



Aprenda com quem faz

# Redes de Computadores

Maximiliano de Carvalho Jacomo

2022



## SUMÁRIO

Capítulo 1. Redes de Computadores .....	4
História e Classificação das Redes de Computadores.....	5
Topologia das Redes de Computadores.....	13
Comunicação e Transmissão de Dados .....	21
Comutação de Dados .....	27
Conhecendo o Jargão das Redes de Computadores.....	29
Entidades de Padronização.....	33
Capítulo 2. Arquitetura e Padrões de Redes de Computadores.....	36
Arquitetura – Modelo de Referência OSI.....	39
Modelo de Arquitetura TCP/IP.....	44
Capítulo 3. Protocolo IP e Endereçamento IP .....	54
Protocolo e Endereçamento IPv4 .....	54
Classes do Endereçamento IPv4.....	60
Máscara de Sub-Redes no IPv4.....	61
Roteadores e Rotas .....	69
Protocolo IPv6.....	74
Capítulo 4. Dispositivos de Interconexão .....	79
VLANs – Redes Locais Virtuais.....	82
Capítulo 5. Elementos de Integração .....	88
Cabeamento Estruturado.....	90
Cabos e Conectores .....	96
Referências .....	106



**XP**e

# > Capítulo 1



## Capítulo 1. Redes de Computadores

---

Sejam todos bem-vindos, meus jovens Padawans!

A partir de agora, iremos iniciar a jornada rumo à galáxia das redes de computadores, onde iremos nos estudar e aprender sobre como os computadores se comunicam, trocam dados e várias outras questões relacionadas a redes de computadores.

Como seu mestre “jedi ou sith”, espero que gostem de se aventurar nessa galáxia que é repleta de conhecimento. E, para começarmos, que tal acionarmos o motor de hiperespaço para chegarmos ao primeiro ponto: conhecimentos básicos sobre redes de computadores? Então, vamos nessa, acionando o hiperespaço!

A primeira pergunta que iremos fazer a você é: Por que redes de computadores? Bem, existe um fato histórico que está presente desde os primórdios da informática que demonstra que todas as organizações estão sempre na busca da comunicação eficiente entre suas áreas de negócio, colaboradores, parceiros, fornecedores e clientes. Essa eficiência está relacionada diretamente aos fundamentos da segurança da informação que são: confidencialidade, integridade e disponibilidade, mas que não se restringem. Afinal, outros fatores como agilidade, não repúdio, facilidade e controle de acesso, custos, taxa de transmissão, padronização, portabilidade, entre outros também devem ser levados em consideração quando realizamos a comunicação e a troca de dados. O que no geral podem ser considerados fatores de sucesso em uma rede de computadores.

Atualmente, as redes de computadores estão presentes em nossas vidas para atender a diversas demandas e necessidades pessoais e profissionais, possibilitando não só a troca de dados e informações, mas

também o compartilhamento de diversos recursos computacionais ou não. Mas, de fato, temos a conclusão de que o casamento entre os computadores e as telecomunicações na década de 60 mudaram de forma radical a forma de comunicação existente na época, proporcionando uma nova forma de integração, interligação e compartilhamento de informações e recursos entre pessoas, sociedades e empresas pelo mundo a fora!

Pinheiro (2003, p.2) enfatiza o objetivo de uma rede de computadores da seguinte maneira:

Independentemente do tamanho e do grau de complexidade, o objetivo básico de uma rede é garantir que todos os recursos disponíveis sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, uma rede de computadores deve possuir regras básicas e mecanismos capazes de garantir o transporte seguro das informações entre os elementos constituintes.

De acordo com Pinheiro, percebe-se que uma rede de computadores é muito mais que uma simples conexão entre hardware e cabos. Isto porque há uma necessidade de uma série de regras (protocolos) que são necessários para regular e controlar a comunicação entre todos os elementos presentes na rede e, em todos os níveis, que vão desde o software que está sendo utilizado pelo usuário até o tipo de meio físico (cabo) de comunicação utilizado para realizar a troca de dados e informações.

### História e Classificação das Redes de Computadores

A exemplo de diversas outras invenções e tecnologias, tais como o telégrafo, os computadores e o radar, as redes de computadores foram criadas para atender as necessidades impostas por uma grande guerra. No caso a chamada “Guerra Fria” entre os EUA e a URSS que se iniciou no final da década de 50, estendendo-se até o início da década de 80.

Na ocasião, existia uma grande “tensão” militar, ideológica, econômica, política e tecnológica entre os dois países, e um medo profundo da humanidade ser extinta por meio de uma guerra nuclear. Com a URSS utilizando na época bases militares de Cuba, os EUA tinham a preocupação de sofrer um ataque de mísseis nucleares em seu território e, diante desta preocupação constante e o medo de ter seu centro de comando e defesa militar, que na época eram concentrados em um único local, ser destruído com um ataque o que deixaria o país sem ação, o governo americano, através do seu departamento de defesa americano ou DID, ordenou, no início da década de 60, a ARPA – *Advanced Research Agency* (Agência de Pesquisas Avançadas), que atualmente é conhecida como DARPA – *Defense Advanced Projects Research Agency* (Agência de Pesquisas Avançadas de Defesa), que desenvolvesse um projeto no qual possibilitasse por meio de uma rede de comunicação a interligação e a troca de informações militares entre dois ou mais pontos distintos e extremos do país. Esse projeto foi nomeado de ARPANET e, além dos militares, faziam parte do projeto as principais universidades e centro de pesquisas do país.

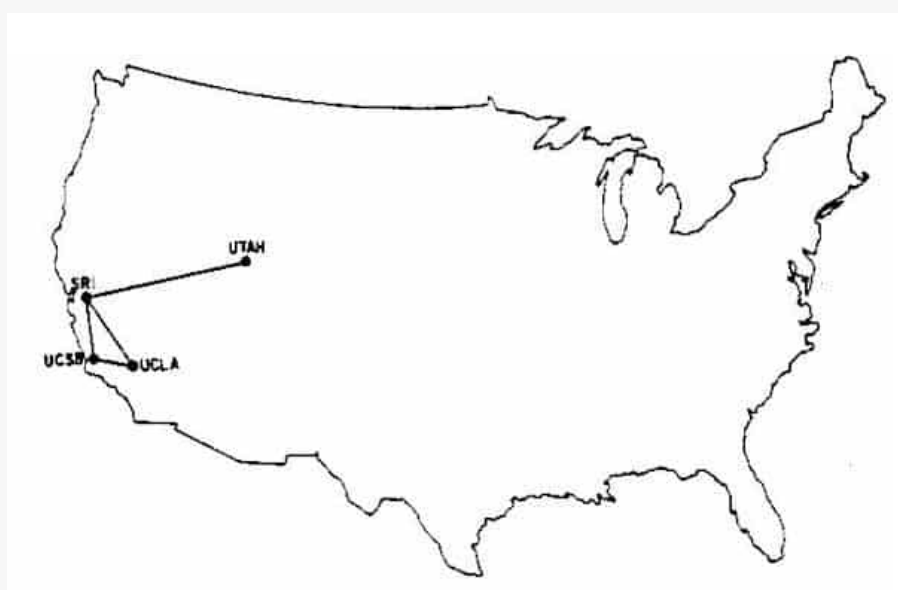
Durante a concepção do projeto, Paul Baran, um pesquisador mestre da Universidade da Califórnia em Los Angeles e inventor da tecnologia de comutação de pacotes, propôs a ideia da construção de uma rede baseada na comunicação digital via comutação de pacotes, no qual foi aceito como a melhor opção para a construção da ARPANET em 1965, no qual o estudo inicial foi intitulado *A Competitive Network of Time Sharing Computers* ou “Rede Competitiva com Computadores Interligados Simultaneamente”.

Inicialmente, em 1961, Leonard Kleinrock apresentou ao mundo uma teoria que defendia a tese de que dois servidores poderiam se comunicar para enviar e receber informações transportadas por meio de pacotes de dados, através de uma rede de nós. A ideia apresentada por

Kleinrock é a de que uma informação poderia ser dividida em pequenas porções “pacotes” e estes poderiam ser enviados por diferentes “caminhos” em uma rede e remontados no destino, formando assim a informação novamente. Na ocasião, o então diretor da DARPA, J. C. R. Licklider, apresentou um conceito de uma rede galáctica para acessar rapidamente dados de qualquer lugar do mundo – parece ser coisa de filmes Star Wars de George Lucas, não é? – Bem, junte as ideias de Kleinrock com as de Licklider e Baran, e eis que surge dentro da ARPA um sistema de comunicações que, por meio de computadores conectados a uma rede descentralizada, era imune a ataques externos. Afinal, se um ou mais nós da rede acabassem sendo destruídos, os outros poderiam continuar funcionando e trocando mensagens!

