

# TECNOLOGIA DA INFORMAÇÃO

REDES E CABEAMENTO



# CONTEÚDO PROGRAMÁTICO

## CAPÍTULO 1

INTRODUÇÃO A REDES _____	05
SURGIMENTO DA PRIMEIRA REDE (ARPANET) _____	05
REDE PAN _____	07
REDE LAN _____	07
REDE CAN _____	08
REDE RAN _____	09
REDE MAN _____	09
REDE WMAN _____	09
REDE WAN _____	10
REDE WWAN _____	10
HIERARQUIA DE REDES: REDE PONTO A PONTO _____	11
HIERARQUIA DE REDES: CLIENTE – SERVIDOR SERVIDORES _____	11

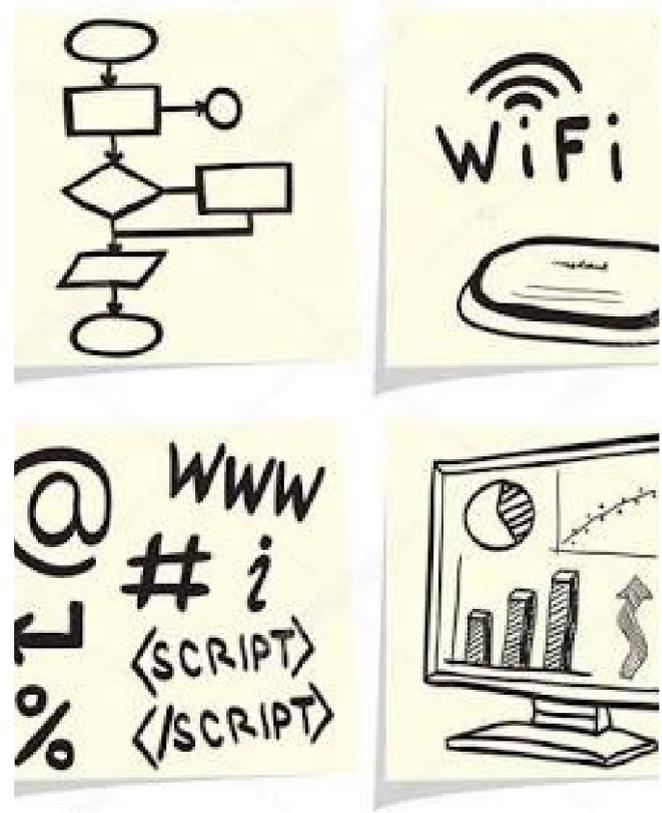
## CAPÍTULO 2

SERVIDOR DE ARQUIVOS E DOMÍNIO _____	13
SERVIDOR DE IMPRESSÃO _____	13
SERVIDOR DE E-MAIL _____	14
SERVIDOR DE BACKUP _____	14
SERVIDOR DE WEB _____	15
SERVIDOR DE DNS _____	15
SERVIDOR DE PROXY _____	15
SERVIDOR DE FTP _____	16
SERVIDOR DE ACESSO REMOTO _____	16
SERVIDOR DE VIRTUALIZAÇÃO _____	16
SERVIDOR DE DOMÍNIO _____	17

## CAPÍTULO 3

SISTEMAS OPERACIONAIS PARA SERVIDORES _____	18
DISPOSITIVOS DE REDES: HOST _____	19
DISPOSITIVOS DE REDES: INTERFACE _____	19
DISPOSITIVOS DE REDES: SWITCH _____	19
DISPOSITIVOS DE REDES: GATEWAY _____	20
DISPOSITIVOS DE REDES: ROTEADORES _____	20
DISPOSITIVOS DE REDES: PROTOCOLO TCP/IP _____	20
DISPOSITIVOS DE REDES: MAC ADDRESS _____	20
DISPOSITIVOS DE REDES: PORTAS _____	21

# CONTEÚDO PROGRAMÁTICO



## CAPÍTULO 4

TOPOLOGIA DE REDES	22
TOPOLOGIA FÍSICA	22
TOPOLOGIA LÓGICA	22
REDE BARRAMENTO	22
REDE ANEL	23
REDE ESTRELA	23
REDE MALHA	24
REDE ÁRVORE	25
REDE HÍBRIDA	25
CONCEITOS DE COMUNICAÇÃO	26
ENDEREÇO IP	26
CLASSES DE IP	27
MÁSCARA DE REDE	27

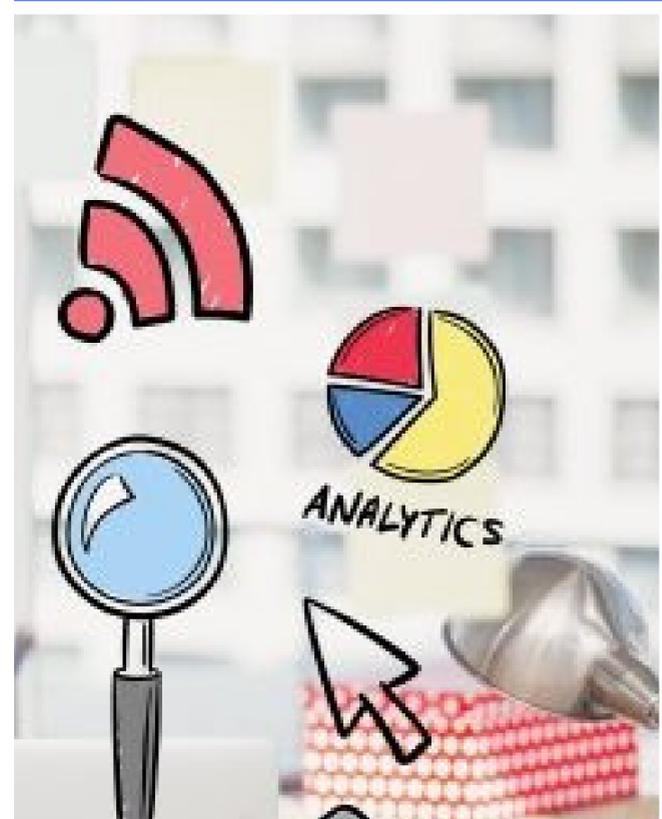
## CAPÍTULO 5

SISTEMA BINÁRIO	27
SUB-REDES	29
CONOTAÇÃO CDRI	31
UNIDADES DE MEDIDA	32



## CAPÍTULO 6

CABEAMENTO ESTRUTURADO	33
MEIOS DE COMUNICAÇÃO DE DADOS	33
PAR TRANÇADO	33
TIPOS DE CABOS	34
ATENUAÇÃO	34
ARQUITETURA DE REDES	35
TIPOS DE ARQUITETURAS DE REDES	35
CATEGORIAS DE CABOS	36

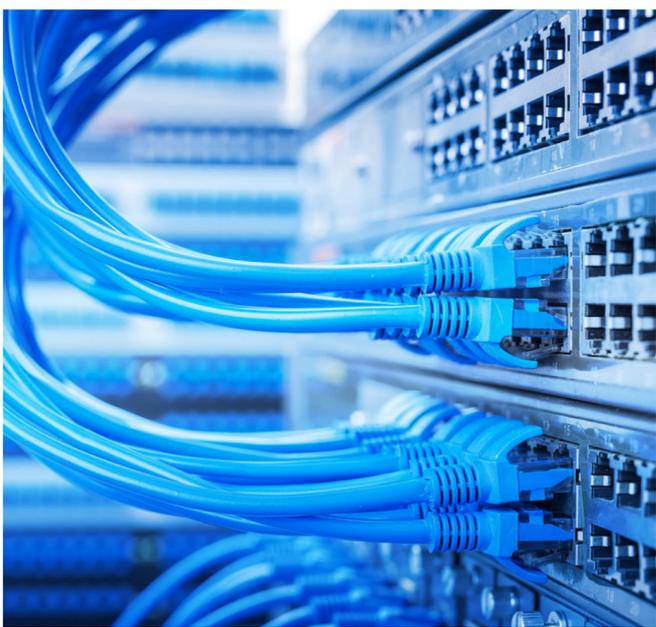


# INTRODUÇÃO A REDES

## O que é uma Rede de computador?

Uma Rede de computadores é formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e compartilhar recursos, interligados por um subsistema de comunicação, ou seja, é quando há pelo menos dois ou mais computadores, e outros dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos, estes podem ser do tipo: dados, impressoras, mensagens (e-mails), entre outros. Uma rede de computadores ou rede de dados é uma rede de telecomunicações digital que permite que compartilhem recursos. Em uma rede de computadores, os dispositivos de computação em rede trocam dados entre si usando um link de dados. As conexões podem ser estabelecidas usando mídia de cabo ou mídia sem fio.

Os dispositivos que originam uma rede de computadores que roteiam e terminam os dados, são denominados de “nós” de rede (ponto de conexão). Os “nós” podem incluir hosts, como computadores pessoais, telefones, servidores, e também hardware de rede.



Dois desses dispositivos podem ser ditos em “rede” quando um dispositivo é capaz de trocar informações com o outro dispositivo, quer eles tenham ou não uma conexão direta uns com os outros. Em suma, uma rede de computadores é formada por um conjunto de módulos processadores (MP's) capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação.

## Surgimento das Redes

Instituídas durante a década de 60, as primeiras redes de computadores tinham o propósito de trocar dados entre dois computadores. O cartão perfurado era o meio utilizado para armazenar dados, sendo que o mesmo constituía-se como uma forma demorada e trabalhosa de transportar grandes quantidades de informações.

Podemos entender que o cartão perfurado era o pai dos disquetes embora nele não ficasse armazenado dados lógicos.

Em 1969 surge a Arpanet que foi desenvolvida dentro do Pentágono. A Arpanet foi totalmente financiada pelo governo dos Estados Unidos durante o período que ficou conhecido como Guerra Fria que era uma guerra entre Estados Unidos e União Soviética. Temendo um ataque por parte da União Soviética, os Estados Unidos tinham como objetivo desenvolver uma rede de comunicação que não os deixassem vulneráveis, caso houvesse algum ataque Soviético ao Pentágono.

Para realizar o primeiro experimento com a rede foram escolhidas quatro Universidades que seriam conectadas em janeiro de 1970 na rede computacional Arpanet que ficava dentro do Pentágono. Foram a Universidade da Califórnia em Los Angeles, o Stanford Research Institute em Palo Alto, a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah. Com a evolução crescente dos meios de comunicação e as tecnologias, a década de 90 ficou caracterizada com a expansão do acesso à internet. Neste caso, redes dos mais variados tipos ganharam seu espaço no mercado. O padrão Ethernet ficou popularizado e se espalhou, sendo utilizado com frequência na construção de redes locais de computadores (Lans). Neste período, o acesso à internet através de linha discada era uma realidade comum em empresas, haja vista que era necessário um modem e uma linha telefônica, o que muitas vezes tornava-se uma solução custosa. Como solução a esta alternativa discada, surgiram as linhas de frame relay (conexão dedicada com velocidades de 64 kbits). Esse tipo de conexão facilitava o acesso à internet em computadores de uma mesma rede, pois permitia compartilhar a conexão entre os computadores da rede, além de permitir que todos estivessem permanentemente conectados.

