



SORC I

Definições

REDE

Computadores ou dispositivos interligados via cabo ou wireless, os quais compartilham recursos entre si

HOST

Define uma máquina ou dispositivo dentro de uma rede

SERVER/SERVIDOR

Uma máquina da rede dedicada a disponibilizar um determinado serviço:

- Impressão
- Diretório
- Banco de dados
- Email

...

CLIENT/CLIENTE

Uma máquina da rede que pode usufruir do serviço de um servidor

Tamanhos de rede



LAN (Local Area Network)

Interligam máquinas dentro de um mesmo espaço físico, geralmente residencial

WLAN (Wireless Local Area Network)

Redes residenciais que conectam a casa das pessoas à Internet



MAN (Metropolitan Area Network)

Redes com extensões de dezenas de quilômetros, alcançando cidades inteiras

WMAN (Wireless Metropolitan Area Network)

Versão sem fio da MAN, com alcance de dezenas de quilômetros por sinais de rádio

PAN (Personal Area Network)

Redes com distâncias bastante limitadas, comumente usadas para conexões Bluetooth e UWB (Ultra Wide Band)

SAN (Storage Area Network)

Redes de área de armazenamento, servindo especificamente para salvar objetos como arquivos de mídia e outros dados

Ex: Google Drive

WAN (Wide Area Network)

Rede de extensão mundial, que atravessa fronteiras entre países, sendo o escopo da própria Internet e composta por pontos essenciais que são os Data Centers

Topologias de Rede

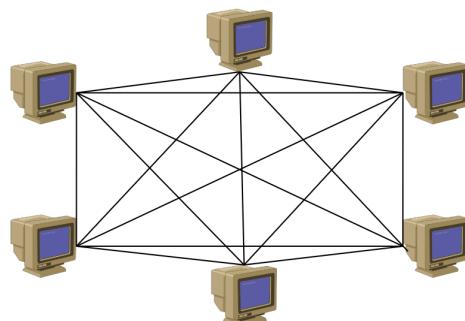
Diz respeito ao layout físico das redes de computadores, como elas estão dispostas ou organizadas num determinado espaço. A topologia de uma rede influencia em diversos outros fatores e deve ser bem planejada antes da montagem da rede.

Malha

Todos os computadores são interligados por vários segmentos de cabos.

Essa topologia não é mais usada atualmente.

- Redundância e confiabilidade
- Diagnóstico fácil
- Custo de instalação
- Complexidade do cabeamento



Exemplo de rede em malha

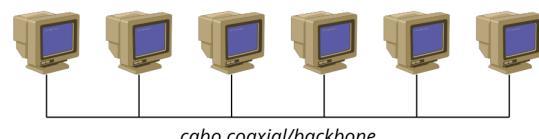
- Falha em qualquer ponto derruba a rede

Barramento

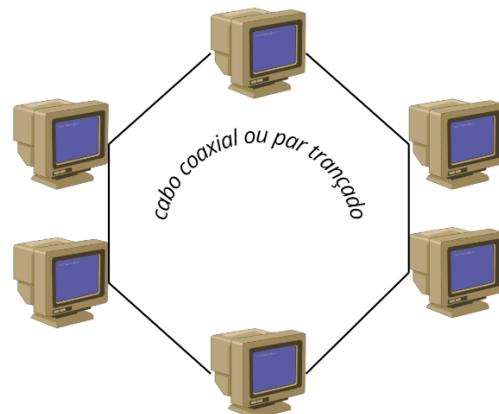
Todos os computadores são ligados a um único cabo que estrutura a rede.

Essa topologia não é mais usada atualmente.

- Economia de cabo
- Simplicidade de instalação
- Facilidade de expansão
- Falha em qualquer ponto derruba a rede



Exemplo de rede em barramento



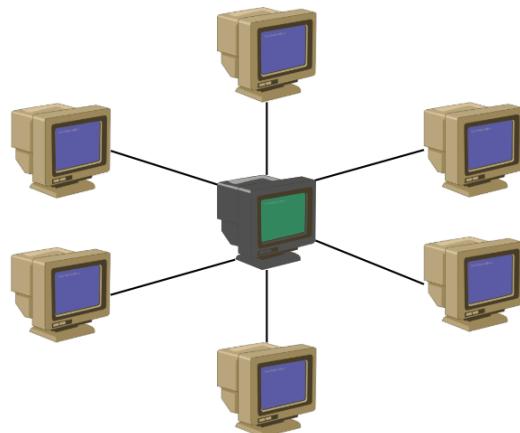
Exemplo de rede em anel

Anel

Cada máquina é ligada a duas outras em sequência, fechando um ciclo.

Essa topologia é raríssima atualmente.

- Acesso igualitário à rede
- Aumento de usuários não impacta performance
- Problemas difíceis de isolar
- Falha em qualquer ponto derruba a rede



Exemplo de rede em estrela

Estrela

Todas as máquinas são ligadas a um dispositivo central chamado

concentrador, que pode ser um switch ou servidor.

Essa topologia é a mais adotada atualmente.

- Fácil adição de dispositivos
- Gerenciamento centralizado
- Falha em qualquer ponto não derruba a rede
- Falha no dispositivo central derruba a rede

Modelo OSI

Não é propriamente uma arquitetura de rede, mas define funções para cada camada de comunicação em rede. Foi criado como uma padronização de fabricantes para comunicação entre dispositivos de rede.

É composto de 7 camadas de comunicação pelas quais os dados transmitidos em rede devem passar para chegar ao seu destino, tanto no envio quanto na recepção.



A primeira camada do modelo OSI é chamada de **física**, porque comprehende os cabeamentos que conectam dispositivos de rede, como switches. Nessa camada, os dados são transferidos bit por bit.

A segunda camada, chamada de **enlace ou ligação**, possui duas subcamadas: uma verifica se existem erros nos dados e outra controla o fluxo desses dados. Podemos encontrar tecnologias como VLans e topologias token ring ou ponto-a-ponto nessa camada.

A subcamada MAC permite conectar diversos computadores em uma rede por meio do endereço físico das máquinas, o endereço MAC. Esse endereço é usado para identificar pacotes de dados e enviá-los da camada física para a próxima subcamada.