Nesse contexto, o EUA estaria seguro se tal tecnologia de rede fosse construída em larga escala, já que as informações essenciais e necessárias à defesa do país estariam protegidas e poderiam ser utilizadas por qualquer computador e um dos vários centros de controle militar do EUA.

Figura 1 - Mapa da Arpanet em 1969.







de computadores exclusiva para uso militar e governo e passou a ser uma rede de computadores acessível a todas as organizações e pessoas, dando assim origem a uma rede maior, no qual passou a ser conhecida por todos nós como a rede mundial de computadores, ou simplesmente a Internet.

É importante ressaltar que, além da ideia inicial, que era a comutação por pacotes desenvolvida por Baran, temos que ter em mente que nada disso seria possível sem o uso de uma “linguagem” comum no qual os computadores pudessem entender e se comunicarem. Ou seja, a comunicação não existiria sem um “protocolo” comum de comunicação. Esse protocolo de comunicação é o TCP/IP, que é a junção de 2 protocolos: O TCP (*Transmission Control Program*) e o IP (*Internet Protocol*), base fundamental para a comunicação entre os diversos nós de rede existentes na Internet. Mas essa história vamos estudar mais adiante, meus jovens Padawans!

Com relação à classificação das redes de computadores, atualmente podemos classificá-las de acordo com a dimensão geográfica na qual esta rede está presente, como foram concebidas e de que forma elas se comunicam uma com as outras. Neste contexto, temos:

- LAN (*Local Area Network*) traduzida como Rede de Área Local, trata-se de uma rede de computadores que possui um alcance geográfico limitado. É considerada o tipo de rede mais comum e utilizada por pessoas e empresas para interligar equipamentos e recursos computacionais em salas, escritórios, prédios comerciais, ambientes domésticos, dentre outros. Esse tipo de rede opera com taxas de transmissão que podem ser de 10Mbps, 100Mbps e 1Gbps. São consideradas redes privadas. Isto significa que são operadas e controladas por uma única entidade. São exemplos de tecnólogas das redes LANs: IEEE 802.3 (ethernet); IEEE 802.3u (fast ethernet) e; IEEE 802.5 (token ring);

- CAN (*Campus Area Network*) traduzida como Rede de Campus, trata-se de um tipo de rede similar a LAN, mas com um propósito de possuir um alcance maior que as LANs. Esse tipo de rede é utilizado para interligar redes LANs de uma mesma entidade, como por exemplo um campus de uma faculdade, condomínios ou centros comerciais em que cada um deles possui sua própria rede LAN e pertencem a mesma organização. Possuem as mesmas taxas de transmissão e tecnologias que as redes LANs.
- MAN (*Metropolitan Area Network*) traduzida como Rede de Área Metropolitana, trata-se de um tipo de rede utilizada para interligar redes LANs em distâncias maiores. Originalmente, foram concebidas pelas Operadoras de Telecom para atender uma demanda crescente de interligação de redes LANs presentes entre empresas que possuíam duas ou mais sedes separadas por algumas dezenas de quilômetros dentro da própria cidade ou em cidades ou municípios diferentes. No geral, possuem taxas de transferência a 1Gbps e utilizam diversas tecnologias, tais como: metro ethernet, ATM e frame-relay. Podem ser redes proprietárias, ou seja, controladas e operadas por uma única entidade ou por várias entidades públicas. Por fim, cabe aqui uma comparação entre as redes do tipo CAN e MAN, pois apesar de serem bem parecidas, há uma grande diferença. Em uma rede CAN toda a sua concepção parte do princípio de utilizar recursos de comunicação privado, que no final pode aumentar o custo financeiro e de administração/operação. Já na rede MAN esses recursos podem ser públicos, tornando assim os custos financeiros e de administração/operação menores.
- WAN (*Wide Area Network*) traduzida como Rede de Longa Distância, se comparada com as demais apresentadas até aqui, as redes do tipo WAN possuem uma cobertura bem superior as redes

do tipo LAN, CAN e WAN. É utilizada para interligar equipamentos e recursos computacionais em áreas com grande distância geográfica, como por exemplo: países e continentes. A Internet é também um outro exemplo de uma rede do tipo WAN. São consideradas redes com um alto custo financeiro, administrativo e operacional. Isto porque, além de serem redes de longas distâncias para que possam manter a comunicação confiável, necessitam de caminhos alternativos que as tornam um tipo de rede virtualmente ilimitada e um conjunto de tecnologias capazes de garantir a confiabilidade da rede. Possuem taxas de transmissão altíssimas, o que possibilita a troca de diversos tipos de pacotes de dados, voz e vídeo. Dentre as vantagens de uma rede do tipo WAN, se comparadas com os outros tipos de redes, está a capacidade de roteamento dinâmico que as redes do tipo WAN possuem. Isso permite que o pacote de dados chega ao seu destino, independente do caminho a seguir. Já que em redes do tipo LAN, por exemplo, esse roteamento é fixo. Como tecnologias utilizadas em redes do tipo WAN, citamos: MPLS, ATM e X.25.

- PAN (*Personal Area Network*) traduzida como Rede de Área Pessoal, trata-se de uma rede com o alcance bem limitado, aproximadamente 10 metros de distância. É um tipo de rede utilizada para interligar equipamentos e recursos computacionais que estão a uma curtíssima distância, como por exemplo: tablets, smartphones, IoT, dentre outros. Ou seja, dispositivos que estão a pequenos metros de separação entre eles. As taxas de transmissão são menores e as tecnologias utilizadas são: bluetooth, USB, RFId.
- SAN (*Storage Area Network*) traduzida como Rede de Área para Armazenamento, trata-se de uma rede criada exclusivamente para interconexão de dispositivos de armazenamento de dados, possibilitando assim um local seguro no qual dados são

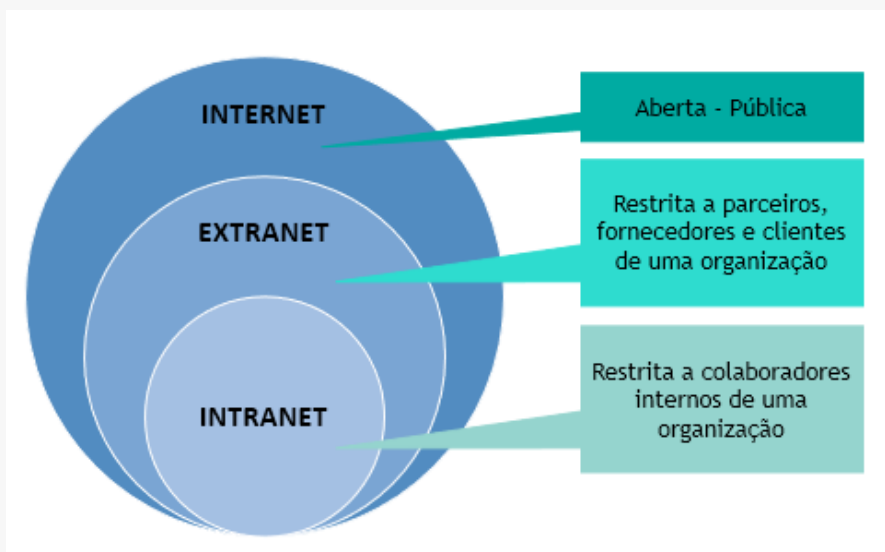
armazenados e distribuídos entre um servidor e demais dispositivos de rede, por exemplo.

- VLAN (*Virtual Local Area Network*) traduzida como Rede de Área Local Virtual, trata-se de um tipo de rede construída sob a forma lógica e não física. Essa construção permite a divisão (segmentação) de uma rede do tipo LAN em diferentes redes virtuais. Quanto aos demais detalhes, tais como taxa de transmissão, tecnologia e outros, são as mesmas de uma rede do tipo LAN.

Ainda com relação a classificação das redes, os mesmos conceitos apresentados aqui, meu jovem Padawan, podem ser aplicados as redes de computadores sem fio. Neste sentido, teremos então as redes do tipo: WLAN, WMAN, WWAN e assim por diante.