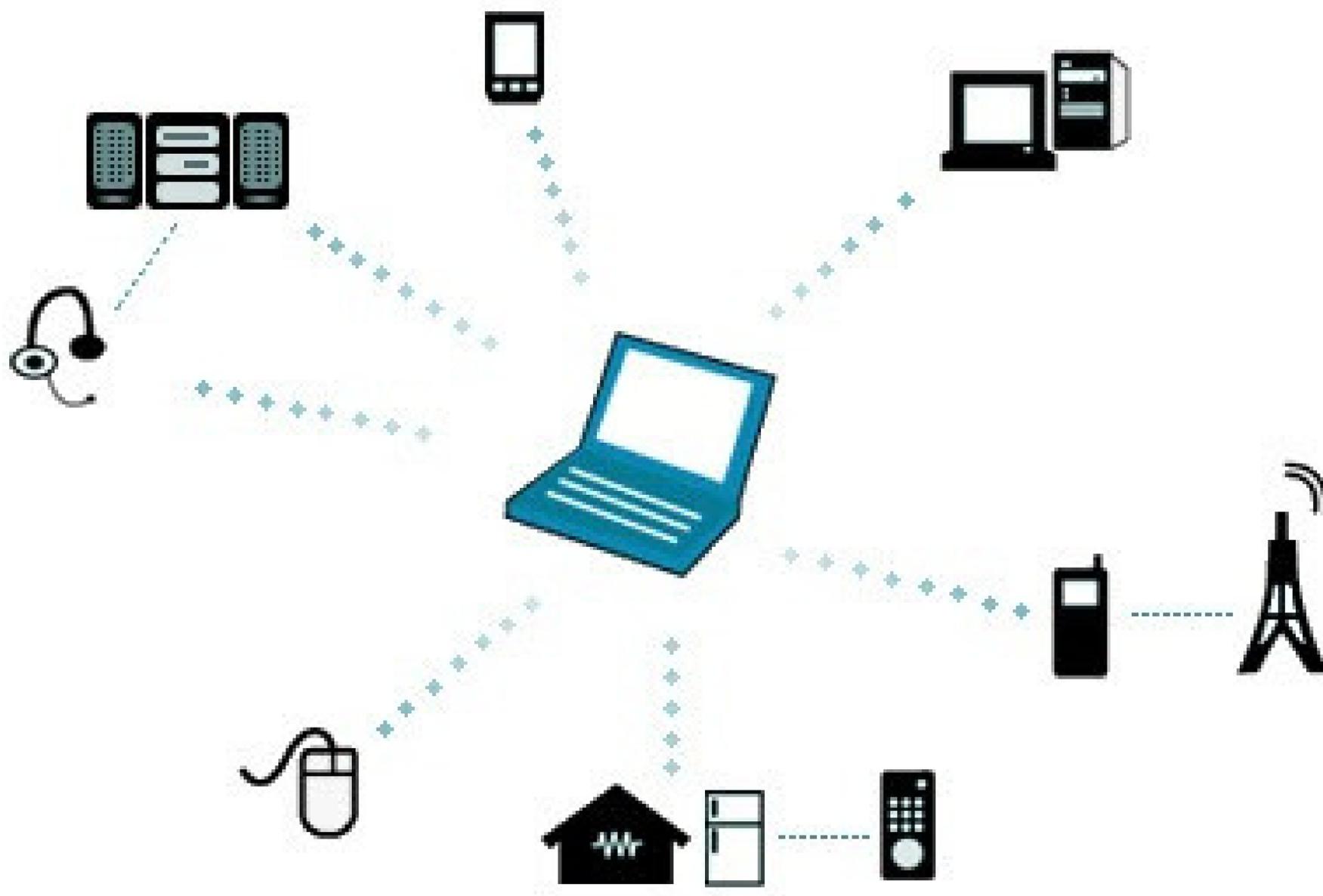
Hoje é possível construir redes através de inúmeras possibilidades: redes cabeadas (Ethernet, fibra óptica), sem-fio (rádio, Bluetooth, WiFi), entre outros. As redes de computadores apesar da evolução e crescente propagação, mantém seu objetivo primordial: Compartilhar recursos



Sistema de processamento de dados da Arpanet, desenvolvida dentro do Pentágono.



Conexão através de redes cabeadas Ethernet, comum nos dias de hoje



## PAN

Uma PAN (Personal Area Network) ou Rede de Área Pessoal, constitui-se de uma rede de computadores formada por dispositivos muito próximos uns dos outros.

Como exemplo deste tipo de rede, pode-se citar dois notebooks em uma sala trocando informações entre si e ligados a uma impressora.

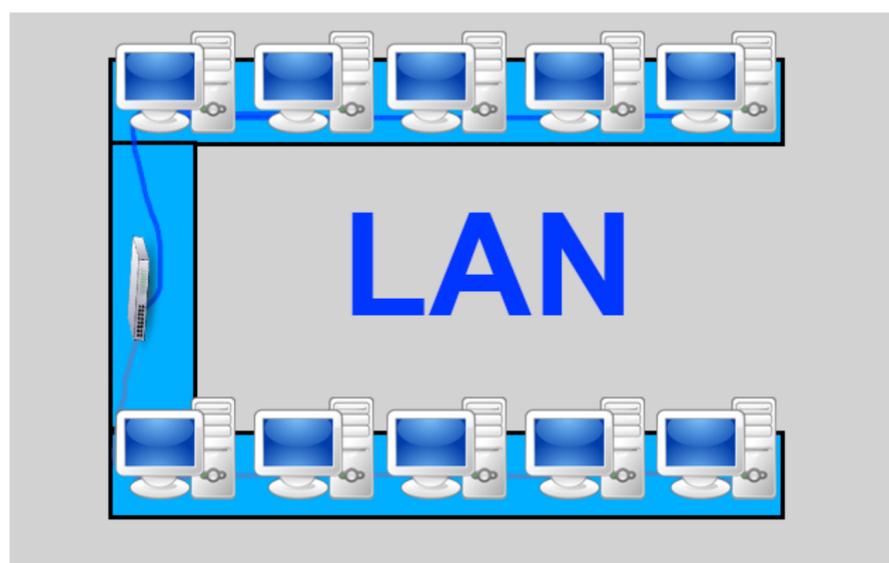
Redes formadas por dispositivos Bluetooth são exemplos de uma LAN

## LAN

Uma LAN (Local Area Network), também conhecida como rede local de computadores, corresponde a uma rede que possui uma “cobertura limitada” quanto a extensão geográfica que pode atuar.

Este tipo de rede é geralmente composto por computadores conectados entre si, através de dispositivos tecnológicos (placas de redes, switch, entre outros), possibilitando o compartilhamento de recursos e a troca de informações.

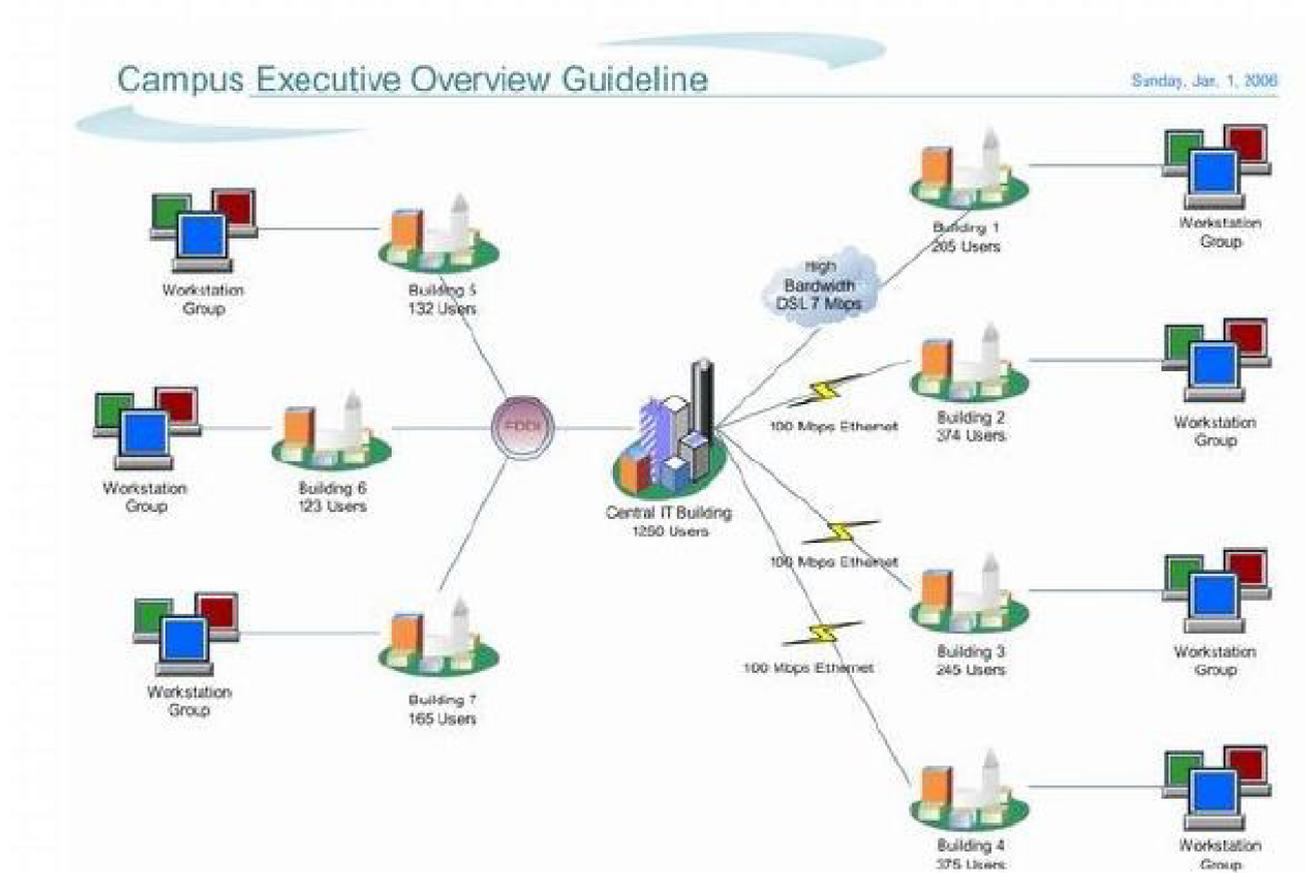
Uma rede local de computadores é utilizada com frequência para conectar computadores em rede, servidores, dispositivos eletrônicos diversos (tablets, netbooks, notebooks, etc.). Sua limitação geográfica faz com que as LAN's sejam utilizadas em casas, escritórios, escolas, empresas, entre outros meios locais.



# CAN

Uma CAN (Campus Area Network) corresponde a uma rede de computadores formada por computadores dispostos em prédios dentro de uma área enorme como um campus de Universidade.

## Comunicação de uma rede CAN



# RAN

RAN significa (Regional Área Network), também conhecida como Rede de Área Regional.

Alguns livros citam que RAN também poderia ser (Radio Área Network) que significa Rede de Área De Rádio no qual se usa torres de rádio para fazer a comunicação.

Ambos estão certos já que citam que o alcance máximo seria menor que uma área metropolitana. Um exemplo seria o grupo RBS. A Zero Hora na avenida Ipiranga que se comunica por rádio com as suas estações de rádio no morro Santa Tereza. Embora a torre de rádio tenha um alcance muito maior do que esta distância, o alcance entra a avenida Ipiranga e o Morro Santana a faz maior que uma LAN e menor que uma área metropolitana inteira. Poucos livros citam que a RAN poderia ser maior que uma área metropolitana o que também seria correto.

## MAN

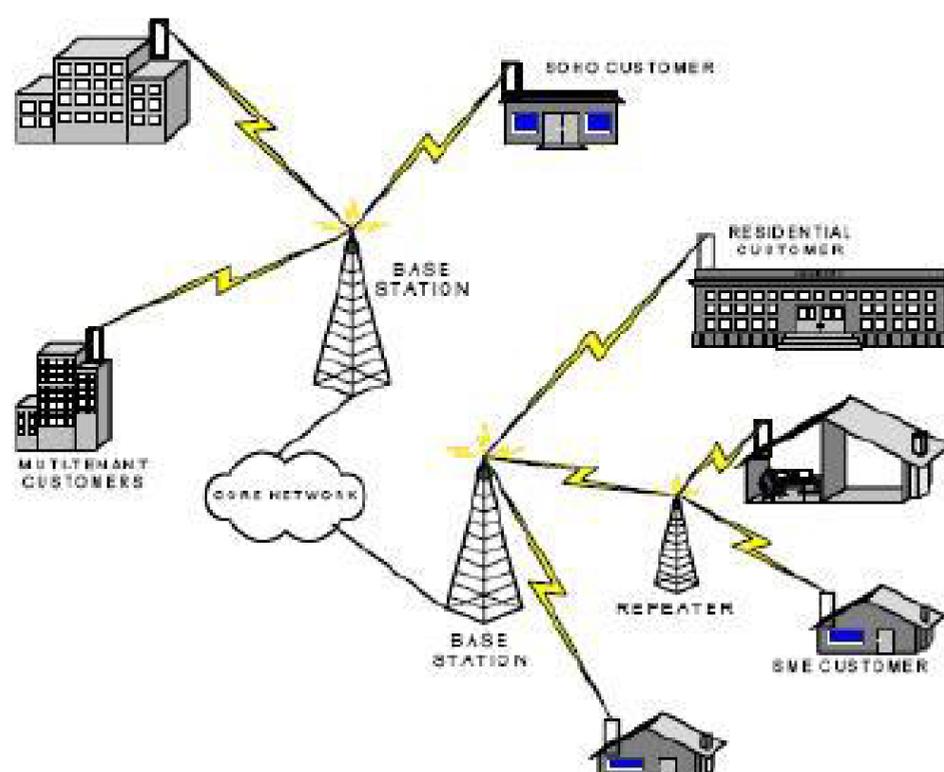
Uma MAN (Metropolitan Area Network) rede de área metropolitana, corresponde a uma rede de computadores que compreende um espaço de média dimensão (região, cidade, campus, entre outros). Geralmente uma MAN está associada a interligação de várias LAN's.