A subcamada LLC controla o fluxo dos dados na rede. Ela permite que vários protocolos da próxima camada sejam simultâneos numa mesma rede.

A terceira camada, de **rede**, é quem usa endereçamento IP do host de origem e do host de destino para definir o caminho dos dados, podendo priorizar alguns pacotes.

Ela usa o endereço IP ao invés do MAC porque esse último é alterado quando os dados passam por dispositivos físicos de rede (roteadores, switches, servidores) antes do dispositivo final. Já o IP não sofre essa

alteração, porque identifica a máquina dentro da rede, e não apenas a máquina física.

Essa camada usa protocolos como IP ou ICMP.

A próxima camada é a de **transporte**. Ela garante que os pacotes vindos da camada anterior sejam enviados e entregues ao destino. Protocolos muito comuns aqui são TCP e UDP, que podem garantir consistência de entregas ou inconsistência em troca de maior velocidade, respectivamente.

Nesse ponto, os dados já possuem um destino conhecido e já podem ser transportados, mas ainda é necessário uma conexão entre os hosts.

A camada de **sessão** é responsável por estabelecer e encerrar as conexões entre os hosts, sincronizando-os. Além disso, ela dá suporte às sessões criadas por meio de registros de log e tarefas de segurança.

No entanto, os pacotes de dados ainda não são acessados aqui, porque antes eles precisam de tratamento.

A camada de **apresentação** consegue traduzir os dados em caracteres e compactá-los. Caso seja necessário, os dados também são criptografados nessa camada. Agora, eles estão prontos para serem consumidos.

A camada de **aplicação** diz respeito à interação humano-máquina que se dá no front-end. Os usuários dos computadores não vêm dados em sua forma primitiva, na verdade eles acessam serviços como e-mails, transferência de arquivos e uso de websites, por onde os dados são exibidos e enviados em formato de mídia.

A camada de aplicação usa protocolos conhecidos como HTTP, FTP, DNS, entre outros.



Protocolos de comunicação

São regras que padronizam a comunicação entre diferentes dispositivos em diferentes redes.



TCP/IP

É uma arquitetura de rede que se baseia em 2 protocolos principais: Transfer Control Protocol e Internet Protocol.

Endereço IP

É uma sequência numérica que identifica um dispositivo dentro de uma rede. Isso significa que, pelo endereço IP de um computador, podemos saber também a rede da qual ele faz parte.

Essa sequência numérica normalmente é visualizada em formato decimal, mas é importante saber sua conversão para binário.

O endereço IP é formado por 4 sequências de números separados por pontos. O valor decimal máximo para cada parte do endereço IP é 255, e o mínimo é 0 (256 valores possíveis)

No entanto, considerando o endereço IP como identificação de dispositivo, cada parte dele vai de 1 até 254 (0 e 255 são números reservados para outras funções que não são identificar hosts)

Em formato decimal, cada parte do endereço IP é um octeto: um número binário composto por 8 bits, e cada bit pode ter o valor de 0 ou 1.

Ao somarmos os 4 octetos, temos 32 bits totais em um endereço IP.

Endereço IP

Em decimal: 4 números de 1 a 255

Em binário: 4 octetos (32 bits)

00000000.00000000.00000000.00000000

Classes de IP

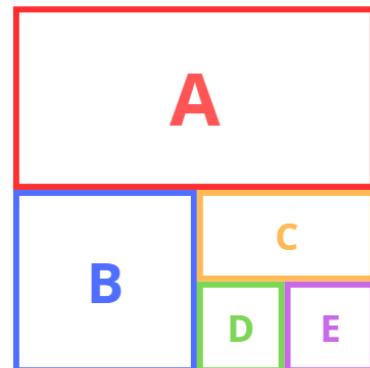
Existem 5 classes de endereço IP: A,B,C,D e E.

Todos os endereços IPs possíveis são divididos entre essas 5 classes, mas não igualmente.

Além disso, as classes se baseiam na primeira parte ou no primeiro octeto do endereço IP. Isso significa que olhando a primeira parte do endereço IP, você descobre a qual classe ele pertence.

Classes	Primeiro octeto em decimal
A	1-126
B	128-191
C	192-223
D	224-239
E	240-255

Classes de IP



Representação da quantidade de endereços em cada classe



As classes ABC são as utilizadas para distribuição de números de hosts.

As classes D e E são usadas por provedores de internet.

Separação Host x Rede

Como um endereço IP pode identificar tanto um dispositivo quanto sua rede, um IP pode ser dividido em 2 partes: uma representa a rede e outra representa o host.

Basicamente, todos os números do endereço são separados: a parte esquerda, ou seja, os primeiros octetos, representam a rede. A parte direita, ou seja, os últimos octetos, representam o host.

Mas como saber quantos octetos são de rede ou de host? Cada classe de endereço IP tem uma quantidade padrão de octetos para rede e para host.

Classes	Primeiro octeto em decimal	Octetos de Rede	Octetos de Host	Máximo de hosts
A	1-126	1	3	16777214
B	128-191	2	2	65534
C	192-223	3	1	254

Naturalmente, as classes com mais octetos de rede podem criar mais subredes, enquanto que classes com mais octetos de host podem ter mais dispositivos conectados à rede.



A classe C é a mais utilizada de todas

Provavelmente o endereço IP do seu computador começa com 192.168.1

Além de podermos separar o endereço IP entre parte de rede e de host, podemos reescrevê-lo na forma de rede ou de host:

- **Endereço de rede:** corresponde ao IP com os octetos de rede, enquanto os restantes são preenchidos com zero.
 - **⚠️ Portanto, IPs terminados em 0 não são usados para hosts e sim para indicar redes!**
- **Endereço de host:** corresponde ao IP apenas com os octetos de host.

Broadcast

Dentro de uma rede, o endereço de broadcast **sempre será o último IP possível**.

Isso significa que o **endereço de broadcast** é composto pelos octetos de rede, enquanto os restantes são preenchidos com o valor máximo: 255.

⚠️ Portanto, IPs terminados em 255 não são usados para host mas para broadcast!

Essa é uma tecnologia que permite transmitir dados para múltiplos hosts de forma simultânea dentro da mesma rede, ou seja, permite a comunicação em massa dentro da rede.

