo de servidores backend, também conhecidos como uma *fazenda de servidores* ou *pool de servidores*.

Os sites modernos de alto tráfego devem atender centenas de milhares, se não milhões, de solicitações simultâneas de usuários ou clientes e devolver os dados corretos de texto, imagens, vídeo ou aplicativos, tudo de forma rápida e confiável. Para dimensionar de forma econômica para atender a esses grandes volumes, as práticas recomendadas modernas de computação geralmente exigem a adição de mais servidores.

Um [balanceador de carga](https://www.nginx.com/solutions/adc) atua como o "policial de trânsito" sentado na frente de seus servidores e roteando solicitações de clientes em todos os servidores capazes de atender a essas solicitações de forma a maximizar a eficiência e a utilização da capacidade e garantir que nenhum servidor esteja sobrecarregado, o que poderia degradar o desempenho. Se um único servidor cair, o balanceador de carga redireciona o tráfego para os servidores on-line restantes. Quando um novo servidor é adicionado ao grupo do servidor, o balanceador de carga começa automaticamente a enviar solicitações para ele.

Desta forma, um balanceador de carga executa as seguintes funções:

* Distribui solicitações de clientes ou carga de rede de forma eficiente em vários servidores
* Garante alta disponibilidade e confiabilidade enviando solicitações apenas para servidores que estão online
* Fornece a flexibilidade para adicionar ou subtrair servidores à medida que a demanda dita

### Algoritmos de balanceamento de carga

Diferentes algoritmos de balanceamento de carga proporcionam diferentes benefícios; a escolha do método de balanceamento de carga depende de suas necessidades:

* Round Robin – As solicitações são distribuídas pelo grupo de servidores sequencialmente.
* Menos Conexões – Uma nova solicitação é enviada ao servidor com o menor número de conexões atuais aos clientes. A capacidade relativa de computação de cada servidor é fatorada para determinar qual deles tem menos conexões.
* Menos Tempo – Envia solicitações ao servidor selecionado por uma fórmula que combina o  
  tempo de resposta mais rápido e menos conexões ativas. Exclusivo do NGINX Plus.
* Hash – Distribui solicitações com base em uma chave que você define, como o endereço IP do cliente ou  
  a URL de solicitação. O NGINX Plus pode opcionalmente aplicar um hash consistente para minimizar a redistribuição  
  de cargas se o conjunto de servidores upstream mudar.
* IP Hash – O endereço IP do cliente é usado para determinar qual servidor recebe a solicitação.
* Random with Two Choices – Escolhe dois servidores aleatoriamente e envia a solicitação para aquele  
  que é selecionado aplicando então o algoritmo Menos Conexões (ou para nginx plus  
  o algoritmo de menos tempo, se assim configurado).

**CDN**

A Content Delivery Network (CDN) é uma rede geograficamente distribuída de servidores e seus data centers que ajudam na distribuição de conteúdo para usuários com atraso mínimo.

Ele faz isso aproximando o conteúdo da localização geográfica dos usuários por meio de data centers estrategicamente localizados chamados Pontos de Presença (PoPs). Os CDNs também envolvem servidores de cache que armazenam e fornecem arquivos armazenados em cache para acelerar os tempos de carregamento da página da Web e reduzir o consumo de largura de banda. Vamos entrar em mais detalhes de como os CDNs funcionam abaixo.

Os serviços de CDN são essenciais para empresas que dependem da entrega de conteúdo aos usuários.

Considere o seguinte:

* Grandes publicações de notícias com leitores em muitos países
* Sites de mídia social que precisam fornecer conteúdo multimídia nos feeds dos usuários
* Sites de entretenimento como netflix entregando conteúdo web de alta definição em tempo real
* Plataformas de e-commerce com milhões de clientes
* Empresas de jogos com conteúdo gráfico pesado sendo acessado por usuários geograficamente distribuídos

Todas essas empresas precisam garantir a aceleração de sua entrega de conteúdo, disponibilidade de serviços, escalabilidade de recursos e segurança de aplicativos web. É aqui que os serviços de CDN brilham como uma vantagem única.