Um exemplo de MAN são as redes ISP (Internet Service Provider) que em português significa "provedor de serviço de internet". Um ISP nada mais é do que uma empresa (provedor) que fornece acesso à internet e demais serviços de um ISP como: contas de e-mail, hospedagem de sites, entre outros, mediante o pagamento de uma mensalidade ou taxa. As formas de conexão a esta rede podem ser através de uma linha telefônica (dial-up), ou uma conexão de banda larga (wireless, cabo ou DSL). As redes ISPs são exemplos clássicos de MAN.



## WMAN

Rede de área metropolitana sem-fio, destina-se principalmente a operadoras de telecomunicações.



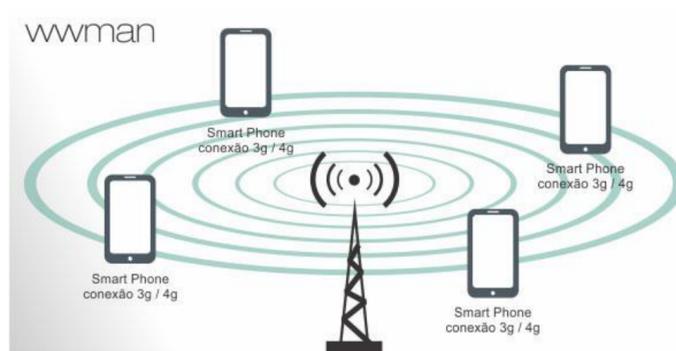
## WAN

Uma WAN (Wide Area Network) ou rede de longa distância, corresponde a uma rede de computadores que abrange uma grande área geográfica, como por exemplo um país, continente, entre outros. As WANs permitem a comunicação a longa distância, interligando redes dentro de uma grande região geográfica.



## WWAN

Rede de longa distância sem fio, são comumente utilizadas para criação de redes de transmissão celular.



## Hierarquia - Rede Ponto a Ponto

Uma rede ponto-a-ponto normalmente é utilizada em pequenas redes. Neste tipo de rede os computadores trocam informações entre si, compartilhando arquivos e recursos.

Uma rede do tipo ponto-a-ponto possui algumas características pontuais:

- É utilizada em pequenas redes;
- São de implementação fácil e de baixo custo;
- Possuem pouca segurança;
- Apresentam um sistema de cabeamento simples.

Ao citarmos uma vantagem e uma desvantagem deste tipo de rede, podemos considerar como ponto positivo o baixo custo para implementar uma rede do tipo ponto-a-ponto, onde todos os computadores podem acessar diretamente todos os demais computadores e seus recursos compartilhados. Um ponto negativo neste tipo de rede está relacionado a baixa segurança que este modelo proporciona.:



## Hierarquia - Rede Ponto a Ponto

Uma rede de computadores do tipo cliente-servidor possui um ou mais servidores, responsáveis por prover serviços de rede aos demais computadores conectados a ele que são chamados de clientes.

Cada cliente (computador que compõe este tipo de rede) que deseja acessar um determinado serviço ou recurso faz essa solicitação

ao servidor da rede, por isso o nome cliente-servidor. Esse tipo de rede surgiu de necessidade de criar uma estrutura que centralizasse o processamento em um computador central da rede (no caso o servidor, com recursos de hardware preparados para tal processamento).



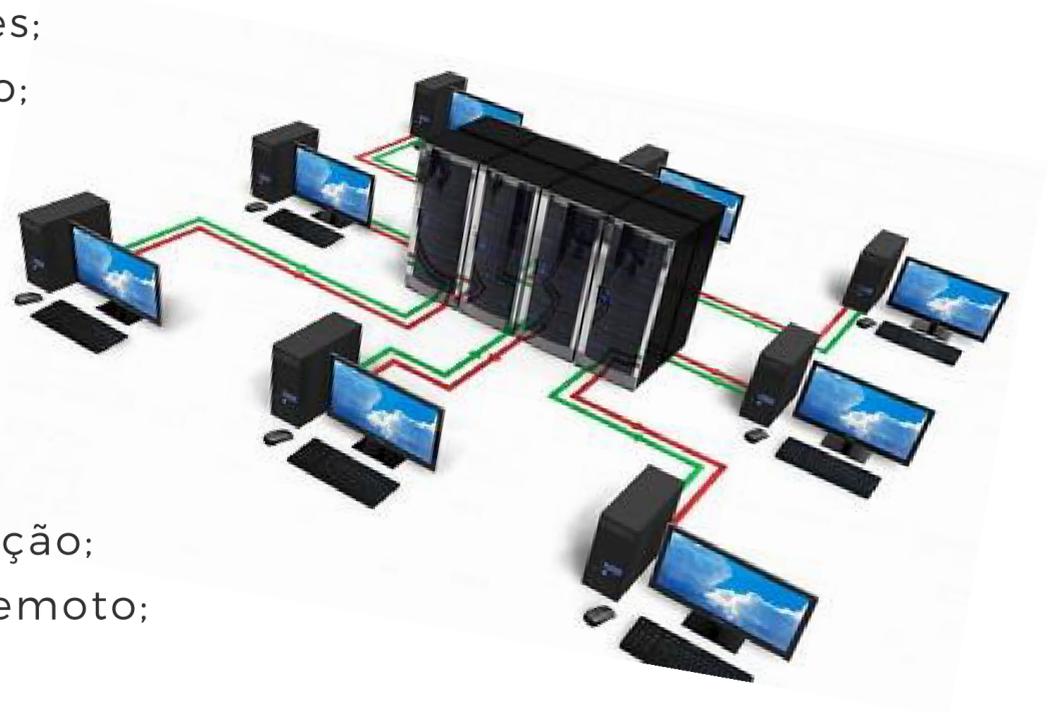
Como características deste tipo de rede podemos citar:

- Maior custo e implementação mais complexa que uma rede do tipo ponto-a-ponto;
- Existência de pelo menos um servidor da rede;
- Redes do tipo cliente-servidor, apresentam uma estrutura de segurança melhorada, pois as informações encontram-se centralizadas no servidor, o que facilita o controle e o gerenciamento dos mesmos;
- Neste tipo de rede não há tolerância a falhas (como existe em um sistema descentralizado) haja vista um único sistema centralizado de informações (servidor);
- Um servidor de rede é um computador projetado (hardware) para suportar a execução de várias tarefas que exigem bastante do hardware (como disco rígido e processador), diferentemente de uma estação de trabalho (cliente), que não possui características para realizar o trabalho de um servidor (quando falamos puramente do hardware necessário a um computador servidor).

# Servidores

Um servidor desempenha diversas tarefas tais como:

- Servidor de Arquivos;
- Servidor de Domínio (Controlador de Domínio);
- Servidor de Aplicações;
- Servidor de Impressão;
- Servidor de FTP;
- Servidor Proxy;
- Servidor DNS;
- Servidor Web;
- Servidor de E-mail;
- Servidor de Backup;
- Servidor de Virtualização;
- Servidor de Acesso Remoto;
- Servidor DHCP.



Para o bom funcionamento de um servidor, que irá trabalhar com grande número de requisições, é necessário que o mesmo possua hardwares para este fim, e não hardware de Desktop.

É importante salientar aqui que o servidor deve ser um computador preparado para exercer esta função, tanto no hardware com que é composto quanto ao software que é empregado no mesmo, ou seja, um servidor deve ter um hardware específico para suportar as atividades de servidor e deve também conter um sistema operacional que forneça à máquina capacidade de prover serviços específicos de servidores.

# SERVIDORES

### Servidor de Arquivos e Domínios

Servidor de arquivo e domínios tem a função de armazenar os dados que são compartilhados entre os diferentes usuários que compõe uma rede de computadores. Entre estes dados estão o armazenamento de arquivos (texto, planilhas e gráficos).

Os programas que manipulam os arquivos são instalados e executados individualmente em cada uma das máquinas, não no servidor, que neste caso é responsável por gerenciar eventuais acessos simultâneos.



### Servidor de Impressão

Servidor de impressão processa os pedidos de impressão solicitados pelos usuários da rede e gerencia a ordem de impressão em caso de pedidos simultâneos (prioridades podem ser implementadas, caso necessário). Cotas de impressão podem ser implementadas como forma de limitar a quantidade de páginas impressas por usuários.



## Servidor de Aplicação

Servidor de Aplicação é responsável por executar aplicações cliente/servidor, como por exemplo, um banco de dados de um sistema de gestão.

Os clientes enviam pedidos ao servidor como uma pesquisa, e o servidor processa as pesquisas e devolve os dados para serem exibidos em aplicações cliente.

A vantagem deste tipo de serviço é que vários usuários podem utilizar uma aplicação ao mesmo tempo.

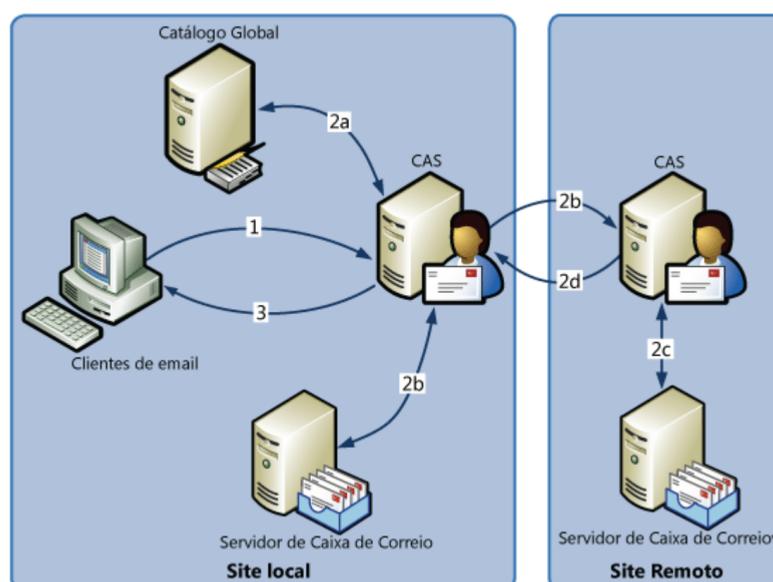
Exemplo: sistema de gestão de call center.

## Servidor de Aplicação



## Servidor de E-mail

Servidor de e-mail é responsável pelo armazenamento e processamento de envio e recebimento de mensagens eletrônicas.



## Servidor de Backup

Servidor de backup é responsável por armazenar e executar a atualização de cópias de segurança dos dados no servidor.



## Servidor WEB

Também conhecido como servidor de hospedagem, armazena as páginas dos usuários que ficarão disponíveis na internet, para acesso pelos clientes via browsers.

Vale salientar que muitas vezes um servidor WEB está ligado a outros serviços do servidor como banco de dados por exemplo.



## Servidor DNS

Estes servidores fazem a tradução dos endereços digitados nas URLs dos browsers em endereços IP e vice-versa.

Este servidor exerce uma tarefa de extrema relevância para as redes de computadores, pois sem eles, cada vez que acessássemos um site, por exemplo, teríamos que digitar seu endereço IP correspondente.