Qualquer mensagem enviada para o endereço de broadcast vai ser retransmitida para todos os hosts dentro da rede.

Quando uma mensagem não chega no seu destino, ela “morre” no endereço de broadcast. Isso impede o looping dos dados à procura do destino.

Em switches gerenciáveis os dados que “morreram” no broadcast são armazenados em logs e só podem ser acessados via linha de código em um terminal.

Máscaras de subrede

São endereços no mesmo formato do IP, só que servem para “mascarar” endereços de IP, no sentido de fazer o IP de uma classe específica funcionar como o IP de outra classe.

Cada classe de IP tem uma máscara padrão, e essa máscara obedece a separação rede-host da sua classe.

Uma máscara de subrede é preenchida com 255 nos octetos de rede e 0 nos octetos de host.

Classes	Máscara de subrede	Octetos de rede	Octetos de host
A	255.0.0.0	1	3
B	255.255.0.0	2	2
C	255.255.255.0	3	1

Por exemplo, um endereço 10.0.0.1 pertence à classe A. Sua rede pode ser dividida em poucas subredes em comparação à classe C porque apenas seu primeiro octeto é de rede. Os três restantes são usados para identificar hosts.

Agora, esse endereço classe A não necessariamente tem uma máscara de classe A. Sua máscara pode ser definida como 255.255.0.0, por exemplo, que é a máscara da classe B. Essa classe, por sua vez, consegue fazer mais subredes.

Isso significa que o IP 10.0.0.1 vai “funcionar” como um IP de classe B, permitindo criar mais subredes. O cálculo usado para criar subredes vai aparecer mais para frente.

A criação de subredes pode ser feita através das máscaras ou de um método que usa apenas o próprio IP.

Notação CIDR

As máscaras de subrede podem ser abreviadas no que chamamos prefixo CIDR (Classless Inter-Domain Routing).

Essa notação indica a classe de um IP através da quantidade de bits de rede que ele tem, sendo precedida por uma barra.

Classes	Prefixo CIDR	Máscara de subrede	Octetos de rede	Bits de rede
A	/8	255.0.0.0	1	8
B	/16	255.255.0.0	2	16
C	/24	255.255.255.0	3	24
...

A notação CIDR basicamente é outra forma de escrever as máscaras. No entanto, ela ainda possui um diferencial: esse tipo de formatação consegue criar mais subredes que a estrutura das classes.

Isso porque esse sistema foi criado com intuito de aumentar a flexibilidade na criação de subredes. Ao invés de condicionar o usuário em 3 tipos de redes padronizadas, o sistema CIDR permite usar quantos bits que você quiser para dividir o IP de rede e de host (dos 32 existentes)

Portanto, quanto maior o número da notação CIDR, mais subredes será possível criar.

Para descobrir os valores dos bits em uma máscara personalizada, use a tabela:

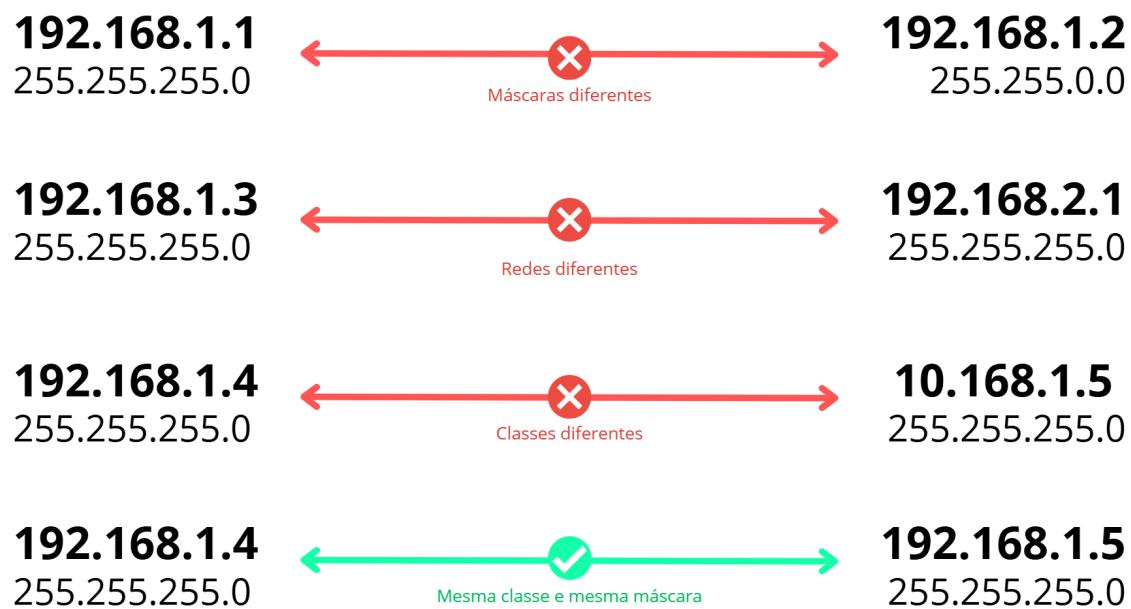
Quando ocorre comunicação

Naturalmente, duas máquinas só podem se comunicar se estiverem conectadas, ou seja, se estiverem numa mesma rede.

Se cada rede possui uma classe específica, então é importante perceber que hosts só se comunicam se seus endereços IP forem da mesma classe.

Outra condição é a máscara de subrede. A máscara dos hosts precisa ser igual para que eles consigam se comunicar ou “enxergar”.

Isso porque a máscara “transforma” a classe de uma rede em outra, ou seja, é como se fossem redes diferentes mesmo com octetos de rede iguais.



Cálculo de Subrede

Vamos aprender a dividir uma rede com base na máscara de subrede que aplicamos no endereço IP.

Um dos jeitos mais fáceis é entender o cálculo passo a passo.

Para começar, você precisa saber de ante mão:

- Qual o endereço da rede
- Qual a máscara de subrede padrão
- Em quantas subredes você deseja dividir a sua rede principal

Primeiramente, vamos entender como cada etapa funciona por cima:

1. Determinamos uma nova máscara para as subredes, que é diferente da máscara padrão da rede principal. Ela vai permitir que mais bits do IP sejam usados para criar essas subredes dentro da rede principal, que não altera sua máscara.
2. Calculamos o salto entre as subredes através de uma fórmula. Esse número vai indicar quantos hosts cada subrede vai conseguir abrigar.
3. Escrevemos a lista de subredes saltando cada octeto final pelo número do salto.