**DNS**

O DNS (Domain Name System – Sistema de nome de domínio) converte nomes de domínio legíveis por humanos (por exemplo, www.amazon.com) em endereços IP legíveis por máquina (por exemplo, 192.0.2.44).

## Fundamentos do DNS

Todos os computadores da internet, abrangendo de smartphones ou laptops a servidores que distribuem conteúdo para grandes websites do comércio, se encontram e se comunicam entre si usando números. Esses números são conhecidos como endereços IP. Ao abrir um navegador e acessar um site, você não precisará lembrar-se de um longo número nem digitá-lo. Em vez disso, você poderá informar um nome de domínio, como exemplo.com, e ainda assim encontrar o que deseja.

Um serviço DNS, como o Amazon Route 53, é um serviço globalmente distribuído que converte nomes legíveis por humanos, como www.exemplo.com, em endereços IP numéricos, como 192.0.2.1, usados pelos computadores para se conectarem entre si. O sistema DNS da internet funciona praticamente como uma agenda de telefone ao gerenciar o mapeamento entre nomes e números. Os servidores DNS convertem solicitações de nomes em endereços IP, controlando qual servidor um usuário final alcançará quando digitar um nome de domínio no navegador da web. Essas solicitações são chamadas consultas.

## O que é DMZ?

DMZ é uma sigla para *Demilitarized Zone*(Zona Desmilitarizada em português), é uma subrede que se situa entre uma rede confiável (a rede da sua organização, por exemplo) e uma rede não confiável (geralmente a internet), provendo assim isolamento físico entre as duas redes, garantido por uma série de regras de conectividade mantidas no *firewall*. O aspecto do isolamento físico do DMZ é importante por o mesmo garantir que a internet acesse apenas os servidores isolados no DMZ, ao invés de acessar diretamente a rede interna da sua organização, como pode ser visto na Figura 3.1. A servidore mais comumente encontrados no DMZ são os de email, FTP, e HTML.

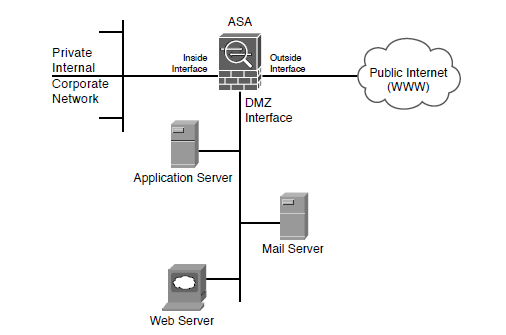
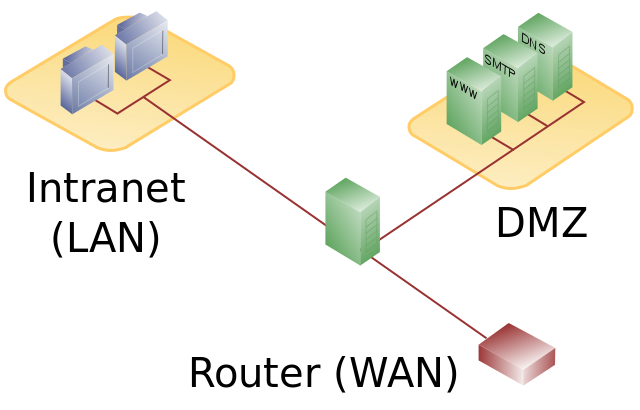
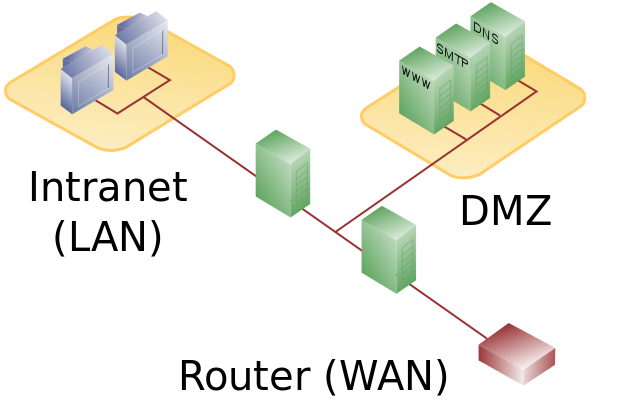