## Servidor Proxy

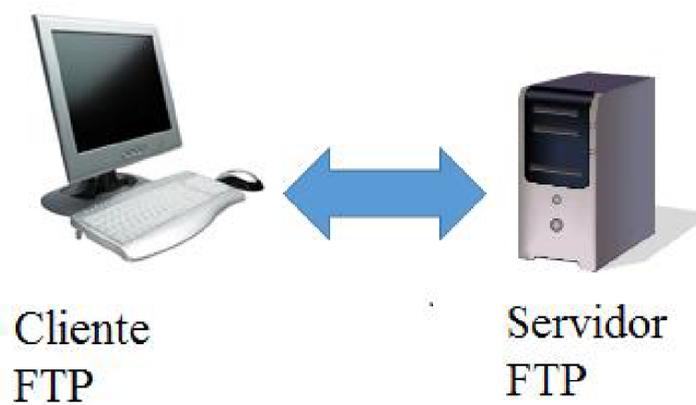
Servidor proxy pode exercer diferentes tipos de serviços a uma rede de computadores. Em geral um proxy está associado a cache, que nada mais é do que o armazenamento local no servidor das páginas da internet mais visitadas. Dessa forma, cada vez que um novo usuário acessar um site já acessado anteriormente, o servidor retornará para este usuário a página armazenada no cache local do servidor, o que se torna muito mais rápido do que abrir uma nova conexão e buscar os dados novamente em um servidor externo. Um dos exemplos mais positivos de se ter um servidor proxy é que se a internet local ou a página solicitada estiver com problemas de conexão, a página se estiver armazenada localmente no servidor proxy, abrirá sem problemas facilitando a navegação.



## Servidor FTP

Também conhecido como servidor de hospedagem, armazena as páginas dos usuários que ficarão disponíveis na internet, para acesso pelos clientes via browsers.

Vale salientar que muitas vezes um servidor WEB está ligado a outros serviços do servidor como banco de dados por exemplo.



## Servidor de Virtualização

Bastante utilizado atualmente como forma de reduzir o número de servidores físicos em uma rede de computadores, um servidor de virtualização permite a criação de várias máquinas virtuais em um mesmo computador servidor.

Assim, pode-se ter em uma mesma rede, diferentes servidores separados, em um mesmo equipamento, fazendo com que dessa maneira, tenha-se uma maior eficiência em termos de energia despendida a estes serviços sendo executados em um mesmo local físico.

Um exemplo seria ter um servidor de domínio Windows com uma VM (Virtual Machine) máquina virtual operando Linux como servidor de câmeras.



## Servidor de Acesso Remoto

Bastante utilizado atualmente como forma de reduzir o número de servidores físicos em uma rede de computadores, um servidor de virtualização permite a criação de várias máquinas virtuais em um mesmo computador servidor.

Assim, pode-se ter em uma mesma rede, diferentes servidores separados, em um mesmo equipamento, fazendo com que dessa maneira, tenha-se uma maior eficiência em termos de energia despendida a estes serviços sendo executados em um mesmo local físico.

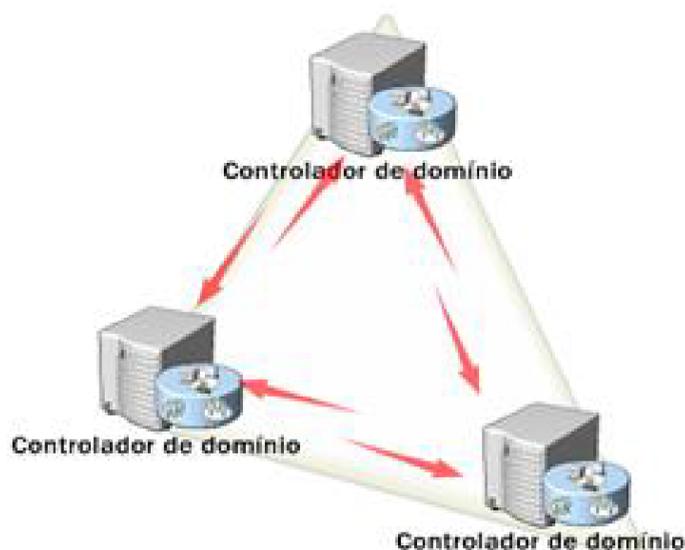
Um exemplo seria ter um servidor de domínio Windows com uma VM (Virtual Machine) máquina virtual operando Linux como servidor de câmeras.



## Servidor de Domínio

Servidores de Domínio, também conhecidos como Controladores de Domínio, são servidores que trabalham com requisições de autenticação e permissões.

O termo Domínio, em redes, foi um conceito introduzido no Windows NT. No Servidor de Domínio o Administrador de Redes cria as contas dos usuários que acessarão os recursos de redes e dependendo das permissões de cada usuário, eles terão ou não restrições de acesso a pastas ou determinados dispositivos de rede.



### Servidor Firewall

Servidor Firewall tem como objetivo ser um sistema de segurança de rede que monitora e controla o tráfego de rede de entrada e saída com base em regras de segurança predeterminadas.

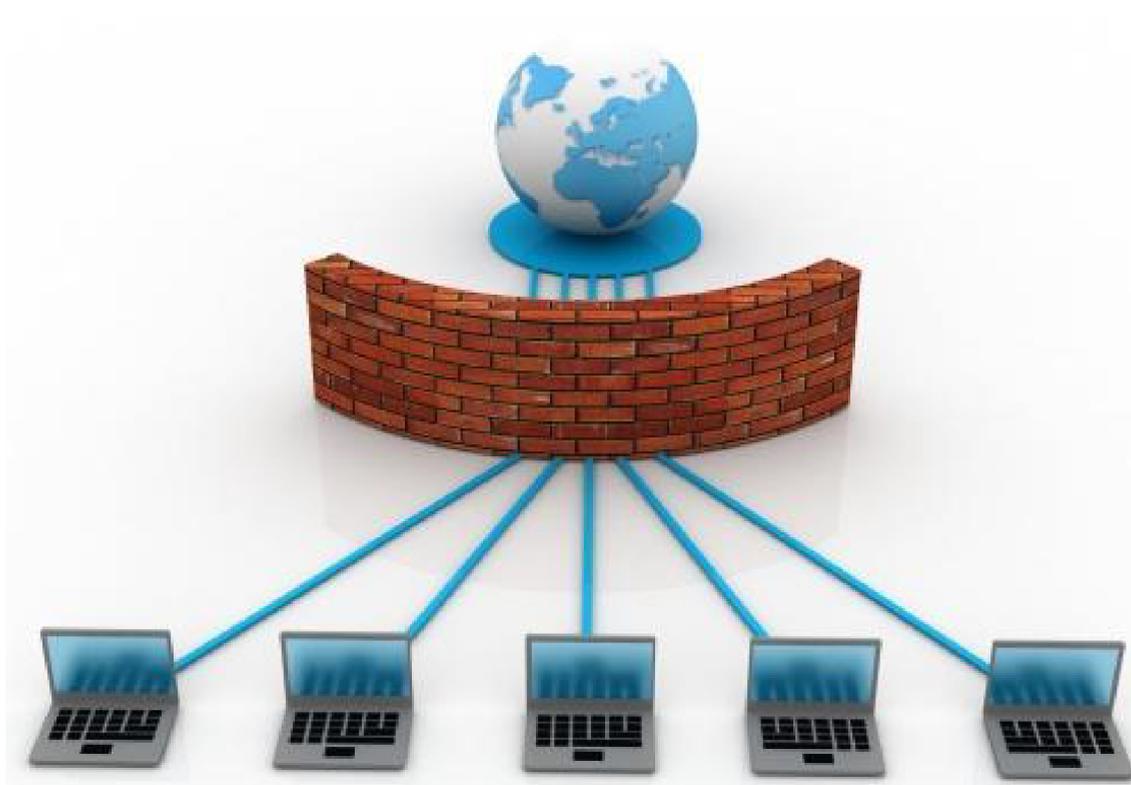
Um firewall tipicamente estabelece uma barreira entre uma rede interna confiável e segura e outra rede externa, como a Internet, que é assumida como não segura ou confiável.

Firewalls são muitas vezes categorizados como firewalls de rede ou firewalls baseados em host, como o Firewall do Windows.

Exemplos práticos de uma política de segurança em uma empresa:

- Proibir que os usuários acessem o domínio Facebook;
- Verificar quais sites os usuários acessam

Trocar o gateway principal da rede, caso o link principal caia, para que o link de backup suba.



## Servidor DHCP

Servidor DHCP tem o objetivo de distribuir IPs automaticamente na rede. Explicando com um exemplo prático: 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 manualmente para cada um deles. Agora, se fossem 100, 200 ou mais, certamente a história seria outra. O Servidor DHCP faz exatamente isto, por meio dele se 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. Sempre que uma das máquinas for desconectada o IP ficará livre para o uso em outra.

Quadro 1.1: Sistemas operacionais para servidores		
Windows	Linux	Mac OS X
Windows 2000 Server	Suse	Mac OS X v10.0 Cheetah
Windows 2003 Server	Debian	Mac OS X v10.1 Puma
Windows 2008 Server	Ubuntu	Mac OS X v10.2 Jaguar
Windows 2012 Server	Mandriva	Mac OS X v10.3 Panther
	Red Hat	Mac OS X v10.4 Tiger
	Fedora	Mac OS X v10.5 Leopard
	Slackware	Mac OS X v10.6 Snow Leopard
		Mac OS X v10.7 Lion
		Mac OS X v10.8 Mountain Lion

## Dispositivos de Rede

Uma rede de computadores é composta por diferentes dispositivos, cada um com sua função, com o objetivo de dar funcionalidade e organização, bem como, prover a comunicação entre os diferentes componentes de uma rede. A seguir são citados os principais dispositivos de uma rede de computadores:

- Dispositivos de Rede Host - Equipamento utilizado pelos usuários finais para processamento das aplicações e conexão à rede. Enquadram-se nesta descrição os notebooks, netbooks, computadores pessoais;
- Dispositivo de Rede Interface - Cada computador, notebook, entre outros dispositivos se conectam à uma rede de computadores através de uma placa de rede. A esta placa de rede é dado o nome de interface de rede. Uma placa de rede pode ser do tipo Ethernet cabeada (na qual um cabo é conectado a esta placa) ou então Ethernet sem fios (placas que se comunicam via Bluetooth, ondas de rádio, etc.);
- Dispositivo de Rede Switch - Um Switch serve de concentrador em uma rede de computadores com a diferença de que recebe um sinal vindo de um Computador Origem e entrega este sinal somente ao Computador Destino. Isto é possível devido a capacidade destes equipamentos em criar um canal de comunicação exclusivo (origem/destino).
- Dispositivo de Rede Gateway - Um Gateway, ou Ponte de Ligação, é um meio intermediário destinado, geralmente, a interligar redes. Exemplos clássicos são os meios de se ligar uma rede local a internet. Servidores de Internet, Firewalls e Roteadores seriam exemplos de Gateway. Para um host de uma rede acessar a internet deve se configurar no host o endereço do gateway.

- Dispositivo de Rede Gateway - Um Gateway, ou Ponte de Ligação, é um meio intermediário destinado, geralmente, a interligar redes. Exemplos clássicos são os meios de se ligar uma rede local a internet. Servidores de Internet, Firewalls e Roteadores seriam exemplos de Gateway. Para um host de uma rede acessar a internet deve se configurar no host o endereço do gateway.
- Dispositivo de Rede Roteadores - No passado, entre os anos de 1990 e 2000, uma Bridge era nada mais que uma ponte de ligação física entre duas ou mais redes de cabeamento diferentes. Usadas antigamente para ligar redes com cabeamento Coaxial, Ethernet ou Fibra Óptica. Hoje em dia as Bridges não existem mais e foram substituídas pelos Roteadores e Acess Points. Mas o seu conceito de interligar redes permanece nos Roteadores, agora interligando redes do mesmo tipo de cabeamento e também redes Wireless.

## Protocolo

Protocolo, em uma rede de computadores, nada mais é do que um conjunto de regras que definem a comunicação dos dispositivos em uma rede. São eles que fazem os computadores de uma rede se comunicarem. Um dos protocolos mais conhecidos de rede de computadores e da própria internet é o protocolo TCP/IP.