Agora, vamos explicar cada etapa do cálculo com exemplos.

1 - Achar a máscara das subredes

A primeira coisa que precisamos fazer é transformar a quantidade de subredes desejadas em uma potência de base 2.

Isso basicamente vai nos dizer quantos bits adicionais serão necessários para a parte de rede, de forma que consiga criar a quantidade de redes necessárias.

Se o número de subredes que você pretende criar é ímpar ou não possui uma potência específica na base 2, você sempre precisa arredondar essa quantidade de subredes para cima, ou seja, para o próximo número que seja possível escrever em 2^x .

Quantidade de subredes	Potência base 2	Bits	Expoente
2	2^1	2	1
3	2^2	4	2
4	2^2	4	2

Quantidade de subredes	Potência base 2	Bits	Expoente
5	2^3	8	3
6	2^3	8	3
7	2^3	8	3
8	2^3	8	3
9	2^4	16	4
10	2^4	16	4
...

Depois de achar o expoente certo, você precisa adicionar o número do expoente ao número da máscara padrão.

O resultado será o prefixo da máscara das subredes que você vai criar.

Perceba que a sua rede principal e as subredes dentro dela terão exatamente o mesmo endereço IP, mas a máscara delas vai ser diferente*

▼ Exemplo: achando o prefixo de 8 subredes para uma rede classe C

192.168.1.0 → Endereço da rede

255.255.255.0 (/24) → Máscara de subrede padrão

8 → Quantidade de subredes necessárias

8 = **2³** → Quantidade de subredes em potência de base 2

3 + **24** = **27** → Adição à máscara padrão

/27 → Máscara das 8 subredes

2 - Achar o salto

Agora que você sabe o prefixo das suas subredes, você precisa converter esse prefixo no formato de máscara de subrede padrão.

Mesmo que existam 3 máscaras de subrede padrões para cada classe de IP, os diferentes prefixos CIDR também podem ser convertidos para esse formato.

Nos casos que fugirem das 3 classes, os bits adicionais devem ser convertidos do formato de octeto para o decimal.

Existe uma tabela que facilita achar esses resultados.

IPv4 CIDR Chart

RIPE NCC

IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0
64 K	16	/16	255.255.0.0
128 K	17	/15	255.254.0.0
256 K	18	/14	255.252.0.0
512 K	19	/13	255.248.0.0
1 M	20	/12	255.240.0.0
2 M	21	/11	255.224.0.0
4 M	22	/10	255.192.0.0
8 M	23	/9	255.128.0.0
16 M	24	/8	255.0.0.0
32 M	25	/7	254.0.0.0
64 M	26	/6	252.0.0.0
128 M	27	/5	248.0.0.0
256 M	28	/4	240.0.0.0
512 M	29	/3	224.0.0.0
1024 M	30	/2	192.0.0.0
2048 M	31	/1	128.0.0.0
4096 M	32	/0	0.0.0.0

$K = 1.024 \bullet M = 1.048.576$

Contact Registration Services:
hostmaster@ripe.net • lir-help@ripe.net

www.ripe.net

Depois de achar a máscara correspondente, o próximo passo é determinar o tamanho das subredes, que é basicamente o número de salto.

Para isso, você precisa usar a fórmula:

$$256 - n = Salto$$

Onde n = último octeto de rede da máscara que você achou

O número de salto pode ser entendido como a quantidade de hosts que cada uma das suas subredes vai ter. Ele vai ser usado para definir cada subrede de forma exata.

- ▼ Exemplo: calculando o salto para 8 subredes numa rede de classe C

192.168.1.0 → Endereço da rede
255.255.255.0 (/24) → Máscara de subrede padrão
8 → Quantidade de subredes necessárias

$/27 = 255.255.255.\textcolor{red}{224}$ → CIDR das subredes em padrão
 $256 - \textcolor{red}{224} = 32$ → Cálculo do salto
32 → Número do salto

3 - Escrevendo as subredes

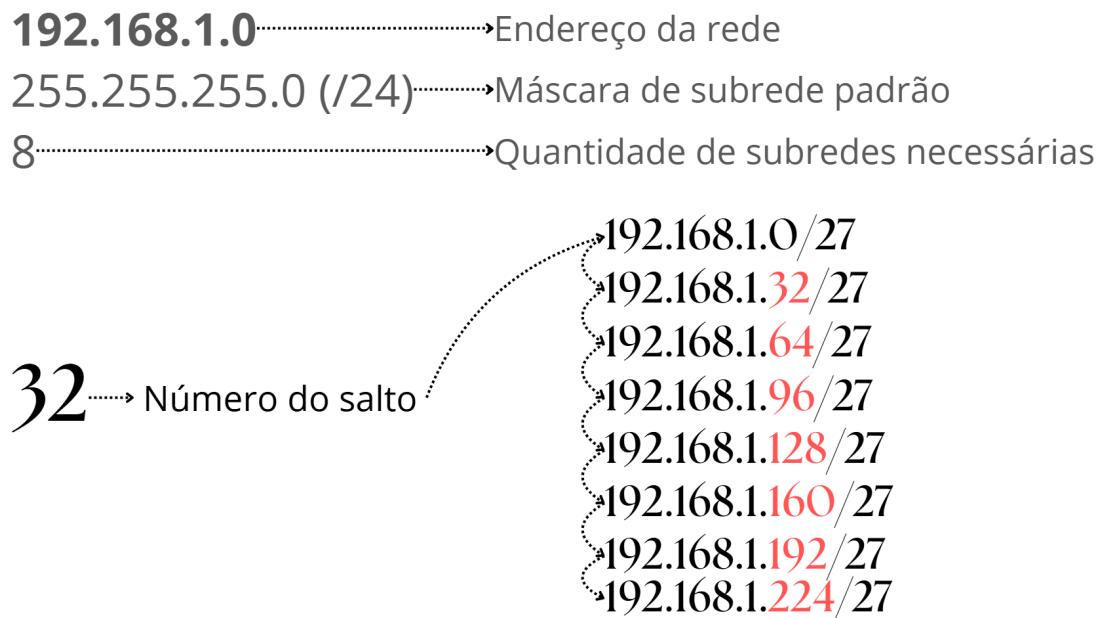
O número de salto será usado para escrever o endereço IP de cada subrede.