Figura 3.1: O isolamento físico do DMZ[1]

Apenas por curiosidade: O termo DMZ surgiu no meio militar, e significava uma área entre as áreas aliadas e inimigas. A DMZ (no sentido original, não computacional) mais famosa do mundo fica entre as fronteiras da Coréia do Norte e Coréia do Sul, que desde o fim da Guerra da Coréia (1953) ainda não assinaram um tratado de paz

## 3.2 - Arquiteturas de DMZ

* *Single Firewall*É a arquitetura apresentada na Figura 3.1. Qualquer *firewall* com pelo menos 3 interfaces de rede pode formar uma arquitetura desse tipo. Neste caso, A primeira interface de rede conecta o *firewall* à internet através do ISP, a segunda interface forma a rede interna e a terceira interface é usada para criar a DMZ. Esse tipo de arquitetura é considerado vulnerável devido ao fato do *firewall* ter que lidar com as requisições para a rede interna e o DMZ, sendo um ponto óbvio de ataque na arquitetura de segurança da rede. Um exemplo mais detalhado dessa arquitetura pode ser visto na figura 3.2.  
    
  Figura 3.2: A arquitetura Single Firewall[2]
* *Multiple Firewall*É a arquitetura considerada a mais segura quando se utiliza um DMZ. Utiliza mais de um firewall (geralmente dois), onde o primeiro, também chamado de firewall exterior ou de *"front-end"* é utilizado para direcionar o tráfego da internet para a DMZ apenas, enquanto os demais são utilizados para direcionar o tráfego da DMZ para a rede interna. Esse tipo de arquitetura é considerado mais seguro pois para que a rede interna seja comprometida, é necessário que os dois *firewalls* sejam comprometidos. Por isso, quando essa arquitetura é utilizada, é comum que se usem *firewalls* de fabricantes diferentes, pois é mais difícil que as falhas de segurança encontradas no produto de um fabricante sejam encontradas no produto de outro, tornando assim a rede mais segura e confiável. Um exemplo dessa arquitetura pode ser visto na figura 3.3.  
    
  Figura 3.2: A arquitetura Multiple Firewall[3]

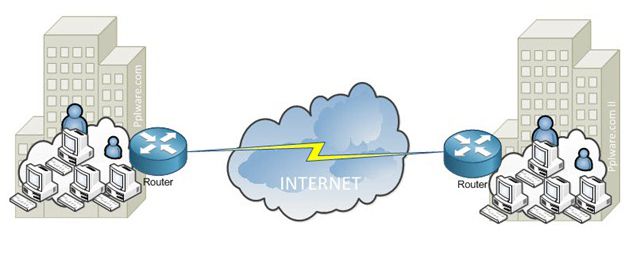
**VPN**

VPN ou Virtual Private Network (Rede Privada Virtual) trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores através de uma rede pública, como a Internet. Ao invés de realizar esse procedimento por meio de links dedicados ou redes de pacotes, como Frame Relay e X.25, utiliza-se a infraestrutura da internet para conectar redes distantes e remotas.

A Rede Privada Virtual possui a grande vantagem de ser bem mais barata que os links dedicados. Além disso, a Internet está presente em todo o mundo com pontos de acesso espalhados por todos os lugares. As redes VPN são muito utilizadas pelas grandes empresas, especialmente nas companhias em que funcionários trabalham remotamente, seja nas ruas ou no sistema home office, para se conectar à estrutura interna mesmo estando longe. Usuários comuns também aproveitam a tecnologia das redes VPN para construírem redes privadas virtuais.

O nível de custo-benefício das redes VPN em comparação com os links dedicados aumenta à medida que as distâncias entre as conexões também aumentam. Os links dedicados são muito caros, apesar de possuírem uma melhor privacidade e segurança em relação às redes Virtual Private Network. Por ser baseada em uma rede pública, onde existe uma enorme quantidade de tráfego de dados que podem ser transmitidos e recebidos por qualquer equipamento atualmente, a VPN não disponibiliza um alto nível de confiabilidade e segurança para com as informações que transitam por ela.