## Protocolo TCP/IP

O TCP/IP é formado por dois protocolos, o TCP (Transmission Control Protocol) e o IP (Internet Protocol). O Internet Protocol (IP), é responsável por fazer com que as informações enviadas por um computador cheguem a outros computadores mesmo que eles estejam em redes fisicamente distintas, ou seja, não existe conexão direta entre eles. Como diz o próprio nome (Inter-net), o IP realiza a conexão entre redes. E é ele quem traz a capacidade da rede TCP/IP de se "reconfigurar" quando uma parte da rede está fora do ar, procurando uma rota (caminho) alternativo para a comunicação. Já o protocolo TCP é um protocolo orientado a conexão. Ele permite que sejam enviadas mensagens de qualquer tamanho e cuida de quebrar as mensagens em pacotes que possam ser enviados pela rede e também cuida de remontar os pacotes no destino e de retransmitir qualquer pacote que seja perdido pela rede, de modo que o destino receba a mensagem original, da maneira como foi enviada. Podemos dizer de certa forma que a mercadoria é o TCP e o caminhão que a leva é o IP.

## Mac Address

O Mac Address (Endereço Mac) é o CPF internacional de todos os dispositivos de rede. Não existem dois CPFs iguais. O endereço MAC é formado por um conjunto de 6 dígitos separados por dois pontos ou hífen. Ex: 00:19:B9:FB:E2:58 Esse endereço é importante pois podemos fazer regras de permissão em um firewall com eles. Por exemplo, barrar qualquer dispositivo de rede que não seja os Mac Address dos computadores. Dessa forma os celulares não conseguiriam funcionar.

## PORTA



Porta é um ponto físico (hardware) ou lógico (software), no qual podem ser feitas conexões, ou seja, um canal através do qual os dados são transferidos entre um dispositivo de entrada e o processador ou entre o processador e um dispositivo de saída. Ou acesso por dentro e por fora do computador.

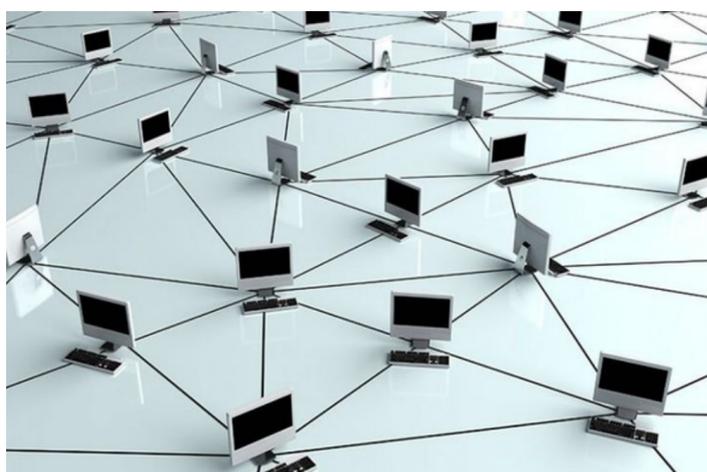
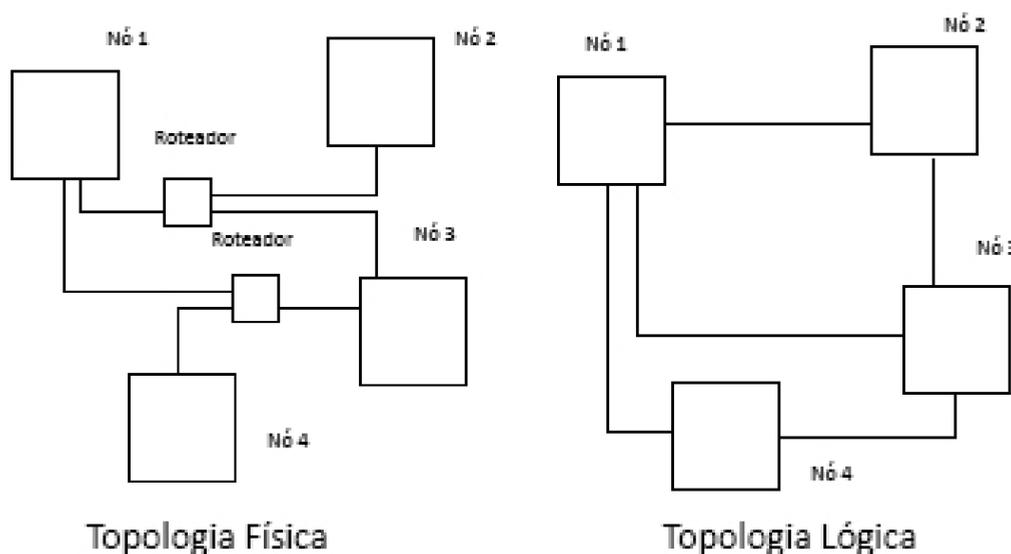
Porta física (hardware) seria uma conexão USB para conectar algum dispositivo no computador.

Porta lógica (software) é uma conexão virtual que pode ser usada na transmissão de dados. A mais comum é a porta protocolada TCP, que é usada para conexão entre computadores e a Internet. Outro exemplo de porta lógica é um software como o Skype que usa um canal de comunicação que é a porta 23399 para enviar e receber dados e que se essa porta for fechada por um Firewall o Skype e qualquer outro software que use essa porta deixaria de funcionar.

## TOPOLOGIA DE REDES

Uma topologia de rede tem o objetivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia física demonstra como os computadores e dispositivos estão dispersos na rede (aparência física da rede).

A topologia lógica demonstra como os dados trafegam na rede (fluxo de dados entre os computadores que compõe a rede).

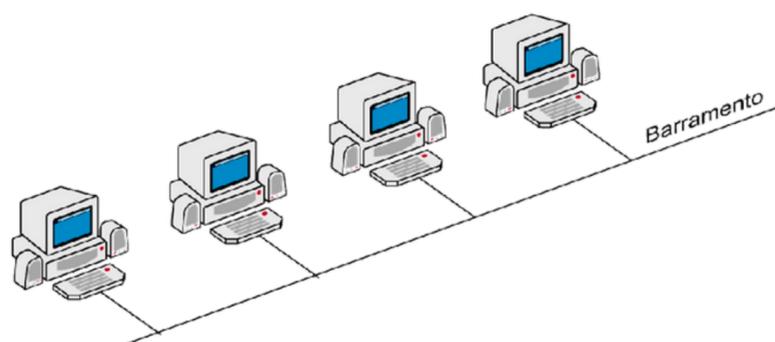


### Topologia de Redes = Barramento

Na topologia em barramento todos os computadores trocam informações entre si através do mesmo cabo, sendo este utilizado para a transmissão de dados entre os computadores.

As características da topologia em barramento são:

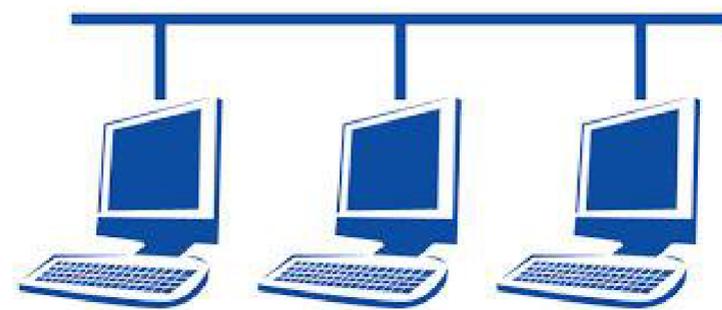
- Estações de trabalho (nós) compartilham do mesmo cabo.
- São de fácil instalação.
- Utilizam pouca quantidade de cabo.
- Baixo custo e facilidade de ser configurada em lugares pequenos.



Como desvantagens deste tipo de topologia, está o fato de que somente um computador pode transmitir informações por vez.

Caso mais de uma estação tente transmitir informações ao mesmo tempo, temos uma

colisão de pacotes. Enquanto houver a colisão de pacotes o computador que estiver enviando os pacotes fará novas tentativas de reenvio várias vezes, até que o barramento esteja disponível para a transmissão e os dados cheguem até o computador receptor.



Outras desvantagens da topologia em barramento são:

- Problemas no cabo (barramento) afetam todos os computadores;
- Muitos computadores na rede oscilam a velocidade da rede;
- Gerenciamento complexo (erros e manutenção da rede).

Uma rede em anel corresponde ao formato que a rede possui, pois os dispositivos conectados na rede formam um circuito fechado, no formato de um anel (ou círculo). Essa rede

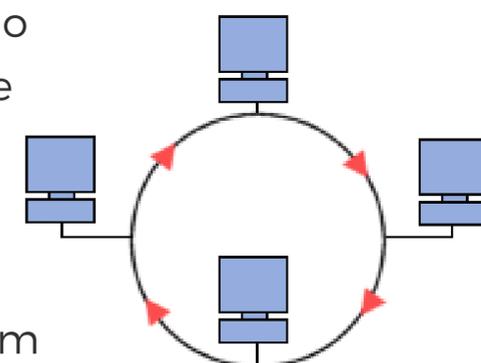
também possui outro nome conhecido, Token Ring, apesar de Token Ring ser um Protocolo de Redes que

é usado nessa topologia. Neste tipo de topologia os dados são transmitidos unidirecionalmente, ou seja, em

uma única direção, até chegar ao computador destino. Desta forma, o sinal emitido, chamado de Token, pelo computador origem passa por diversos outros computadores, que retransmitem este sinal até que o mesmo chegue ao computador destino.

Como vantagens desta topologia estão:

- Manutenção mais rápida e fácil que na topologia Barramento.
- Como desvantagens desta topologia está:
- Atraso no processamento de dados por ser uma rede unilateral.



## Topologia de Redes = Estrela

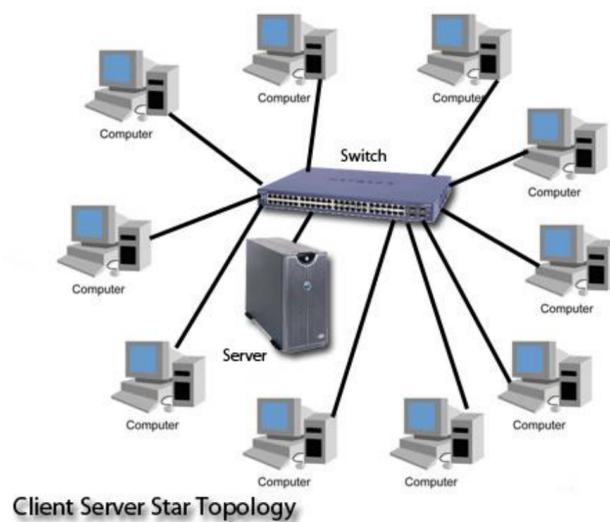
Uma rede em estrela possui esta denominação, pois faz uso de um concentrador na rede. Um concentrador nada mais é do que um dispositivo (switch ou roteador) que faz a comunicação entre os computadores que fazem parte desta rede. Dessa forma, qualquer computador que queira trocar dados com outro computador da mesma rede, deve enviar esta informação ao concentrador para que o mesmo faça a entrega dos dados. A topologia em estrela apresenta algumas vantagens, as quais são:

- Fácil identificação de falhas em cabos pelos switchs;
- Fácil instalação de novos computadores ligados á rede;
- Falha em um computador da rede não afeta os outros;

Como desvantagens ligadas a esta topologia, estão

Quanto mais distantes os computadores, mais caro será a rede.

Caso de falha no centralizador afeta toda a rede conectada a ele.



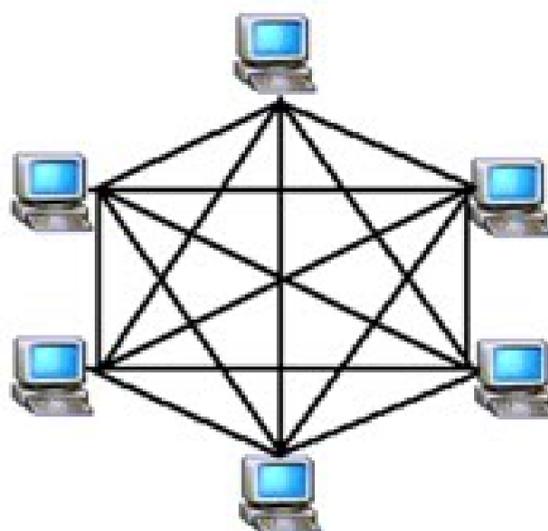
## Topologia de Redes - Malha

A rede malha é oposta a rede Estrela. Sua rede é descentralizada onde cada computador é ligado diretamente a todos os outros computadores da rede. Não possui um centralizador como um switch. Então em uma rede de malha que contém 5 computadores, cada computador deve ter 4 interfaces de rede para fazer a comunicação com os outros 4 computadores.