Algumas vezes os IPs das subredes que você vai escrever vão parecer IPs de host porque não terminarão em zero. Mas se você lembrar qual é o prefixo das subredes, você vai entender que os IPs de host vão estar entre esses IPs de subrede.

Basicamente, você pega o endereço IP da sua rede (terminado em 0) e adiciona o número de salto até que você defina a quantidade de subredes que você queria.

O salto deve ser adicionado no último octeto de rede, considerando as novas máscaras das subredes.

- ▼ Exemplo: escrevendo as 8 subredes de uma rede classe C



Dispositivos de Rede

Podemos entender as redes de computadores entre parte lógica ou virtual e parte física, e na parte física das redes existem muitos dispositivos além dos computadores e celulares.

Uma enorme gama de dispositivos eletrônicos podem estar conectados a uma rede, e dentre eles precisamos destacar aqueles dedicados à própria rede.

Switch/Hub

Esse tipo de dispositivo é chamado de “concentrador” porque possui muitas portas RJ45 nas quais se conectam outros dispositivos.

A topologia em estrela geralmente usa switches como dispositivo central.

A função de um switch é permitir a comunicação entre os dispositivos da rede de forma centralizada, ou seja, a rede só cai se o switch falhar.



Hub de 8 portas

Switch de 8 portas

O hub é semelhante ao switch, uma espécie de versão mais antiga e limitada. A diferença é:

- **Hub:** também chamado de terminal burro, tem a mesma função do switch, mas as mensagens precisam caminhar de porta em porta até achar o seu host destinatário.
- **Switch:** possui tabelamento de rota (usa o endereço MAC dos hosts), o qual permite que uma mensagem enviada de um host seja diretamente enviada ao seu destinatário, ou seja, a velocidade da comunicação é maior

Além disso, existem dois tipos de switches quanto ao gerenciamento:

- Switches simples apenas trocam informações entre os hosts
- Switches gerenciáveis permitem mais opções de manipulação da rede e por isso são mais caros

Roteador

Dispositivo de rede que pode servir como um switch, mas sua principal função é conectar a sua rede à Internet oferecida por uma provedora.

Um roteador comum consegue suportar:

- 4 dispositivos via cabo

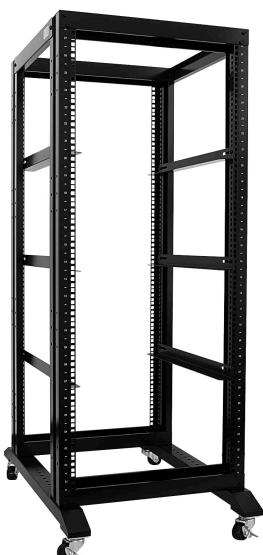
- 32 dispositivos via wireless



Roteador D-Link

Rack

Compartimento grande feito para guardar e organizar centros de cabeamento como servidores, switches e roteadores.



Rack

Em suas laterais existem furos para fixar os dispositivos. Cada 3 furos em sequência é considerado uma medida de 1U, que é uma unidade de espaço de servidor.

Ou seja, cada servidor tem um tamanho medido em Us que deve ser considerado no rack.

Para fixar os dispositivos nos furos se utiliza uma espécie de parafuso chamado porca gaiola.

Keystone



Keystone

Equipamento que conecta um cabo de rede através de uma porta RJ45 fêmea.

Pode ser encaixado em placas de parede e patch painels.

Usa um cabo chamado patch cable ou patch cord e pode conectar qualquer dispositivo com cabos RJ45.

Geralmente é usado para ligar dispositivos como antenas, câmeras, sensores e outros mais comuns.

Patch painel (dados)

Equipamento que conecta os cabos que vêm da keystone em várias portas traseiras apenas para organizar o cabeamento. Sua parte frontal permite conexão com dispositivos na parte frontal de um rack, por exemplo, que é onde geralmente os patch painels são usados.



Patch painel

Organizador de cabo

Chapa de metal que organiza os cabos no interior do rack, evitando emaranhados e facilitando a manutenção da rede.

Pode ser composto de várias formas como anéis, calhas, braçadeiras e canaletas. Podem ainda ser verticais ou horizontais.

Basicamente agrupa os cabos para evitar confusões e facilita a identificação dos mesmos.



Organizador de cabos para rack

Voice painel (telefonia)

Versão do patch painel para telefonia, ou seja, usa conectores RJ11 ao invés dos RJ45.

Basicamente recebe um ponto de rede de telefone na parte traseira e na parte frontal liga esses pontos a uma central telefônica.



Voice painel

Central PABX

Dispositivo de telefonia com placas que transformam conexões de um tronco telefônico em vários ramais internos, facilitando a comunicação dentro da telefônica com a rede externa.



Central PABX

Basicamente é um sistema que direciona chamadas à empresa de forma automática e permite chamadas internas sem usar linhas externas, ou seja, facilita o gerenciamento da telefônica.

Só pode ser acessado remotamente por linha de comando.

Nobreak

Dispositivo que oferece energia para computadores em caso de quedas de forma contínua, ou seja, evitando o desligamento brusco e a consequente possível perda de dados.

Quando a energia cai, o nobreak alterna o canal de energia para suas baterias. Ele possui um tempo e uma voltagem máximas que consegue oferecer ao dispositivo.

Sua parte traseira tem conectores fêmea para cabos específicos que conectam o computador.



Nobreak

O nobreak é basicamente um mini-gerador com baterias. Ele é muito importante em empresas que não podem ser interrompidas pela falta de energia, como hospitais.