Por fim, atualmente podemos ainda classificar as redes de computadores de acordo com o seu formato de acesso. Teremos então: (a) a Internet, que é considerada uma rede aberta a qualquer pessoa, organização ou entidade, ou seja, pública; (b) a Extranet, que é considerada uma rede restrita (privada) pertencente a uma organização ou entidade e que somente parceiros, fornecedores ou clientes dessa organização ou entidade podem acessar e, a (c) Intranet, no qual também é considerada uma rede privada, pertencente a uma organização ou entidade, no qual o acesso é restrito a somente áreas e colaboradores internos da organização ou entidade.

Figura 4 - Internet, Extranet e Intranet.



### Topologia das Redes de Computadores

Ao estudarmos a classificação das redes de computadores, observamos que elas são classificadas de acordo com a extensão e a abrangência geográfica. Porém, precisamos compreender a forma como elas se interconectam. Neste contexto é que entra a topologia, meus jovens Padawans!

Para que aconteça a interconexão entre os diversos equipamentos (computadores, switch, roteadores, impressoras etc.), é necessário que estes estejam conectados por algum meio físico. Essa conexão pode ser feita por meio de cabos ou por meio de sinais de rádio (wireless). De forma genérica, a topologia é a forma com a qual a estrutura de rede de computadores é representada.

Nesse cenário a topologia de uma rede de computadores poderá ser representada de forma física e/ou de forma lógica. Ou seja, teremos a denominada topologia de rede de computadores física no qual irá demonstrar como os dispositivos de rede estão conectados fisicamente, representado as estratégias utilizadas para a organização física, bem como a disposição do cabeamento e dos dispositivos/elementos da rede. Já a

topologia de rede de computadores lógica tem como objetivo organizar como a rede irá desempenhar seu trabalho. Ou seja, como essa rede irá endereçar os pacotes de dados, controlar os recursos disponíveis na rede, os acessos aos nós e dispositivos da rede, dentre outras questões que visam tornar a rede de computadores mais eficiente.

Atentando-se à topológica física, uma rede poderá ser constituída de diversas formas, dentre as quais destacam-se: topologia anel, topologia árvore, topologia barramento, topologia estrela, topologia híbrida, topologia malha e topologia ponto a ponto.

Todas as topologias apresentadas possuem suas características e são utilizadas de acordo com o projeto de rede a ser desenvolvido. Porém, todas têm o mesmo objetivo, representar da forma pela qual os elementos de redes estão interconectados. Ou seja, a visão física da organização da rede.

Outro ponto interessante com relação à topologia das redes é que algumas serão mais robustas e estáveis, porém, com um custo/investimento mais alto. Outras, por sua vez, serão mais acessíveis em termos de custos/investimento, porém, mais vulneráveis a falhas. Afinal, a definição da topologia física na qual a rede será construída terá como impacto direto custos relacionados a modelos de cabos de conexão, equipamentos de interconexão (switch, roteadores etc.), tipos de conectores etc.

Nesse sentido, definir a topologia física a ser utilizada na rede deve ser considerado um trabalho importante. Isso porque, caso seja escolhido uma topologia física complexa, quando bem concebida, a rede de computadores torna-se mais eficiente e eficaz na transmissão de dados. Porém, é importante lembrar que quanto maior for a complexidade dessa topologia física, maior será a dificuldade de realizar manutenções, principalmente por equipes que porventura não estão familiarizadas com o

projeto da rede e respectivamente com a topologia física utilizada por não estarem desde o começo no projeto.

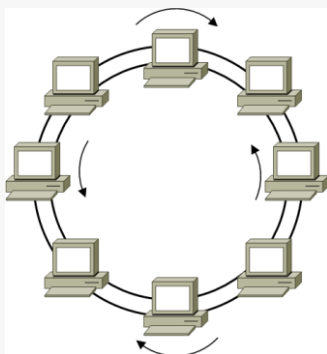
Bem, meus jovens Padawans, conforme observado, existem diversas topologias que podemos utilizar, vamos aqui apresentar as mais utilizadas pelas organizações e suas redes de computadores.

### Topologia ANEL

Também conhecida como topologia *ring*, é uma topologia que interliga fisicamente os dispositivos da rede em um mesmo círculo. Daí o nome “anel” que faz a analogia a um círculo. Nesse tipo de topologia, cada dispositivo terá pelo menos 2 outros dispositivos “vizinhos” no qual os dados poderão passar. Porém, o fluxo de dados acaba sendo unidirecional, ou seja, em uma única direção, o que pode por um lado ser uma “dor de cabeça” no caso de uma indisponibilidade de algum nó da rede.

Se por um lado temos o caso da indisponibilidade causada por um nó da rede que irá impedir que o pacote de dados siga o seu caminho, tornando assim uma desvantagem nesse tipo de topologia, por outro lado temos como vantagem a eficiência na transmissão de pacotes de dados. Isto porque, se todos os nós da rede estiverem em perfeito funcionamento, a topologia anel permite uma transmissão de pacotes de dados sem erros. Para sanar o problema de indisponibilidade provocado no caso de uma perda de um nó da rede, as empresas que utilizam esse tipo de topologia constroem 2 anéis, sendo que no primeiro anel os pacotes de dados são enviados em uma direção e o segunda anel os pacotes de dados são enviados na direção oposta, proporcionando assim a redundância dos anéis e da rede como um todo.

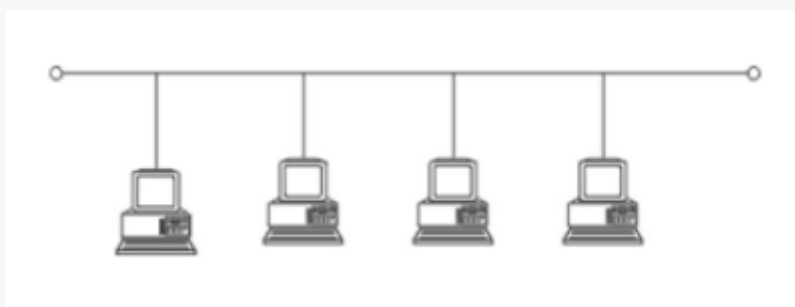
Figura 5 - Topologia Física ANEL (com redundância).



### Topologia BARRAMENTO

Considerada por muitos especialistas em redes de computadores a topologia física mais simples e prática de todas as outras. Também conhecida como “*bus*”, “*line*” ou “*backbone*”, nesse tipo de topologia os dispositivos são interconectados de forma paralela através de um único cabo, e os pacotes de dados são transmitidos de forma unidirecional. Como vantagem desse tipo de topologia temos os fatores custo (financeiro) e complexidade. Isso porque, para implementar uma topologia física do tipo barramento, não é necessários grandes investimentos e a complexidade com relação a organização e manutenção é baixíssimo, além da simplicidade na inclusão de novos dispositivos a rede. Mas essa facilidade e simplicidade oferecida possui um preço. Ou seja, similar a topologia física anel, no qual os pacotes de dados fluem em uma única direção, caso aconteça uma indisponibilidade de algum nó do barramento a rede inteira irá parar.

Figura 6 - Topologia Física Barramento.

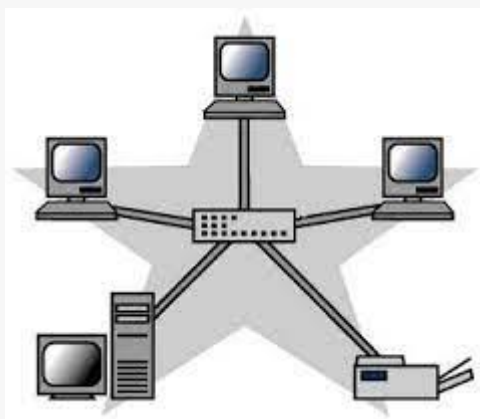




### Topologia ESTRELA

É considerada uma das topologias mais comuns e utilizadas em redes de computadores por priorizar a simplicidade. Essa topologia recebe o nome “estrela” em analogia de seu layout ser similar a uma estrela no qual existe a presença de um nó central que recebe os outros nós da rede, formando assim uma estrela. A vantagem mais significativa desse tipo de topologia é o gerenciamento. Isso porque cada conexão é independente e todas se conectam ao nó central. Temos também que citar como vantagem a tolerância a falhas, já que caso um nó qualquer da rede apresente uma falha ou indisponibilidade, este por sua vez não afetará em nada a rede. Afinal, o fluxo de dados é sempre exclusivo entre o nó central e os demais outros nós da rede. Porém, não podemos deixar de citar a principal desvantagem nesse tipo de topologia, que é justamente a existência de um nó central. Ou seja, todas as conexões passam e dependem desse nó central e, caso justo esse nó central falhe ou sofra alguma indisponibilidade, toda a rede será comprometida.