Como vantagens deste tipo de rede, podemos citar:

- Tempo de espera curto por causa dos muitos canais de comunicação onde pelo menos um canal faz a ligação direta entre origem e destino.
- Problemas na rede não interferem no funcionamento dos demais computadores.

Uma desvantagem desta topologia está no custo de implementação da mesma, uma vez que para isso, existe a necessidade de instalar uma quantidade de interfaces de rede em cada máquina semelhante a mesma quantidade de computadores existentes na rede em malha.

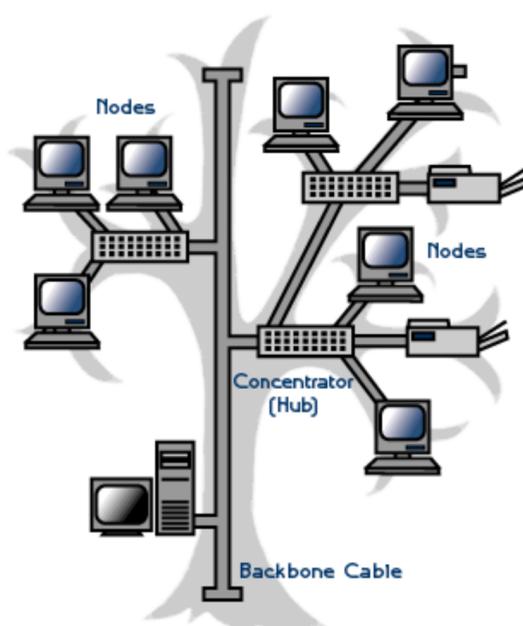


## Topologia de Redes - Árvore

Uma topologia de árvore é uma topologia de rede híbrida onde Redes Estrelas são interligadas usando uma Rede Barramento.

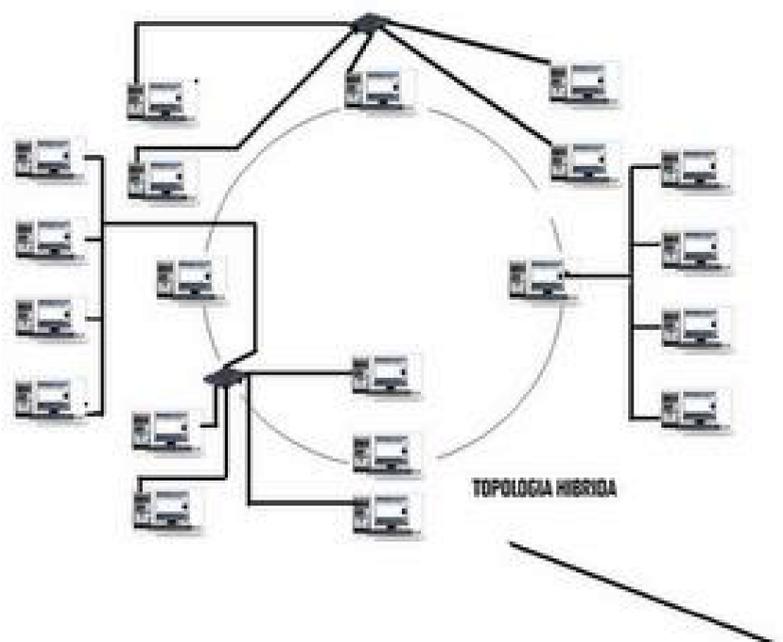
Foi criada para se unificar as vantagens de usar uma rede Barramento e uma rede Estrela embora se tenha também suas desvantagens.

Especificamente o ponto positivo da Topologia Árvore, que veio da Topologia Barramento, seria o baixo custo no cabeamento em redes muito grandes. Em redes pequenas ou médias essa diferença de custo não é muito grande e as empresas preferem por optar por uma rede Estrela para não terem o ponto negativo da Topologia Árvore, vindo da Topologia Barramento, que seria possíveis problemas no cabo (barramento) que afetaria todos os computadores.



## Topologia de Redes - Híbrida

É chamada de topologia híbrida aquela topologia que é formada por diferentes tipos de topologia, ou seja, é formada pela união, por exemplo de uma rede em barramento e uma rede em estrela, entre outras. A finalidade de uma topologia do tipo híbrida está no fato de poder aproveitar o que existe de melhor (custo/benefício) entre os diferentes tipos de topologias, adaptando-as às necessidades de uma empresa, universidade, ou o ambiente onde será aplicada.



## Conceitos de Comunicação

A comunicação entre dois equipamentos pode ser categorizada em 3 tipos:

- Simplex: Quando só um computador origem envia dados à um computador destino e o computador destino nunca envia nada para o computador origem;
- Half-Duplex: Os dois computadores enviam e recebem dados porém quando um envia o outro só recebe, sendo impossível os dois enviarem ao mesmo tempo;
- Full-Duplex: Ambos os computadores enviam e recebem ao mesmo tempo.

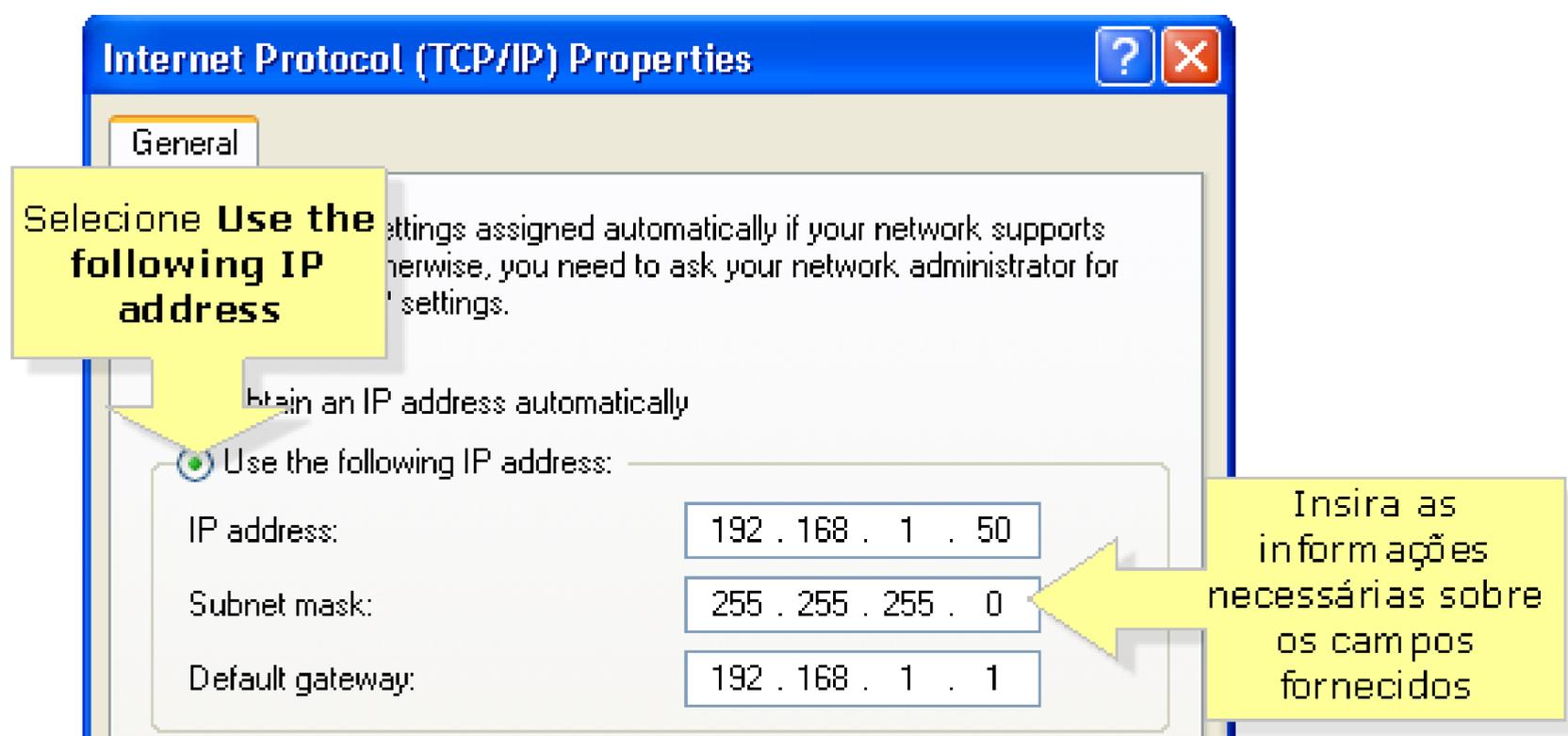
## Endereço de IP

O IP é o endereço lógico que cada dispositivo na rede tem que ter para que se comunique com os outros dispositivos.

O endereço IP de um dispositivo usando a versão 4 do Protocolo IP (IPV4) é um número formado por 4 conjuntos de dígitos que vão do 0 até o 255.

Ex: 192.168.0.2

O comando para verificar o IP do próprio computador usando Windows é o IPConfig.



# Classes do IP

Existem 5 endereços de IP:

Classe	Decimal de Máscara de Sub-Rede	Hosts por Rede	Redes	Endereços de Início e Fim
A	255.0.0.0	16 Milhões	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Milhões	192.0.0.0 - 223.255.255.255
D	Reservado para grupos multicast			224.0.0.0 - 239.255.255.255
E	Reservado para uso futuro, ou com o objetivo de Pesquisa e Desenvolvimento			240.0.0.0 - 254.255.255.254

A Máscara de Rede é quem define quantos computadores existem em determinada rede. Hoje esse conceito não existe mais, as redes são formadas pela Máscara de Rede que pode ter um tamanho muito maior do que o necessário, porém a limitação da quantidade de máquinas em cada rede é delimitada hoje em dia pelo DHCP. Mas é importante mesmo assim entender como funciona a Máscara de Rede.

Veja o exemplo:

- Temos 2 máquinas na secretaria. Qual classe de IP devemos usar?

Depende de como você quer dividir sua rede.

Vamos imaginar o seguinte:

Desejamos criar 1 rede com dois computadores. Então se o máximo de redes é 1 e o máximo de hosts são 2 podemos usar qualquer classe de IP neste caso. Então vamos ver como faríamos para que no laboratório de informática A, a rede esteja configurada para não aceitar um 3o computador.

Mas para isso, temos que entender o Sistema Binário.

## Sistema Binário

O sistema binário é um sistema de numeração posicional em que todas as quantidades se representam com base em dois números, ou seja, zero e um (0 e 1).

Sistema de numeração posicional é um modo de representação numérica na qual o valor de cada algarismo depende da sua posição relativa na composição do número.

O valor do número é a soma de cada algarismo que o compõe, considerando a posição em que o mesmo se encontra.

A Máscara de Rede trabalha com valores que vão de 0 a 255.

Vamos verificar como calcular os números 0 e 255 no sistema binário. Como vimos o sistema binário é um sistema de numeração posicional em que todas as quantidades se representam com base em dois números, ou seja, zero e um (0 e 1). Esse sistema trabalha com um sistema de 8 bits, que são os dígitos 0 ou 1. O sistema de 8 bits também é chamado de Octeto.