Filtro de linha

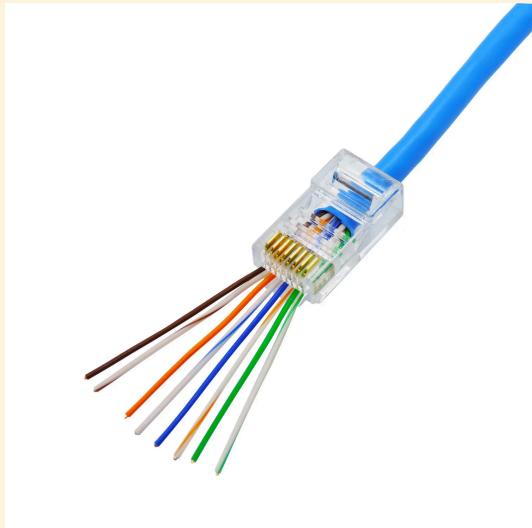
Estabilizador

Cabeamento

Conectores

RJ45

Usados para cabo UTP ou par-trançado



RJ45 macho



RJ45 fêmea (keystone)

BNC

Usados para cabo coaxial



BNC macho



BNC fêmea

ST

Usados para fibra óptica



Cabos

Coaxial

Composto por um fio de cobre revestido de isolante e blindagem.

É resistente mas sua velocidade de transmissão é baixa.

Não é utilizado atualmente. Antigamente, era comum em topologias de barramento.

Fibra óptica

Composto por duas camadas de vidro ou plástico de alta pureza por onde a luz viaja e mais duas camadas protetoras.

É o cabo mais veloz de todos em questão de transmissão de dados.

Par-trançado ou UTP

Composto por 4 pares de fio de cobre isolados com plástico e, todos juntos, protegidos por outra camada externa.

Dividido em 8 categorias de velocidade, cada uma com seu próprio padrão, frequência e taxa de transferência (e preço)

Dos 8 fios, apenas 4 (1,2,3 e 6) são usados efetivamente para dados. O restante é para telefonia.

Categorias do cabo UTP	Taxa de transmissão (MHZ)	Velocidade
cat 5e	100	100 Mbps
cat 6	250	1 Gbps
cat 6a	500	10 Gbps
cat 7	600	10/40 Gbps
cat 8	2000	40 Gbps

*A distância máxima recomendada pelos fabricantes é de 100 metros de cabo para todas as categorias

Patch cable ou patch cord

Cabo de rede que conecta um dispositivo a uma keystone (conector fêmea do RJ45 que geralmente se encontra nas paredes como as tomadas)

Geralmente é usado para ligar dispositivos como antenas, câmeras, sensores e outros mais comuns.

Existe uma versão do patch cable para fibra óptica, pela qual é possível conectar uma residência à provedora de Internet.

Sua manutenção exige alicate putdown.

Kit de crimpagem

Fluxo de dados

Em um switch, os dados podem ser transmitidos de maneiras diferentes quanto ao sentido e a simultaneidade:

- SIMPLEX: transmissão ocorre em 1 sentido, ou seja, existe apenas um emissor e um receptor.
 - Exemplo: rádios e televisões
- HALF-DUPLEX: transmissão ocorre em 2 sentidos alternadamente.
 - Exemplo: comunicação entre computadores
- FULL-DUPLEX: transmissão ocorre em 2 sentidos simultaneamente.
 - Exemplo: serviço de telefonia, redes de computadores, ...

Windows Server 2022

É um sistema operacional da Microsoft dedicado para gerenciamento de servidores. Algumas de suas versões ao longo do tempo (junto com os OSs

para estação de trabalho)

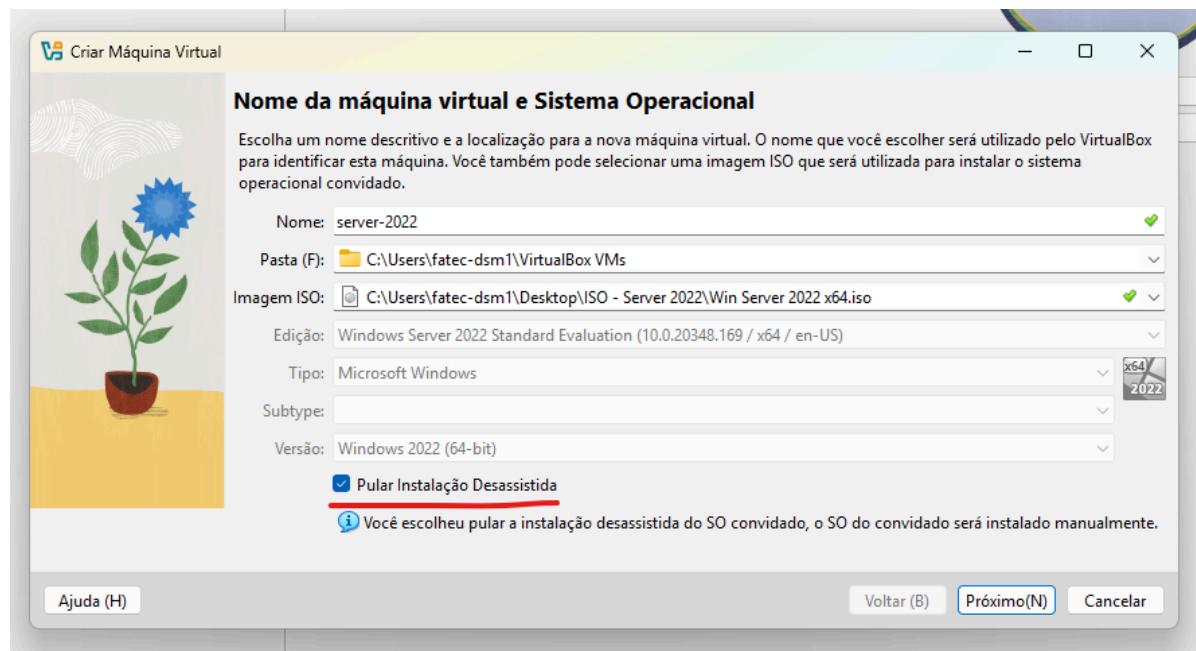
- Windowsnt 3.5 e Windows Workstation 3.5
-