Figura 7 – Topologia Física Estrela.



### Topologia ÁRVORE

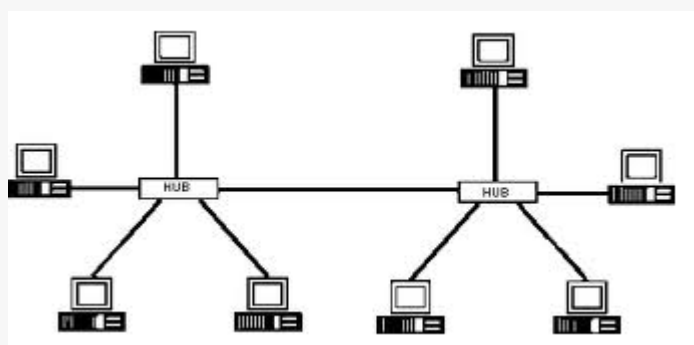
Nesse tipo de topologia, existe uma hierarquia na disposição dos nós da rede. Nesse caso há a presença de um nó central no qual os pacotes de dados irão partir e redistribuídos pelos outros nós da rede. Inicialmente,

como vantagem desse tipo de topologia, podemos citar a eliminação das vulnerabilidades presentes na topologia anel e barramento, incluindo a facilidade de identificação e reparo de erros, uma vez que se torna fácil a identificação do nó com falha.

Outra vantagem está relacionada ao layout da topologia, que por sua vez é considerado simples e prático pelos especialistas e oferece um crescimento contínuo na rede, facilitando a adição de novos nós de rede. Porém, como nas outras topologias, a topologia árvore também possui desvantagens. Sendo a mais significativa, a presença de nó central, que a exemplo da topologia estrela, caso aconteça alguma indisponibilidade a rede pode ficar off-line.

Por fim, outra desvantagem que podemos citar está relacionada ao custo de implementação. Isto porque a topologia árvore requer uma organização e layout mais detalhado, o que acaba aumentando os custos de implementação.

Figura 8 - Topologia Física Árvore.



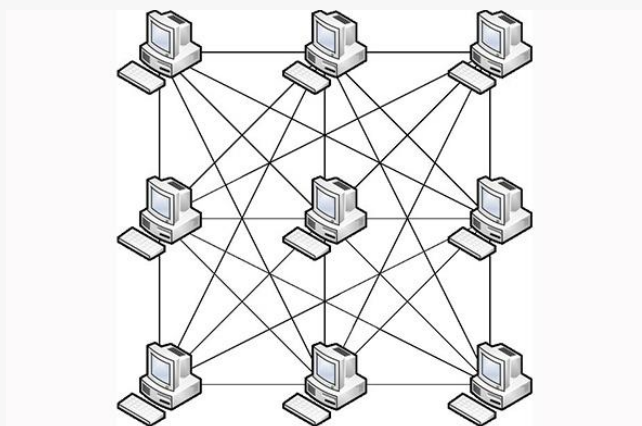
### Topologia MALHA

Definitivamente, seu ponto forte é a confiabilidade. Nesse tipo de topologia há um incentivo para que todos os nós sejam interconectados entre si, evitando assim erros na entrega dos pacotes. No geral, a topologia malha é utilizado em redes maiores. Porém, é aquele ditado, meu jovem Padawan, – quanto maior o número de nós/dispositivos conectados na

rede, maior será a complexidade de instalação, custo, operação, administração e manutenção.

Acredito que você deva ter percebido que na topologia malha as grandes vantagens são confiabilidade e escalabilidades. Se pensou assim, você está correto! Isso dá porque todos os nós/dispositivos estão conectados entre si, o que significa que uma falha de um ou mais nós da rede não irá derrubar a rede como um todo. Agora, o que talvez você não tenha percebido como vantagem é que como todos os nós/dispositivos estão interconectados entre si, haverá sempre um caminho “rota” alternativo pelo qual o pacote de dados poderá seguir para chegar ao seu destino. Mas temos também desvantagens! Como exemplo citamos a complexidade no momento do planejamento desse tipo de topologia, afinal, haverá diversos nós/dispositivos de rede que precisarão ser interconectados entre si e com diferentes pontos de interconexão, tornando assim a topologia complexa e com um custo financeiro alto de implementação.

Figura 9 - Topologia Física Malha.



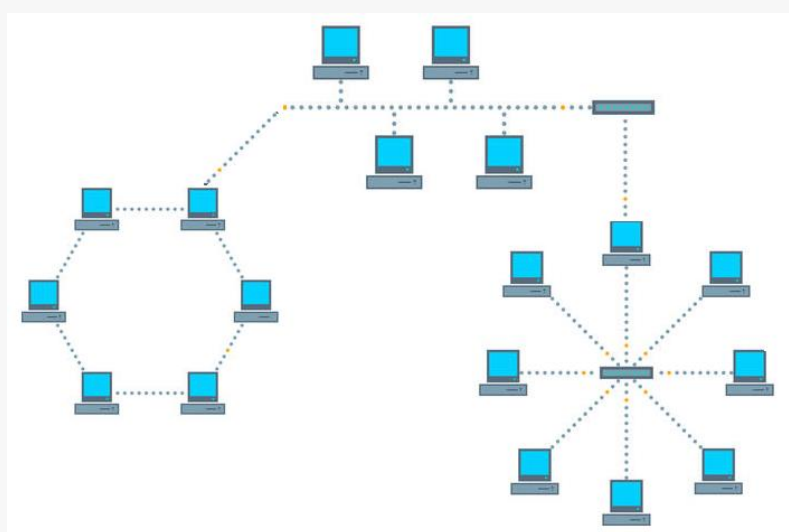
### Topologia HÍBRIDA

Como o nome sugere, nesse tipo de topologia há uma mistura de dois ou mais outros tipos de topologia de redes. Por esse motivo é sem dúvida o tipo de topologia mais utilizado no mercado e nas redes de

computadores. Como principal vantagem temos a flexibilidade e adaptabilidade. Afinal, nesse modelo de topologia o planejamento e organização de uma rede de computadores passa a ser flexível e adaptável, não só na possibilidade de mesclar os outros tipos de topologia, mas também de possibilitar o crescimento da rede, aproveitando todo o investimento já realizado anteriormente.

Mesmo sendo a topologia preferida e utilizada pela maioria das redes de computadores, a topologia híbrida apresenta como desvantagem a complexidade. Isto porque, mesmo sendo considerada uma solução prática para integrar diversas outras topologias já existentes no ambiente, toda nova integração exigirá muito planejamento, atenção e experiência dos analistas de redes ou equipes de TI envolvidas na organização da rede.

Figura 10 - Topologia Física Híbrida.



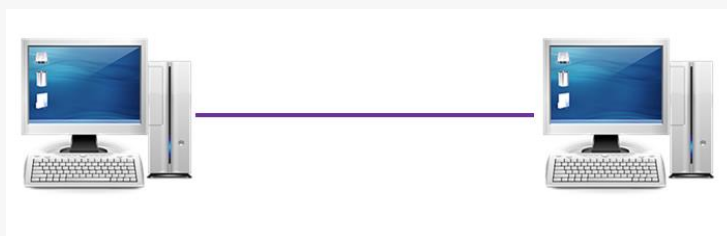
### Topologia PONTO A PONTO

Temos aqui a mais simples de todas as topologias de redes de computadores apresentadas. Como o próprio nome sugere, nesse tipo de topologia a interligação é realizada ponto a ponto, ou seja, dispositivo a dispositivo. Devido a essa extrema simplicidade, a topologia ponto a ponto é considerada a alternativa mais popular quando se trata de redes de

computadores em ambientes domésticos, residenciais ou qualquer outro ambiente que necessite de uma interligação rápida entre dois dispositivos.

Percebe-se que a topologia ponto a ponto é ideal para interligar 2 dispositivos e promove uma comunicação rápida entre ambos os pontos conectados. Porém, lembre-se que esse layout ou cenário “ponto a ponto” é indicado para interligar apenas 2 dispositivos e, nesse contexto, quando se trata de redes com um número maior de nós/dispositivos a topologia ponto a ponto se torna inadequada.

Figura 11 - Topologia Física Ponto a Ponto.