Então vamos ver aqui como é o sistema de 8 bits binário:

128 64 32 16 8 4 2 1

Como podemos notar os números são múltiplos de 2. Por isso esse é outro nome dado à esse sistema. Sistema de Base 2. Por padrão todos os bits estão desligados, ou seja, com valor dígito binário 0:

128 64 32 16 8 4 2 1  
0 0 0 0 0 0 0 0

Por estarem desligados o valor total gerado é 0. Agora imaginemos que o 4o bit está ligado. O 4o bit é representado pelo 8. Ficaria assim:

128 64 32 16 8 4 2 1  
0 0 0 0 1 0 0 0

Pelo 4o bit estar ligado e seu valor ser 8, o valor total gerado é 8. Agora imaginemos que o 7o bit está ligado. O 7o bit é representado pelo 64. Ficaria assim:

128 64 32 16 8 4 2 1  
0 1 0 0 0 0 0 0

Pelo 7o bit estar ligado e seu valor ser 64, o valor total gerado é 64. E se além do 7o bit estar ligado, a gente ligar o 6o bit? Ficaria assim:

128 64 32 16 8 4 2 1  
0 1 1 0 0 0 0 0

Logo então a soma do 6o bit que tem como valor o 32 e do 7o bit que tem como valor o 64 seria:

$$64+32=96$$

Como ficaria se quiséssemos que no sistema binário saísse o valor 100? Primeiro temos que compreender que não podemos pegar o 8o bit de cara pois ele tem um valor maior que 100. Então vamos pegar o 7o bit que possui o valor de 64:

```
128 64 32 16 8 4 2 1
0 1 0 0 0 0 0 0
```

Agora para complementarmos devemos pegar o 6o bit que possui o valor de 32:

```
128 64 32 16 8 4 2 1
0 1 1 0 0 0 0 0
```

Até aqui temos  $64+32=96$

Como temos 96 e falta 4 para completarmos o número 100, vamos pegar o 3o bit que tem como valor o 4.

```
128 64 32 16 8 4 2 1
0 1 1 0 0 1 0 0
```

Agora completamos a conta:  $64+32+4=100$

E o número 100 em binário é 01100100

## Máscara de Sub-Rede

Analisando a máscara de rede da classe A: O primeiro dígito representa a quantidade de redes disponíveis, no caso 127. E o segundo, terceiro e quarto dígito representam a quantidade de hosts em cada sub-rede que seriam 16 milhões. Na Classe C onde vamos executar o exemplo, os três dígitos são relativos ao endereço de rede que seriam 2 milhões e o último dígito representa o número de hosts que seria 254. No nosso exemplo vamos definir que a primeira rede disponível na classe C, será a rede que vamos criar, e ela terá 2 hosts. Pela tabela anterior vimos que a classe C começa em 192.0.0.0 sendo que o último dígito é referente a quantidade de máquinas e os três primeiros dígitos é a identificação da rede.

## Máscara de Rede

Então como a nossa rede neste exemplo começa em 192.0.0.0 teríamos os seguintes endereços. 192.0.0.0 neste caso, ou qualquer outro IP que seja o primeiro IP de uma rede será sempre reservado para que a própria sub-rede funcione. Então no nosso exemplo ele será usado para fazer nosso exemplo apenas funcionar. Então ficaria:

192.0.0.0 – Rede

192.0.0.1 – Computador 1

192.0.0.2 – Computador 2

192.0.0.3 – Broadcast

O último endereço IP de qualquer rede será sempre reservado para Broadcast. Broadcast é o canal de comunicação da rede para enviar pacotes para todos os hosts da rede de uma única vez.

E agora como vamos calcular a máscara de rede dessa sub-rede? Usando o sistema binário. Uma máscara de rede é formada pelo número 255 que representa a identificação da classe da rede conforme a tabela abaixo:

Classe	Decimal de Máscara de Sub-Rede	Hosts por Rede	Redes	Endereços de Início e Fim
A	255.0.0.0	16 Milhões	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Milhões	192.0.0.0 - 223.255.255.255
D	Reservado para grupos multicast			224.0.0.0 - 239.255.255.255
E	Reservado para uso futuro, ou com o objetivo de Pesquisa e Desenvolvimento			240.0.0.0 - 254.255.255.254

A Classe A é formada por 255.0.0.0

A Classe B é formada por 255.255.0.0

A Classe C é formada por 255.255.255.0

O 255 quando representa a identificação da rede nunca muda nas classes IP.

O que PODE mudar é o dígito 0 pois ele representa a quantidade de hosts na rede.

Então na nossa classe C já temos o 255.255.255

Falta calcular o próximo dígito.

O 255 vem do binário como já vimos que é: 11111111

Então se queremos 2 computadores na rede, temos que usar a seguinte fórmula para calcular o número de hosts em uma rede:

$$2^n - 2 = \text{número de hosts desejados na rede}$$

No caso desejamos 2 hosts na rede.

$$\text{Então a fórmula vai ficar } 2^n - 2 = 2$$

Neste caso a potência na base 2 será o 2 pois  $2^2 = 4$

Logo:

$$2^n - 2 = \text{número de hosts desejados na rede}$$

$$2^n - 2 = 2$$

$$2^2 - 2 = 2$$

$$4 - 2 = 2$$

Esse número 2 encontrado vai representar no sistema binário que os dois primeiros bits não serão contados.

128 64 32 16 8 4 2 1

1 1 1 1 1 0 0

Então vamos contar os bits que serão usados

$128+64+32+16+8+4=252$

Então a máscara de sub-rede final será 255.255.255.252 e será ela que controlará automaticamente todas as sub-redes da classe C.

Então as duas primeiras subredes da classe C ficariam assim:

192.0.0.0 Reservado para a Rede 1 funcionar

192.0.0.1 Host 1 da Rede 1

192.0.0.2 Host 2 da Rede 1

192.0.0.3 Reservado para Broadcast da Rede 1

192.0.0.4 Reservado para a Rede 2 funcionar

192.0.0.5 Host 1 da Rede 2

192.0.0.6 Host 2 da Rede 2

192.0.0.7 Reservado para Broadcast da Rede 2

E assim por diante....

Lembrando novamente que hoje esse conceito não existe mais, as redes são formadas pela Máscara de Rede que pode ter um tamanho muito maior do que o necessário, porém a limitação da quantidade de máquinas em cada rede é delimitada hoje em dia pelo DHCP.

Mas tudo o que vimos até agora é para entendermos outra coisa, a conotação CDRI.

## Conotação CDRI

CDRI quer dizer Classless Inter-Domain Routing. Foi criada em 1993 para facilitar e resumir o número de informações passadas entre os técnicos e principalmente facilitar a questão de roteamento entre sub-redes.

Verificando o nosso exemplo anterior onde nossa máscara de rede era

255.255.255.252

Lembrando que cada 255 em binário é representando por 11111111 e que o 252 que acabamos de calcular era 11111100.

A máscara de rede representada em binário é:

255 255 255 252

11111111.11111111.11111111.11111100

O total de bits usados foram 30.

Então em CDRI podemos dizer que nossa rede é 192.0.0/30

Lembrando que o IPV4 é formado por um número IP, Máscara de Rede entre outras coisas, porém o endereço IP e a Máscara de Rede são sempre o mínimo de informação que devemos configurar manualmente em uma máquina caso ela não esteja com IP DHCP.

Os técnicos quando falam em fazer por exemplo uma rede 192.0.0/30, estão falando exatamente o que acabamos de fazer:

192.0.0.0 Reservado para a Rede 1 funcionar  
192.0.0.1 Host 1 da Rede 1  
192.0.0.2 Host 2 da Rede 1  
192.0.0.3 Reservado para Broadcast da Rede 1  
192.0.0.4 Reservado para a Rede 2 funcionar  
192.0.0.5 Host 1 da Rede 2  
192.0.0.6 Host 2 da Rede 2  
192.0.0.7 Reservado para Broadcast da Rede 2

E assim por diante...

No nosso caso onde temos nesse modelo 192.0.0/30, significa que a cada 4 IP's temos uma rede funcional.

Lembrando:

192.0.0.0 Reservado para a Rede 1 funcionar  
192.0.0.1 Host 1 da Rede 1  
192.0.0.2 Host 2 da Rede 1  
192.0.0.3 Reservado para Broadcast da Rede 1

Isso significa que teríamos mais ou menos 60 sub-redes de 2 hosts.

Caso precisemos fazer um roteamento em todas as sub-redes, em vez de apontar o endereço IP em cada uma, podemos genericamente rotear usando o CDRI. Ficaria o roteamento usando o 192.0.0/30 que ficaria bem mais fácil. Lembrando novamente que hoje em dia o DHCP que é usado para controle de sub-redes. DHCP e roteamento vamos ver mais para frente.

## Unidades de Medida

No nosso caso onde temos nesse modelo 192.0.0/30, significa que a cada 4 IP's temos uma rede funcional. Lembrando:

192.0.0.0 Reservado para a Rede 1 funcionar  
192.0.0.1 Host 1 da Rede 1  
192.0.0.2 Host 2 da Rede 1  
192.0.0.3 Reservado para Broadcast da Rede 1

Isso significa que teríamos mais ou menos 60 sub-redes de 2 hosts.

Caso precisemos fazer um roteamento em todas as sub-redes, em vez de apontar o endereço IP em cada uma, podemos genericamente rotear usando o CDRI. Ficaria o roteamento usando o 192.0.0/30 que ficaria bem mais fácil. Lembrando novamente que hoje em dia o DHCP que é usado para controle de sub-redes. DHCP e roteamento vamos ver mais para frente.

1 bit (b) = menor informação para ser armazenada ou transferida

8 bits (b) = 1 Byte (B)

128 Bytes (B) = 1 Kilobit (Kb)

8 Kilobits (Kb) = 1 KiloByte (KB)

128 KiloBytes (KB) = 1 Megabit (Mb)

8 Megabits (Mb) = 1 MegaByte (MB)

128 MegaBytes (MB) = 1 Gigabit (Gb)

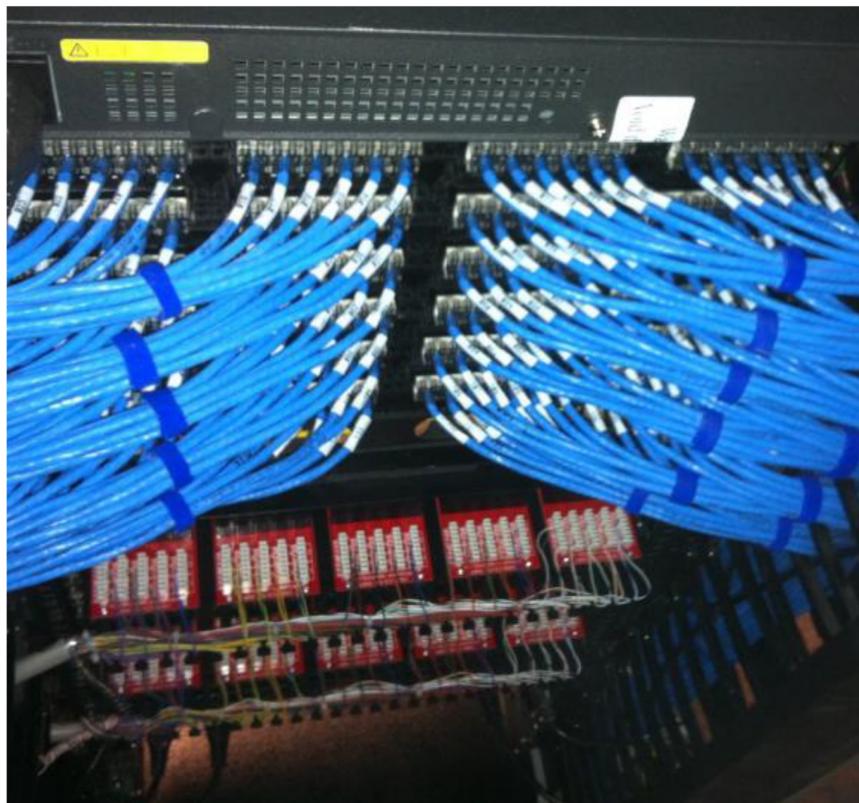
8 Gigabits (Gb) = 1 GigaByte (GB)

128 GigaBytes (GB) = 1 Terrabit (Tb)

8 Terrabits (Tb) = 1 TerraByte (TB)

# CABEAMENTO ESTRUTURADO

Cabeamento Estruturado é a parte das Redes que estuda a organização dos meios de comunicação nas áreas da telefonia e informática em uma infraestrutura.