Instalação na máquina física

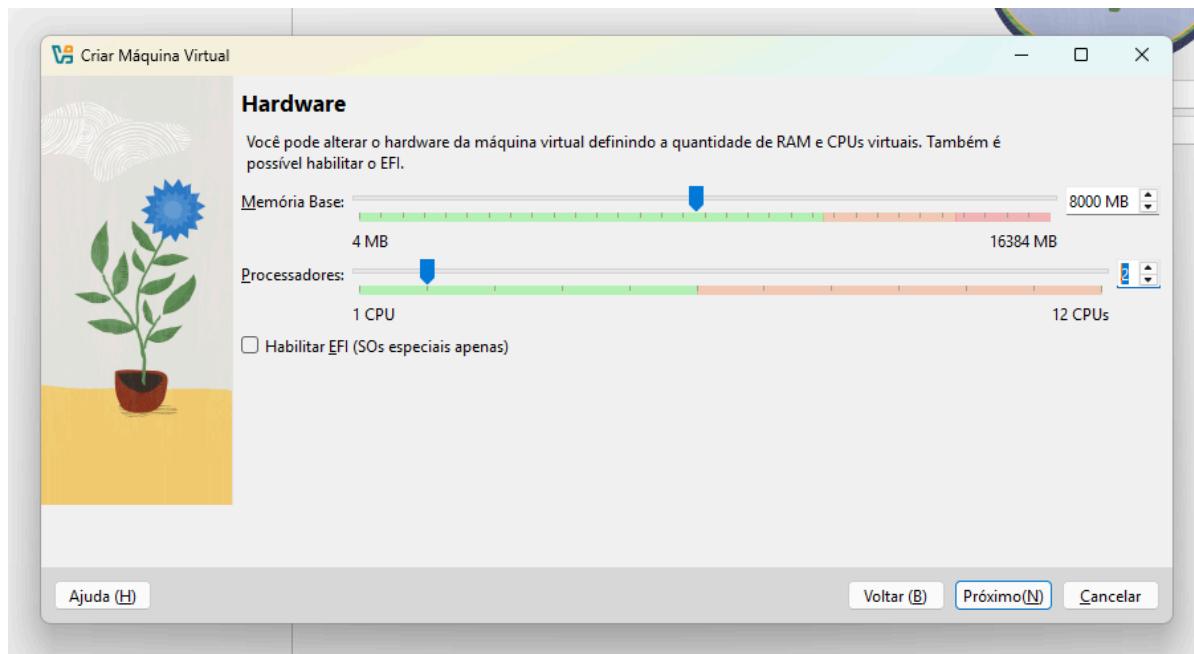
Em aula, vamos programar boot do Windows Server 2022 em um pendrive, para conseguir abrir o OS nos computadores físicos.

Instalação na máquina virtual

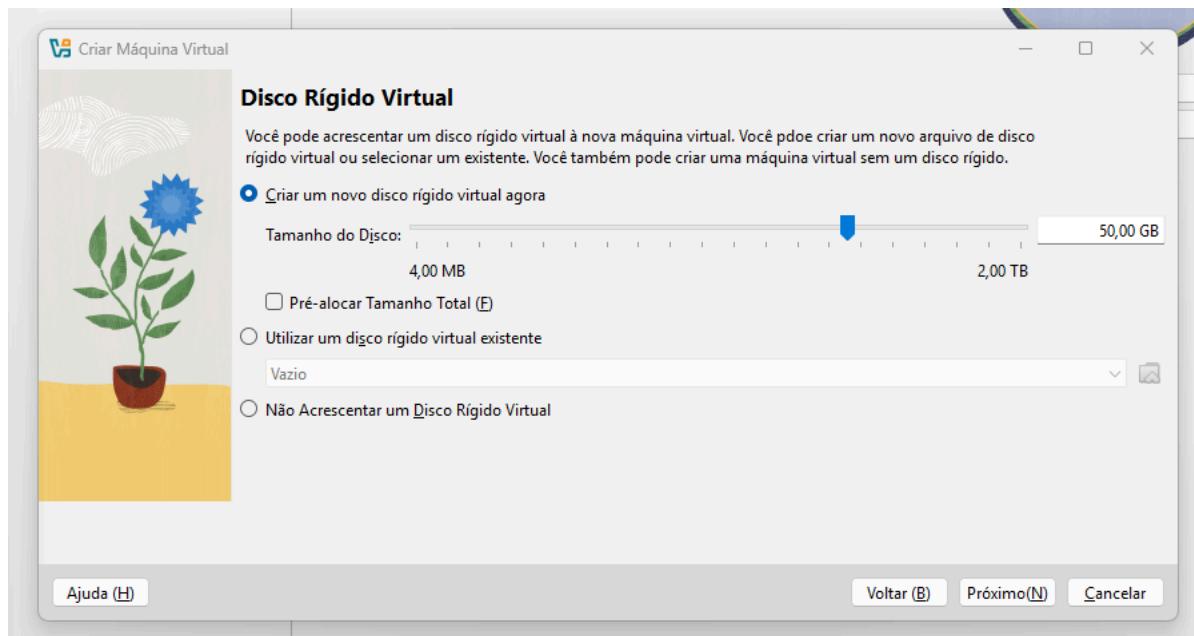
Em aula, usamos o Oracle Virtual Box para criar a máquina virtual onde será instalado o Windows Server 2022.