### Comunicação e Transmissão de Dados

Conforme podemos observar até aqui, meus jovens Padawans, uma rede de computadores será um ambiente no qual haverá vários recursos computacionais espalhados em várias localizações. Ou seja, será um ambiente distribuído. Nesse caso há a necessidade explícita de que esses vários recursos computacionais se comuniquem entre si e, sendo assim, temos então a necessidade de um sistema de comunicação que permita essa interação.

Podemos então pressupor que um sistema de comunicação será então o mecanismo de distribuição para que possa ser realizado não só a troca de dados e informações, mas também todo o controle, e neste ponto é indispensável a existência de uma rede física para realizar toda essa interligação.

No campo da ciência, a comunicação de dados é compreendida como uma disciplina da área da ciência da computação que trata da

transmissão de informações entre diferentes dispositivos/sistemas computacionais através de um meio de transmissão. Já a transmissão de informações é compreendida como a passagem de sinais através de meios físicos de comunicação que compõe as redes de computadores.

Um sistema básico de comunicação de dados é composto por cinco elementos. São eles:

- Mensagem – trata-se da informação (conjunto de dados) a ser transmitido entre um emissor e um ou vários receptores. É considerado o objeto “central” de qualquer tipo de comunicação de dados, estabelecidos entre duas ou mais partes, podendo ser constituído de texto, número, figura, áudio, vídeo e/ou qualquer outro tipo de dados, seja de forma pura ou combinada.
- Transmissor ou emissor – é compreendido como quem “emite” ou “envia” a mensagem para um ou mais receptores. Pode ser: uma pessoa, um grupo de pessoas, um dispositivo ou sistema computacional. As duas principais funções de um transmissor ou emissor é: (a) realizar a codificação da mensagem no formato ideal ao meio ou canal de comunicação – ex. digital, analógico etc., e; (b) transmitir a mensagem no meio ou canal de comunicação.
- Receptor – trata-se de quem recebe a mensagem. Podendo ser também uma pessoa, um grupo de pessoas, um dispositivo ou sistema computacional. A principal função do receptor é a de decodificar e interpretar a mensagem recebida para o formato original e compreensível.
- Meio físico ou canal de comunicação – trata-se do caminho físico ou virtual pelo qual a mensagem foi transmitida. Esse

meio físico ou canal de comunicação poderá ser de diversos tipos, como por exemplo: fibra óptica, rádio frequência ou virtualmente. As principais funções de um meio físico ou canal de comunicação são: interligar o emissor ao receptor(es) e realizar o transporte da mensagem com os seus respectivos protocolos de comunicação.

- Protocolo – pode ser compreendido como o conjunto de regras padronizadas, que tem como objetivo realizar o controle da comunicação entre o transmissor e o receptor, ou ainda como o conjunto de instruções e padrões necessários e utilizados para que exista a comunicação entre dois ou mais sistemas de comunicação. Dentre as suas funções, as principais são: garantir a eficiência da comunicação entre os pontos; evitar erros ou perda de mensagens durante o processo de transmissão ou comunicação de dados e, por fim, realizar todas as correções na transmissão da mensagem, quando necessárias.

Aprofundando nos conceitos relacionados a protocolos, eles podem ser classificados em duas categorias, que por sua vez estão associadas diretamente ao tipo de controle a ser estabelecido durante a transmissão da mensagem. Sendo assim, temos: (a) protocolos orientados para a conexão – que são protocolos que realizam um controle na transmissão das mensagens durante todo o processo de comunicação estabelecido e existente entre o transmissor e o receptor. Esses controles são realizados por meio de “avisos” que confirmam ou não a entrega da mensagem ao receptor, possibilitando assim o transmissor validar não só o envio da mensagem, mas também a confirmação de recebimento por parte do receptor. Como exemplo citamos o protocolo TCP; (b) protocolos não orientados para a conexão – nesse caso, não há nenhum tipo de controle

na transmissão da mensagem. Ou seja, o transmissor envia a mensagem e não fica sabendo se o receptor recebeu ou não. A transmissão das mensagens que utilizam esse tipo de protocolo é realizada em blocos denominados “datagramas”. Como exemplo citamos o protocolo UDP.

É importante ressaltar que o protocolo define apenas a maneira pela qual o transmissor e o receptor devem se comunicar. Ou seja, definem apenas a “forma” e a “sequência” das mensagens a serem trocadas entre ambos os lados. Outro ponto importante a ser lembrado é que para que uma aplicação utilize um protocolo, esta deverá realizar a tradução do protocolo utilizado em linguagem de máquina.

Com relação à transmissão de dados, esta poderá ocorrer de três modos:

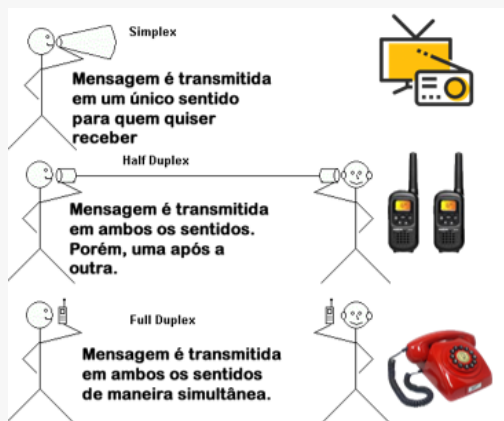
(1) transmissão de dados – SIMPLEX, nesse modo a mensagem ocorre em um único sentido, ou seja, UNIDIRECIONAL (transmissor → receptor) e este papel não se inverte nunca durante o processo de comunicação. Como exemplo desse modo de transmissão citamos o rádio AM/FM e a televisão;

(2) HALF DUPLEX, nesse modo a mensagem ocorre em ambos os sentidos, porém, nunca de maneira simultânea, ou seja, as transmissões são BIDIRECIONAIS, mas por compartilharem o mesmo canal de comunicação, o envio e o recebimento não são realizados simultaneamente. Como exemplo citamos os rádios de comunicação, também conhecidos como Walk-Tocs;

(3) FULL DUPLEX, nesse modo a mensagem também ocorre em ambos os sentidos, porém, são realizadas de forma simultânea, sendo então BIDIRECIONAIS com envio e recebimento ao mesmo tempo. Como exemplo, citamos as linhas de telefone e as redes de computadores.

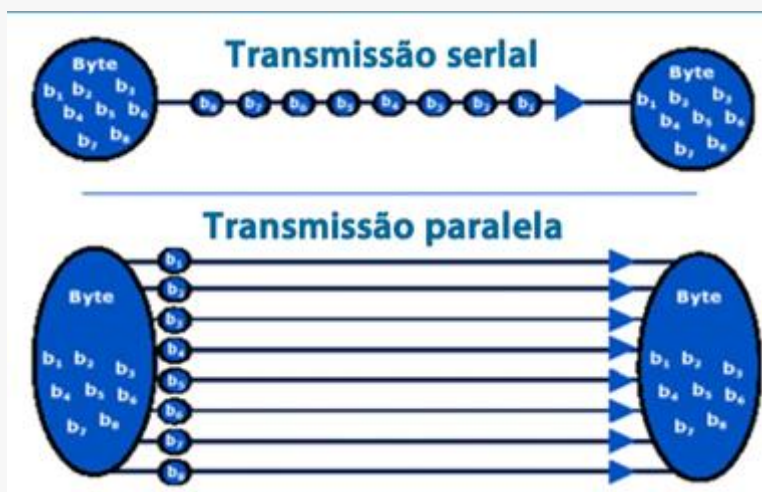


Figura 12 - Modos de Transmissão de Dados.



Além dos modos de transmissão mencionados, as transmissões também podem ocorrer de forma SERIAL, onde os dados são enviados um a um, e PARALELA, onde os dados são enviados simultaneamente.

Figura 13 - Transmissão Serial vs. Paralela.