Porém, por meio da criptografia nas informações e nas comunicações entre hosts da rede privada é possível aumentar consideravelmente a confidenciabilidade dos dados que trafegam pela rede. Por meio do sistema de tunelamento, os dados podem ser enviados sem que outros usuários tenham acesso, e mesmo que os tenham, ainda os receberão criptografados. Por isso, é fundamental que os dispositivos responsáveis por cuidar da rede VPN devem ser capazes de garantir segurança e integridade das informações e dos dados que são transmitidos.



O IPSec (IP Security Protocol) é uma suite de protocolos criado para a construção de túneis seguros sobre redes de internet e intranet. Essa ferramenta permite que todos os dados passem pelo gateway para serem cifrados antes de percorrerem o caminho para a máquina de destino ou decifrado antes do recebimento dos dados.

Outro problema que a rede VPN pode trazer é em relação à dependência da velocidade da Internet disponível, ainda mais se a quantidade de tráfego que ela envia for bastante grande. Por isso, algumas empresas podem ter dificuldades em utilizá-la caso as suas conexões não forem estáveis e velozes. Conexões ruins podem acarretar problemas técnicos e atrasos sem que o usuário tenha controle sobre isso.

Obviamente, para se criar uma rede VPN é necessário ter pelo menos dois computadores conectados à internet, além de um programa de gerenciamento de rede VPN instalado em cada máquina. Para enviar os dados, o programa criptografa e encapsula as informações, além de adicionar o número de IP da máquina remetente para que o computador de destino possa identificar quem enviou os dados. Por meio do sistema de tunelamento, os dados percorrem o caminho até chegar à máquina receptora que identifica imediatamente as informações de IP que foram enviadas pela máquina remetente. Após isso, o processo inverso é realizado, com a "descriptografação" e armazenamento dos dados no computador de destino.

**Gateway**

Simplificando, um gateway padrão é um nó que permite uma conexão perfeita entre redes, permitindo que uma máquina converse com outra máquina em uma rede diferente. É chamado de gateway 'padrão' porque é a primeira e padrão rota tomada a menos que outra opção seja solicitada ativamente.

O uso mais comum para o gateway padrão é ter acesso a uma página web, onde a solicitação será enviada através do gateway antes de ir para a internet. Outro uso fundamental é conectar dispositivos em uma [sub-rede](http://www.itpro.co.uk/network-internet/31770/what-is-subnetting) com dispositivos em outra, com o gateway padrão agindo como um intermediário.

Os gateways padrão são essencialmente sistemas de roteamento que garantem que a solicitação seja enviada para o destino certo, mesmo que o remetente e o receptor usem [protocolos de rede diferentes](https://www.itpro.co.uk/network-internet/30416/http-vs-https-what-difference-does-it-make-to-security).

O dispositivo que envia a solicitação é o 'dispositivo originário', e como parte do processo, o dispositivo enviará uma solicitação de acesso usando uma tabela de roteamento. Isso determina a rota mais eficiente para enviar a solicitação e qual deve ser o roteador. O gateway padrão recebe qualquer solicitação que não tenha um roteador específico identificado, garantindo que os dados ainda possam fluir.

Quando você tem uma pequena rede, como em casa, o gateway padrão geralmente será o roteador principal. No entanto, à medida que as redes aumentam de tamanho, ou nos casos em que várias redes podem estar operando simultaneamente, um sistema de sub-redes será usado juntamente com um gateway padrão específico.

### Como encontrar o endereço IP do gateway padrão

Localizar o [endereço IP](https://www.itpro.co.uk/virtual-private-network-vpn/30351/how-do-you-hide-an-ip-address) do gateway padrão é especialmente importante, pois permite que você descubra quaisquer problemas que possa ter com sua rede ao solucionar problemas ou acessar a ferramenta de gerenciamento baseada na Web do roteador.