## Meio de Trasmissão de Dados

Existem dois tipos de transmissão de dados: Meio Físico (Cabeamento) e Meio Não-Físico (Wireless).

Podemos entender tipo de transmissão de dados, qualquer meio de transmissão que transporte pacotes de informações entre dois ou mais pontos. Por exemplo, um cabeamento que faça a comunicação entre um servidor e seus hosts. O meio físico mais popular em redes pelo custo benefício é o cabeamento de par trançado onde temos maior flexibilidade e menor custo.

## Par Traçado

Por que se chama Par Trançado? Porque são usados pares de fios onde esses pares acabam proporcionando uma barreira eletromagnética que protege as transmissões de dados de interferências externas, sem que se precise usar cabos com blindagem para isso, como os cabos coaxiais por exemplo, ele normalmente é encontrado na cor azul no caso dos cabos ethernet. O Par Trançado possui 4 pares de fios podendo ser crimpados de 3 maneiras diferentes dependendo da sua utilização:

- Crimpagem CrossOver: Usado em situações como a comunicação direta entre dois computadores sem uso de switch ou roteador.
- Crimpagem RollOver: Usado para acessar a porta de console de um switch ou roteador gerenciável. Muito usado nos equipamentos da Cisco.
- Crimpagem Direto: O mais usado nas redes domésticas e empresariais. Utilizado em comunicações entre computadores utilizando switches ou roteadores. Diferente da situação envolvendo o cabo CrossOver.

Existem 4 tipos de Cabos par Trançado:

- Par Trançado UTP - UTP (Unshielded Twisted Pair): Sem blindagem e o mais barato. É o mais comum usado em redes domésticas e empresariais;



- Par Trançado FTP - FTP (Foiled Twisted Pair): Um cabo melhor protegido contra interferências externas já que cada par é coberto por uma fina película de metal;



- Par Trançado UFTP - UFTP (Unshielded Foiled Twisted Pair): Um cabo melhor protegido contra interferências externas. A diferença é que existe uma malha que protege os 4 pares ao mesmo tempo em vez de uma fina película que cobre cada par;



- Par trançado SFTP - SFTP (Shielded and Foiled Twisted Pair): O cabo mais protegido pois além de possuir uma fina película em cada par, possui uma malha em volta de todos os pares.



## Atenuações

Uma analogia para ilustrarmos a atenuação seria aquela observada com fogos de artifício. Os fogos de artifício quando acesos se deslocam com um brilho intenso que vai diminuindo a medida que sua energia vai acabando. Esta situação ilustra o sinal transmitido em um cabo real. Se estes fogos seguissem indefinidamente, com o mesmo brilho, até serem perdidos de vista teríamos a situação equivalente do cabo ideal, ou sem perdas independentes de seu comprimento. O que ocorre, no entanto, é que em função dos materiais utilizados na construção de um cabo assim como de seu comprimento, parte deste sinal se perde de alguma forma. Fisicamente a atenuação depende da frequência do sinal e da construção do cabo, portanto a qualidade construtiva dos condutores são determinantes na redução deste fenômeno. Dentro da área de cabeamento estruturado, quanto maior for a frequência do cabo, menor será a atenuação dele, ou seja, menor será a perda de dados de acordo com o comprimento do cabo.

## Arquitetura das Redes

Arquitetura de Redes é o campo das Redes de Computadores que estuda as funcionalidades da rede, cabeamento estruturado e os métodos de implementação dos sistemas nos computadores.

Resumindo em outras palavras, é o projeto de uma Rede que mostra como ela é fisicamente e como funciona logicamente com seus dispositivos físicos, configurações e formato de dados. Em telecomunicações, a especificação de uma arquitetura de rede também pode incluir uma descrição detalhada dos produtos e serviços prestados através de uma rede de telecomunicações, além de mostrar como funciona a geração de valores a serem cobrados dos clientes.

## Tipos de Arquiteturas

Hoje em dia, "Ethernet" é quase sinônimo de rede. Por ser um padrão aberto, qualquer fabricante pode fabricar placas e outros componentes de rede e desenvolver soluções, o que aumenta a concorrência e o volume produzido, derrubando os preços. Dentro do cenário atual, desenvolver padrões proprietários de rede não faz muito sentido, pois além de produzir as placas o fabricante precisaria arcar com todos os custos relacionados ao desenvolvimento e à divulgação da tecnologia. Mas nem sempre foi assim. Durante a década de 1980 o padrão Ethernet disputava a supremacia com dois padrões então proprietários, o Arcnet e o Token Ring. O Arcnet chegou a ser mais popular que o Ethernet e o Token Ring, chegou perto de dominar as redes corporativas. O Arcnet é o mais antigo, ele foi desenvolvido em 1976 e as primeiras placas e hubs chegaram ao mercado em 1977, a custos relativamente baixos para os padrões da época. As redes Arcnet utilizavam uma topologia de estrela, que lembra bastante as das redes atuais. Naquela época se usava um hub central e um cabo individual entre ele e cada estação. Outra diferença nas redes Arcnet comparado com o que usamos hoje é que na Arcnet eram utilizados cabos coaxiais e não cabos de par trançado. Esta arquitetura era mais flexível que a dos primeiros padrões Ethernet, que ainda utilizavam uma arquitetura de barramento, com um cabo compartilhado.



Na Arcnet os cabos podiam ter até 610 metros, mais do que em qualquer padrão Ethernet para fios de cobre naquela época e, durante muito tempo, as placas Arcnet foram mais baratas, o que fez com que a arquitetura fosse bastante popular até perto do final da década de 1980. Os dois grandes problemas da Arcnet eram a baixa taxa de transferência, apenas 2.5 megabits, e o fato do padrão ser proprietário, o que limitou o número de fabricantes produzindo equipamentos e impediu que os preços caíssem na mesma velocidade que os Ethernet que começaram caros e foram diminuindo o valor.

Eventualmente, o padrão foi aberto, dando origem ao Ansi Arcnet. Surgiram então mais opções de cabeamento, incluindo o uso de cabos de par trançado e cabos de fibra óptica e, em 1999, foi lançado um padrão atualizado, o Arcnet Plus, que passou a transmitir de 4 megabits para 20 megabits. Mas já era tarde demais. Em 1995 a Ethernet já começava a usar taxas de 100 megabits e isso acabou com a arquitetura da Arcnet que só 4 anos mais tarde dobrou sua transferência mas que não chegava nem aos pés da velocidade do padrão Ethernet. A Arcnet era cara e lenta. O motivo do fracasso da rede Arcnet que embora naquele momento fosse superior em desempenho à rede Ethernet, a Ethernet tinha uma visão de futuro de 10 anos na frente onde ela imaginava que os computadores teriam mais hardware e conseqüentemente o fluxo de dados transmitidos na rede seriam maior e ela já projetava a rede com essas características futurísticas enquanto a rede Arcnet não se preocupou com esse tipo de visão. Do outro lado existia as redes Token Ring em formato de anel. Embora tivessem atraso nas comunicações por causa do protocolo Token, em 1989 passaram a operar de 4 megabits para 16 megabits e eram mais rápidas que as redes Arcnet e Ethernet. A diferença entre Arcnet e a Token Ring em termos de desempenho era que enquanto a Arcnet tinha uma rede sólida mas não tão rápida quanto a Token Ring, a Token Ring tinha uma rede mais rápida porém um protocolo mais lento e praticamente igualava as duas redes. Pequenas empresas optavam por usar Arcnet pelo custo benefício enquanto as maiores empresas usavam Token Ring que não tinha o melhor custo benefício mas eram mais rápidas. Ambas estavam almejando o domínio até a Ethernet chegar com o padrão de 100 megabits de transmissão e ser o melhor custo benefício entre elas. A Ethernet era mais rápida e mais barata.

## Servidor de Virtualização

As categorias de cabos existem para diferenciar a tecnologia de cada cabeamento. Quanto maior a categoria, mais atual é o cabo, maior é o número de torções em par trançado para evitar interferências eletromagnéticas e maior o fluxo de dados que pode trafegar. Lembrando que as categorias são para diferentes tipos de cabos de Redes e diferentes tipos de cabo de telefonia.



### CAT 1

A categoria 1 de cabos foi uma categoria UTP (Unshielded Twisted Pair) no qual foi designado para comunicações com telefone. A frequência máxima de transmissão (fluxo de dados) do Cat1 era de 1MHz, sendo que a do Cat 5 é de 100MHz, vemos que o Cat1 não é adequado para transmissão de dados. Cat1 não é mais usado e nem reconhecido pelas novas normas da Telecommunications Industry Association (TIA).

## CAT 2

A categoria 2 de cabeamento também chamada de Cat2 foi uma categoria de cabo UTP (Unshielded Twisted Pair) no qual foi designado para comunicações com telefone e transmissão de dados. A frequência máxima de transmissão (fluxo de dados) do Cat2 era de 4MHz. O Cat2 usava 4 pares trançados com 8 fios no total e foi usada em redes Token Ring e ArcNet.

Cat1 não é mais usado e nem reconhecido pelas novas normas da Telecommunications Industry Association (TIA).



## CAT 3

A categoria 2 de cabeamento também chamada de Cat2 foi uma categoria de cabo UTP (Unshielded Twisted Pair) no qual foi designado para comunicações com telefone e transmissão de dados.

A frequência máxima de transmissão (fluxo de dados) do Cat2 era de 4MHz. O Cat2 usava 4 pares trançados com 8 fios no total e foi usada em redes Token Ring e ArcNet.

Cat1 não é mais usado e nem reconhecido pelas novas normas da Telecommunications Industry Association (TIA).



## CAT 4

A categoria 4 também chamada de Cat4 foi uma categoria de cabo UTP (Unshielded Twisted Pair) onde o cabo era formado por 4 pares trançados operando a 16 megabits e onde a frequência era de 20 MHz. Foi usado em telefonia, redes token ring e redes 10Base-T mas foi rapidamente superada e substituída pelos cabos da Categoria 5. Cat4 não é mais usado e nem reconhecido pelas novas normas da Telecommunications Industry Association (TIA).

## CAT 5

A Categoria 5, também conhecida como Cat5, é uma categoria de cabo UTP (Unshielded Twisted Pair) usada para carregar pacotes de dados e inclusive outros tipos de sinais como telefonia e vídeo. Conseguem carregar até 100 megabits. A performance do cabo é de até 100 MHz e é usado em redes 10BASE-T e 100BASE-T. As redes 100Base-T podem usar tanto cabos CAT3, CAT5 ou acima de CAT5. Porém redes 100Base-T que não usam cabos CAT3, possuindo só cabos CAT5 ou superiores, são chamadas de redes 100Base-TX por possuir uma performance de transmissão de dados maior comparado as redes 100Base-T onde existem cabeamento CAT3 que possuem uma performance inferior. O Cat 5 foi rapidamente substituído pelo Cat5e.

## CAT 5e

A Categoria 5e, também conhecida como Cat5e, é uma categoria de cabo UTP (Unshielded Twisted Pair) usada para carregar pacotes de dados e inclusive outros tipos de sinais como telefonia e vídeo.

Conseguem carregar até 1000 megabits.

A performance do cabo é de até 100 MHz e é usado em redes 10BASE-T, 100BASE-T e 1000BASE-T. O Cat5e é basicamente uma versão melhorada do Cat5 pois proporciona maior velocidade que o anterior. O Cat5e é o cabo mais utilizado atualmente por técnicos em suporte pela a maioria dos clientes possuem redes 100BASE-T e poucos possuem redes 1000BASE-T.

## CAT 6

A Categoria 6, também conhecida como Cat6, é uma categoria de cabo UTP (Unshielded Twisted Pair) usada para carregar pacotes de dados e inclusive outros tipos de sinais como telefonia e vídeo.

Conseguem carregar até 10000 megabits. A performance do cabo é de até 250 MHz e é usado em redes 1000BASE-T e 10000BASE-T.

A rede 10000BASE-T é mais conhecida como rede 10GBASE-T.

O Cat6 ainda não é muito usado por redes no Brasil devido ao alto custo de uma infraestrutura para comportar uma rede 10GBASE-T. Ainda existem as categorias Cat6e e Cat7 mas por seu uso ser ainda mais raro não serão abordadas no curso.