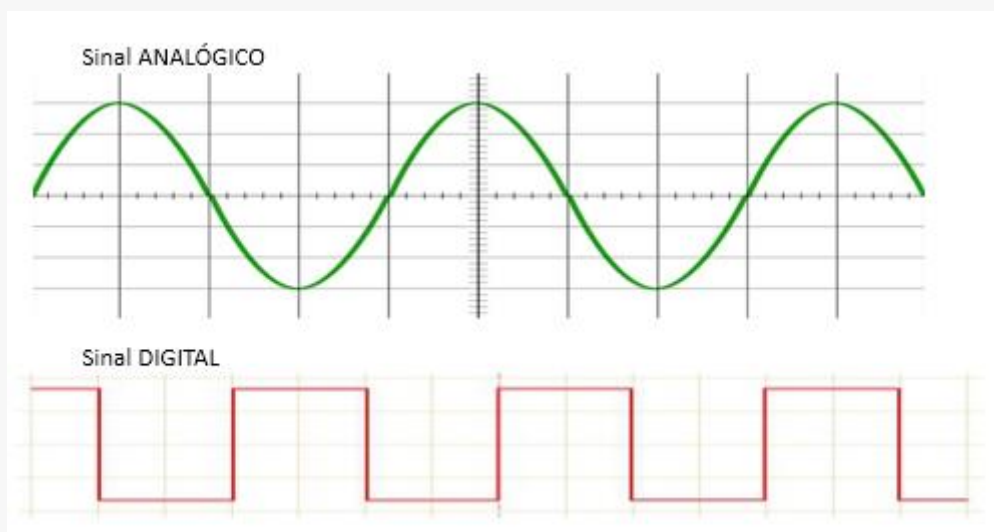


Com relação à transmissão serial vs. paralela, temos como principal vantagem no modo paralelo a rapidez. Já no modo serial a confiabilidade.

No quesito formato de transmissão de dados, os modos serão (a) ANALÓGICO – no qual não há uma ocorrência de variação do sinal em uma de suas dimensões, ou seja, não há uma constante variação de suas ondas dimensionais. Como exemplo citamos o som e a luz; (b) DIGITAL, no qual o formato é do tipo não contínuo. Isso significa que há uma variação no sinal.

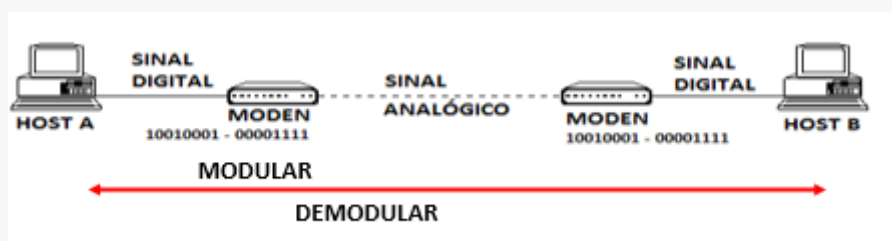
Por exemplo, em uma rede de computadores, dizemos que está transmitindo sinal ou não. Isso é representado por um código de dois símbolos (0) e (1), conhecidos como dígito binário ou simplesmente bit, onde (1) representa a presença de corrente elétrica (sinal) e (0) representa a ausência de corrente elétrica (sinal).

Figura 14 - Sinal Analógico vs. Digital.



Com relação ao processo de conversão de um sinal DIGITAL para ANALÓGICO, denominamos de MODULAÇÃO, e o processo inverso de DEMODULAÇÃO. A modulação ou demodulação de sinais digitais para analógicos, e vice-versa, é realizada por um dispositivo denominado MODEM.

Figura 15 - Processo de Modulação e De Modulação – MODEM.



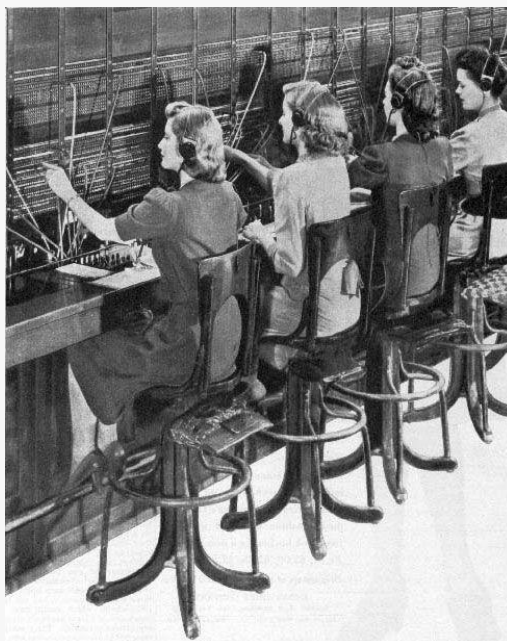
## Comutação de Dados

Antes da criação das redes de computadores, existiam as redes de telecomunicações, que por sua vez não eram interligadas entre si. Nesse contexto, a necessidade de estabelecer formas capazes de realizar a interligação entre essas redes de telecomunicações existentes se tornou cada vez mais imprescindível e primordial na época.

Como resultado dessa necessidade, foram criadas as REDES COMUTADAS, que tinham como principal objetivo realizar a interligação e interconexão das redes de telecomunicações distintas e existentes na época.

COMUTAÇÃO significa troca ou substituição. No passado, a comunicação era realizada de forma manual, no qual havia a presença de uma pessoa “telefonista” que tinha a função de interligar manualmente as redes de telecomunicações fisicamente através de um painel e cabos, realizando assim o fechamento de um ponto de comunicação a outro. Porém, acredito que vocês já devem ter percebido que essa forma não era nada eficiente!

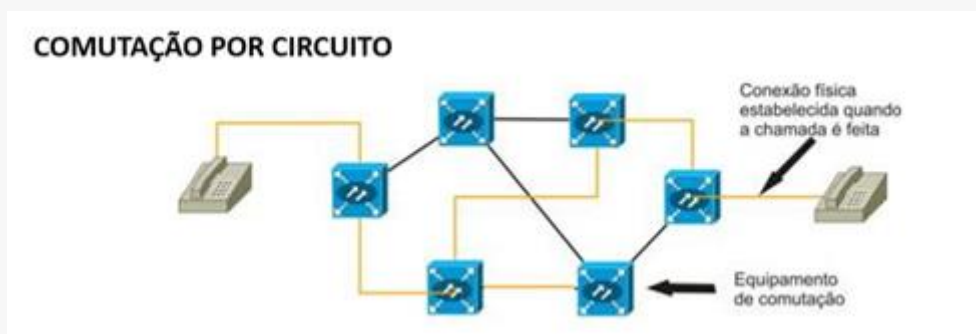
Figura 16 - Telefonistas realizando a comutação em 1943.



Com a evolução das telecomunicações e a entrada de novos conceitos tecnológicos, a interligação realizada manualmente pelas telefonistas passou a ser realizada de forma automática, por meio das centrais telefônicas. Isso criou uma forma mais eficiente de comutar as ligações telefônicas.

A comutação de dados pode ser realizada de duas formas, sendo a primeira conhecida como **COMUTAÇÃO POR CIRCUITO**, onde os pontos que vão se comunicar precisam de um caminho específico, dedicado e exclusivo, que geralmente são realizados por circuitos físicos ou através da criação de circuitos virtuais do tipo FDM – sigla para a divisão em canais de frequência ou TDM – sigla para divisão em canais por tempo.

Figura 17 - Comutação por Circuito.



A segunda forma é conhecida como **COMUTAÇÃO POR PACOTES**, nessa forma não há a necessidade de haver circuitos dedicados, ou seja, não é preciso haver uma ligação única, dedicada e exclusiva para haver a comunicação entre a origem e o destino. Isso apresentou como resultado a redução dos custos operacionais e financeiros com relação ao meio físico se comparados com os custos existentes para manter esses meios físicos exigidos na comutação por circuito.

A comutação por pacote pode ser implementada de duas formas. A primeira realizada por circuitos virtuais, em que cada comutador grava uma tabela na qual contém as identificações de cada circuito e

respectivamente o caminho (rota) por onde os pacotes deverão seguir; a segunda por meio de datagramas, no qual os pacotes são enviados por caminhos (rotas) diferentes de acordo com uma tabela de roteamento presente em cada comutador.

Além da questão de “ser ou não” dedicado o meio de comunicação, a comutação por circuito e a comutação por pacotes possuem outras diferenças, tais como: (a) a configuração da chamada; (b) a forma pela qual os dados ou pacotes são enviados; (c) a tolerância a erros e falhas; (d) o tratamento com relação a congestionamentos existentes no meio de comunicação e, (e) o formato de tarifação (valor cobrado) entre o modo de comutação.

Observando as diferenças existentes entre ambas (por circuito e por pacote) percebe-se que na comutação por circuito temos uma garantia que os pacotes chegarão ao seu destino. Isto devido ao caminho ser “dedicado e exclusivo”. Porém, essa “exclusividade” consome recursos e possui um custo financeiro e operacional alto. Já no caso da comutação por pacotes, há um menor consumo de recursos e um menor custo financeiro e operacional, justamente pelo fato de não haver um caminho “dedicado e exclusivo”. Porém, não há a garantia que os pacotes chegarão ao seu destino, meus jovens Padawans!