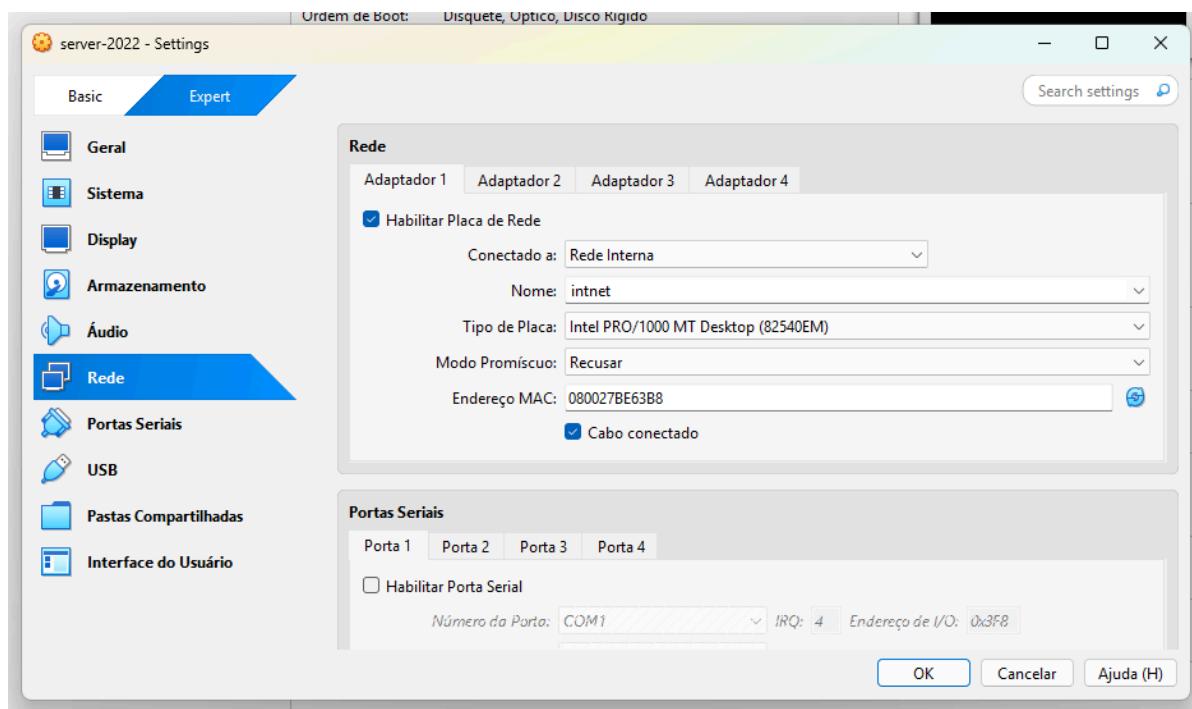
- Nome: é apenas um nome descritivo para a máquina virtual dentro do Oracle Virtual Box
- Pasta: onde a máquina virtual se localiza no computador
- Imagem ISO: selecione o arquivo ISO com o sistema operacional
- Pular Instalação Desassistida: é melhor ativar para evitar problemas na instalação do Windows Server 2022



- Memória Base: considerando os 16GB de RAM dos computadores da fatec, dedicaremos 8GB para quando formos usar a máquina virtual
- Processadores: considerando os computadores da fatec, vamos usar 2 CPUs



- Tamanho do Disco: considerando os computadores da fatec,



- Configurações>Rede>Expert: troque a conexão da placa de rede de NAT para Rede Interna

Sobre as conexões da placa de rede:

- **Rede NAT**: mascara o IP da rede física para conectar a máquina física à Internet dentro da máquina virtual, usando uma outra classe mascarada para navegar na internet.
- **Rede Interna**: não conecta nem na rede física nem na rede virtual, “cria” uma máquina para usar uma rede isolada.
- **Modo Bridge**: placa de rede da máquina virtual junto com a rede física. Busca o DHCP da rede física, podendo causar problemas com máscara de subrede. Faz a ponte entre a rede virtual e física.

Após esse processo, você pode iniciar a máquina virtual e a instalação do Windows Server 2022. As próximas configurações são de língua, partição, instalação e usuário com senha.

Login no Windows Server 2022

CTRL direito + DELETE : abre tela de usuário e senha da máquina virtual
(usar CTRL esquerdo + ALT +DELETE tenta trocar o da máquina física)

Senha da máquina virtual da Fatec

fatec@1234

(por padrão, cria-se um usuário chamado Administrador)

Toda vez que você loga no Windows Server, automaticamente se abre um software chamado **Server Manager**. É um programa dedicado ao gerenciamento do servidor, o qual possui todas as configurações que você precisa para mexer no servidor virtual.

Existem três passos fundamentais antes de transformar a máquina virtual em um servidor:

1. Alterar o nome da máquina virtual em si.

Para isso, vá nas configurações do windows e renomeie o dispositivo. Você vai precisar reiniciar a máquina virtual.

2. Fixar o IP da máquina virtual.

Use Windows+R para abrir o Executar e digite ncpa.cpl para abrir diretamente as configurações da placa de rede. Abra as propriedades da placa e clique duas vezes no texto “Internet Protocol V4 (TCP/IPv4)” para definir manualmente o IP.

Nos computadores da fatec usaremos:

Endereço IP: 10.12.27.200

Máscara de subrede: 255.255.255.0 (/24)

Gateway padrão: 10.12.27.1

Servidor DNS preferencial: 208.67.222.222

Servidor DNS alternativo: 208.67.220.220

O gateway é caminho de comunicação entre a rede interna e a rede externa.

O DNS é um servidor que converte os endereços IP dos websites para nomes de domínio e vice-versa. Os nomes de domínio são usados nas barras de pesquisa dos navegadores para encontrar os websites.

Os servidores DNS mais utilizados são os da Google: 8.8.8.8 (primário) e 4.4.4.4 (secundário)

Existe um outro provedor DNS muito usado chamado Open DNS:
208.67.222.222 (primário) e 208.67.220.220 (secundário)

3. Desativar o firewall da máquina virtual.

Entre no painel de controle do windows, acesse o Windows Defender Firewall e desative-o (nas opções laterais) tanto para a rede privada quanto para redes públicas ou convidados.

CMD: ipconfig /all

Usar ipconfig com parâmetro all mostra todas as configurações da sua placa de rede, sem exceções

Mac Adress: endereço físico da placa de rede, 8 conjuntos de dígitos separados por hífen

Após todos esses procedimentos, a máquina virtual está preparada para se tornar um servidor. Agora precisamos instalar três serviços pelo Server Manager para, definitivamente, transformar a máquina num servidor.

Dentro do Server Manager, selecione Manage no menu superior direito e, após, Add Roles and Features.

Na lista dos serviços, os três obrigatórios para servidores são:

- Active Directory Domain Services
- DHCP Server
- DNS Server

Para cada serviço adicionado, abrirá uma janela perguntando se você quer aplicar acessórios - aceitaremos todos.

Você pode avançar até a etapa de confirmação e instalar os serviços.

Após a instalação, você precisa reiniciar a máquina virtual.

Ao entrar novamente no Server Manager, os serviços instalados serão carregados e disponibilizados no menu lateral.

*DHCP (Dynamic Host Configuration Protocol)

Desligamento da máquina virtual

Prefira desligar pela interface do sistema operacional, e não fechando a janela da máquina virtual. Esse último método pode corromper os arquivos da virtualização.