Felizmente, o endereço de gateway padrão é muito fácil de encontrar. Se o seu sistema operacional de escolha for o Windows, basta ir ao Painel de Controle e selecionar a Central de Rede e Compartilhamento. Dependendo da versão, clique nas opções do adaptador Alterar ou alterar as configurações do adaptador. Em seguida, localize a rede para a qual você gostaria de encontrar o gateway padrão. Ao localizá-lo, clique duas vezes nele e escolha "Detalhes" do pop-up. Lá, você poderá ler o [IPv4](https://www.itpro.co.uk/internet-protocol-version-6-ipv6/30657/whatever-happened-to-ipv6) Default Gateway que estará em algum lugar da lista.

O processo é ainda mais simples para usuários de MacOS: vá para Preferências do Sistema e selecione Rede, seguido pelo nome da rede que você está usando. O endereço IP será exibido na guia TCP/IP como uma série de números em 'Roteador'.

**Proxy**

Os servidores proxy são uma ferramenta essencial para [permanecer anônimos enquanto navegam na Web](https://www.itpro.co.uk/security/privacy/355506/switch-to-the-anonymous-web), servindo como intermediário entre o dispositivo do usuário, seja um telefone, tablet ou PC, e o servidor de onde está solicitando informações.

Como o nome sugere, essas ferramentas atuam como proxies em nome do usuário e mascaram sua verdadeira identidade enviando informações falsas para um servidor de destino. Isso impede que o servidor descubra quem está solicitando informações, incluindo o local de origem dessa solicitação.

O principal apelo do uso de servidores proxy é que eles normalmente [bloqueiam a comunicação de dados pessoais](https://www.itpro.co.uk/general-data-protection-regulation-gdpr), no entanto, de certa forma, compreensivelmente, os servidores proxy têm a reputação de facilitar o crime online devido ao anonimato que fornecem.No entanto, há muitos benefícios para usuários e empresas cotidianas. Algumas organizações usam servidores proxy para testar a qualidade das conexões com seus serviços de regiões específicas em todo o mundo. Os consumidores também podem contornar bloqueios regionais em conteúdo online, como o Netflix, ou simplesmente usá-los como uma camada adicional de segurança enquanto usam a internet em ambientes públicos.

### **Como funciona um servidor proxy?**

Cada usuário que acessa a internet a partir de um dispositivo recebe seu próprio [endereço IP](https://www.itpro.co.uk/network-internet/31770/what-is-subnetting) exclusivo, um identificador que é usado para avaliar de onde a conexão está vindo. Por exemplo, se um usuário abrisse uma página da Web e navegasse para o Google, o endereço IP do usuário seria enviado para o Google, o que alteraria sua página inicial e os resultados de pesquisa com base na localização do usuário.

Um servidor proxy funciona como um intermediário entre o usuário e o servidor do site, o que significa que o endereço IP deve primeiro passar pelo proxy antes de ser enviado em diante. Os proxies têm uma variedade de funções dependendo de sua configuração (veja abaixo), mas a maioria impede que a localização de um usuário seja descoberta enviando um endereço IP diferente para o servidor. No que diz respeito ao servidor, o IP que ele recebe é o enviado pelo dispositivo do usuário.

**Proxy Reverso**

Um proxy reverso é um servidor de rede geralmente instalado para ficar na frente de um servidor Web. Todas as conexões originadas externamente são endereçadas para um dos servidores Web através de um roteamento feito pelo servidor [proxy](https://pt.wikipedia.org/wiki/Proxy), que pode tratar ele mesmo a requisição ou encaminhar a requisição toda ou parcialmente a um servidor Web, que tratará dela.

Um proxy reverso repassa o tráfego de rede recebido para um conjunto de servidores, tornando-o a única interface para as requisições externas. Por exemplo, um proxy reverso pode ser usado para balancear a carga de um cluster de servidores Web. O que é exatamente o oposto de um proxy convencional, que age como um despachante para o tráfego de saída de uma rede, representando as requisições dos clientes internos para os servidores externos à rede a qual o servidor proxy atende.