### Conhecendo o Jargão das Redes de Computadores

É importante que você, meu jovem Padawan, conheça os jargões utilizados nas redes de computadores. Esse conhecimento facilita o entendimento e a compreensão das redes. Sendo assim, vamos conhecer alguns dos mais utilizados.

JARGÃO	SIGNIFICADO
AGENTE	Programa ou processo de computador que opera sobre uma aplicação cliente ou servidor, realizando uma função específica.

ALIAS	Apelido ou segundo nome. Utilizado para referenciar, por exemplo, um endereço IP, um apelido para um dispositivo etc., também é um dos comandos básicos de um sistema operacional UNIX ou LINUX.
APLICAÇÃO	Programa que utiliza serviços ou recursos de uma rede de computadores.
BACKBONE	Interconexão central de uma rede de computadores. Pode ser compreendida como a “espinha dorsal” de uma rede, na qual todas as conexões estão interligadas. No geral um backbone possui altas taxas de transmissão e podem realizar o tráfego de grandes quantidades de dados de qualquer tipo.
BAUD RATE	Medida de taxa de transmissão elétrica de dados em uma linha de comunicação – vide bps.
BPS	Medida da taxa de transferência real de dados de uma linha de comunicação. É referenciada em bits por segundo. Variantes incluem: Kbps (= 1.000 bps), Mbps (= 1.000.000 bps) e Gbps (= 1.000.000.000 bps).
BRIDGE	Dispositivo que tem a função de conectar duas ou mais redes. Pode ser compreendido como repetidor ou ponte.
CLIENTE	Processador ou programa de computador que solicita serviços ou recursos a um servidor de rede.
DATAGRAMA	Pacote de informação e dados complementares.
DIAL-UP	Método de acesso via rede telefônica convencional a um computador remoto.
DOMÍNIO	Trata-se de uma parte da hierarquia de nomes da Internet (DNS), utilizado para identificar uma entidade na rede.
DNS	<i>Domain Name System</i> – trata-se de um serviço e um protocolo da família TCP/IP que tem como função armazenar e prover consultas a informações sobre recursos da rede.
DOWNLOAD	Processo de transferência de um arquivo em um computador remoto para um computador local através da rede.
ETHERNET	Padrão utilizado em conexões físicas de redes de computadores LAN.
FDDI	Padrão utilizado em conexões físicas de redes de computadores por meio de cabos de fibra óptica.
FIREWALL	Dispositivo de segurança de borda presente nas redes de computadores, que tem como função controlar o tráfego de entrada e saída entre a rede WAN e a rede LAN, podendo exercer outras funções relacionadas à segurança cibernética, tais como: detecção e prevenção de intrusão a

	rede, controle de acesso remoto via rede virtual privada (VPN), dentre outros.
FTP	Protocolo padrão utilizado em redes de computadores para a transferência de arquivos entre computadores.
GATEWAY	Sistema que permite o intercâmbio de serviços e recursos entre redes de computadores.
HOST	Nome dado ao computador conectado à rede ou à Internet.
HTML	Linguagem de programação padrão para desenvolvimento de páginas na WEB (WWW).
HTTP	Protocolo pertencente a pilha TCP/IP, que permite acessar hipertextos e páginas desenvolvidas para a rede ou Internet. Podendo esse possuir uma variante para estabelecer conexões seguras (HTTPS).
IP	Protocolo responsável por realizar o endereçamento e roteamento de host e pacotes entre aplicações na rede ou Internet. Pertence a pilha de protocolos TCP/IP.
ISO	Organização internacional formada por diversas entidades de vários países que tem como missão propor padrões para protocolos de rede. O padrão mais conhecido é o modelo conceitual de arquitetura de redes OSI.
NFS	Protocolo desenvolvido pela SUN Microsystems que permite o compartilhamento de arquivos entre host em uma rede de computadores.
NIS	Trata-se de um sistema distribuído de base de dados que troca cópia de arquivos de configuração.
NÓ	Qualquer dispositivo computacional conectado a uma rede de computadores.
NOC	Centro de operações de redes, sua função é a de realizar o gerenciamento dos aspectos operacionais de uma rede, tais como controle de acesso, roteamento, monitoramento de links de comunicação etc.
PACOTE	Dado encapsulado para transmissão em uma rede de computadores.
PING	Programa utilizado para realizar testes de conectividade e alcance de uma rede de computadores através do protocolo ICMP.
POP	Ponto de presença de uma rede de computadores. Atenção, não confunda PoP com POP. Este último é um protocolo pertencente a pilha



	TCP/IP utilizado por clientes de correio eletrônico para manipulação de mensagens (e-mail).
PORTA	Abstração utilizada pela pilha TCP/IP para designar conexões simultâneas em um único host. Pode ser compreendido como um canal físico de entrada ou de um host.
PPP	Protocolo pertencente a pilha TCP/IP, utilizado para realizar conexões via interfaces serial e MODEM.
PROVEDOR DE ACESSO	Entidade responsável em prover o acesso à rede mundial de computadores – Internet.
REPETIDOR	Dispositivo computacional que tem como objetivo propagar por meio da regeneração e amplificação os sinais elétricos em uma conexão de dados.
RFC	Trata-se de uma série de documentos que descrevem aspectos relacionados com as redes e a Internet, tais como: padrões, protocolos, serviços etc.
ROTEADOR (ROUTER)	Dispositivo computacional que tem como objetivo encaminhar pacotes de comunicação de dados entre redes distintas através da escolha das melhores rotas e de uma tabela de roteamento.
SERVIDOR	Sistema computacional responsável por prover serviços e recursos solicitados por clientes em uma rede de computadores.
SNMP	Protocolo pertencente a pilha TCP/IP que tem como objetivo monitorar e controlar serviços e dispositivos em uma rede TCP/IP.
TCP/IP	Trata-se de um conjunto de protocolos (ou pilha de protocolos) utilizados para a comunicação de dados inter-redes, proposto pela ARPA e utilizado na ARPANET. Atualmente é o padrão utilizado em redes de computadores e na Internet.
TRANSCEIVER	Dispositivo computacional utilizado para a conexão física de um nó a uma rede LAN.
URL	Trata-se de um localizador que permite identificar e acessar um serviço ou recurso na rede ou na Internet.
WHOIS	Banco de dados que contém informações sobre domínios, redes, hosts e pessoas na Internet. Trata-se de um serviço de diretórios da Internet.
WWW	Meta-rede, baseado em hipertextos que realiza a integração de diversos serviços e recursos disponíveis na Internet, que possibilita ainda o acesso a informações multimídia.



Bem, jovens Padawans, apresentamos a vocês alguns dos jargões mais utilizados pela comunidade de analistas, pesquisadores, estudiosos e entusiastas de redes de computadores. Porém, vale ressaltar que isso é apenas uma pequena parte de um glossário enorme de palavras, nomenclaturas e jargões utilizados na galáxia das redes de computadores e na Internet.

### Entidades de Padronização

Desde os primórdios das redes de telecomunicações, da informática, da computação e das redes de computadores, as entidades de padronização exerceram e exercem um papel importantíssimo e fundamental para a criação e o estabelecimento de padrões e melhores práticas para a criação de dispositivos computacionais, modelos de arquiteturas, normas, redes de computadores e muito mais.

No geral, as entidades de padronizações são instituições formadas por estudiosos, pesquisadores, cientistas, analistas, engenheiros, organizações privadas e governamentais, entusiastas de tecnologias, entre outros de diversos países que, como mencionado anteriormente, reúnem conhecimentos para promover a criação, adoção e disseminação de padrões, normas, regras, frameworks, arquiteturas e melhores práticas voltadas a diversas áreas, tais como: engenharia elétrica, indústria, eletrônica, computação, redes etc.

Na disciplina redes de computadores, as entidades mais relevantes são:

SIGLA	ENTIDADE
ISO	<i>International Standards Organization</i>

ANSI	<i>American National Standards</i>
IEEE	<i>Institute of Electrical and Eletronics Engineers</i>
ITU-T	<i>International Telecommunications Union</i>
EIA	<i>Eletronic Industries Association</i>
TIA	<i>Telecommunications Industry Association</i>
ABNT	<i>Associação Brasileira de Normas Técnicas</i>



**XP**e

## > Capítulo 2



## Capítulo 2. Arquitetura e Padrões de Redes de Computadores

---

Se você, jovem Padawan, chegou até aqui, deve ter percebido que as redes de computadores não são apenas equipamentos computacionais ligados a cabos que realizam a troca de mensagens. Muito pelo contrário, as redes de computadores são sistemas complexos, compostos por muitas partes, com diferentes dispositivos interconectados, através de vários tipos de enlaces, organizadas e classificadas de diversas formas e tipos diferentes. E tudo isso a todo momento compartilhando aplicações, sistemas e recursos, trocando dados e informações, por meio de uma pilha de protocolos de comunicação e através de meios (canais) de comunicação físicos ou virtuais comutados por pacotes em sinais digitais (em alguns casos raros – sinais analógicos). Ufa!!!!

Por isso tudo e muito mais é que precisamos organizar as redes de uma maneira estrutural. E é aí que entra a “arquitetura de redes”, que visa: (a) reduzir a complexidade existente nas redes de computadores; (b) definir, distribuir e organizar os protocolos de redes e os meios de comunicação; (c) implementar uma modularidade de transporte em camadas para a comunicação de dados na rede de computadores.

Diante do contexto apresentado, o primeiro passo de toda essa organização é a separação de toda a arquitetura da rede em camadas. Essa separação em camadas permite a implementação de serviços, mecanismos e funcionalidades específicas, além da modularização, manutenção e atualização de todo o sistema de redes de computadores.

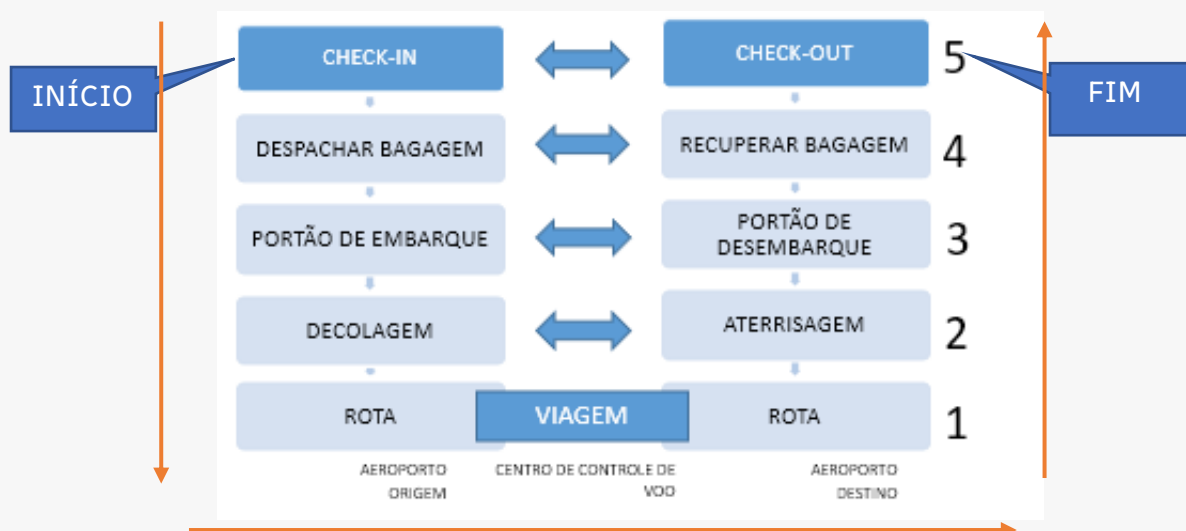
O legal disso tudo é que a modularização em camadas permite realizar todas as implementações e/ou modificações de serviços e recursos da rede de forma restrita e segmentada, sem que uma implementação ou alteração realizada em uma camada específica altere ou danifique serviços, recursos ou funcionalidades presente nas outras demais camadas.

Para compreendermos melhor, meu jovem Padawan, a modularização de camadas em uma rede de computadores, vamos fazer uma analogia à realização de uma viagem de avião.

Na analogia em questão, durante uma viagem de avião, hipoteticamente falando, vamos ter 5 processos, sendo eles: 5) check-in no aeroporto; 4) despacho da bagagem; 3) a ida até o portão de embarque do voo; 2) decolagem do avião e, por fim, 1) rota do voo.

Observe que os itens expostos acima referem-se apenas ao processo de ida, temos que também mapear o processo de volta, que no caso seria o inverso da ida. Vamos lá... 1) rota do voo; 2) aterrissagem do avião; 3) portão de desembarque; 4) recuperação das bagagens despachadas e, por fim, o 5) checkout. Bem, neste contexto toda apresentado, vamos transformar cada uma das etapas em camadas. Observe como ficará (figura 18):

Figura 18 - Processo / Camadas.



Conforme você pode observar, há uma lógica que você terá que seguir. Ou seja, há uma sequência ou caminho que deverá ser seguido por você para que seja concluído todo o processo de sua viagem. E esse caminho começa quando realiza o check-in (camada 5) e que te faz seguir

adiante (ou melhor – descendo) em cada camada. Ex.: 5,4,3,2,1 → 1,2,3,4 e 5.

Bom, supondo que os passageiros no momento do embarque sejam separados por ordem de idade pela cia aérea, qual camada deve ter seus serviços modificados?

Se sua resposta, jovem Padawan, foi a camada 3, está correto! Daí você percebe que as demais camadas continuam inalteradas. Ou seja, a modificação realizada no serviço contido na camada 3 não afeta em nada as demais camadas. É esse justamente o princípio da arquitetura em camadas de uma rede de computadores!

Esse modelo de arquitetura em camadas proporciona, como mencionado anteriormente, a modularização da rede e a facilidade da compreensão das complexidades existentes na mesma. Possibilitando assim que os mais diversos e variados dispositivos, tecnologias, serviços e recursos de inúmeros fabricantes e desenvolvedores possam ser implementados nas redes de computadores. Ou seja, permite a INTEROPERABILIDADE, que, como definição, é a capacidade de um sistema (seja ele informatizado ou não) de se comunicar de maneira transparente ou o mais próximo disto, com outro sistema similar ou não.

No contexto apresentado, podemos, então, meu jovem Padawan, compreender que a interoperabilidade criada pela arquitetura em camadas permite que uma rede de computadores, e respectivamente todos os elementos contidos nela, se comunique de forma transparente com outras redes, independente se ambas as redes são semelhantes ou não.

Eis aí o “boom” das redes de computadores. Ou seja, foi justamente a interoperabilidade advinda do conceito proposto na arquitetura em camadas que possibilitou o crescimento e a expansão das redes de computadores. Isso porque, antes do conceito de arquitetura em camadas,

as redes de computadores – no início da computação e das primeiras redes - eram proprietárias, fazendo com que as empresas ficassem reféns e à mercê de uma única tecnologia desenvolvida por um único fabricante.

É fato que a interoperabilidade foi sem dúvida um ponto decisivo na tecnologia computacional, pois possibilitou não só o funcionamento de forma transparente de diversos tipos de redes de fabricantes e tecnologias diferentes, mas também toda a computação, sistemas de informação e por que não dizer toda a tecnologia da informação?!

### Arquitetura – Modelo de Referência OSI

O modelo de referência OSI é um modelo que tem como objetivo fornecer uma estrutura conceitual, que descreve as funções de um sistema de rede ou de telecomunicação. Ou seja, seu propósito é o de servir como um modelo padrão para protocolos de comunicação entre vários sistemas, possibilitando a interoperabilidade e a comunicação de dados entre os mais diversos e variados sistemas computacionais presentes em uma rede de computadores.

Vale lembrar que inicialmente a computação tinha como base grandes computadores que eram conhecidos como “*mainframes*”. Eles eram ligados a terminais que possuíam uma única função, servir como entrada (*input*) e saída (*output*) de dados.

Todo o processamento de dados era realizado no computador central, ou seja, no mainframe, e os terminais de entrada/saída eram dessa maneira conhecidos como “terminais burros”, isto porque não possuíam nenhum poder de processamento e eram interconectados por meio de uma rede local de comunicação de dados ao mainframe.

Com o desenvolvimento de novas tecnologias computacionais por parte de diversos desenvolvedores e fabricantes, que possibilitaram “bombar”, vamos dizer assim, os terminais burros, transformando-os

computadores com poder de processamento e o aumento contínuo do número de pessoas (usuários) e empresas utilizando cada vez mais esses novos e diversos dispositivos computacionais, a necessidade de realizar a interconexão entre esses diversos dispositivos dos mais variados desenvolvedores e fabricantes fez com que se buscasse novas tecnologias e formas de interligar a comunicação de dados.

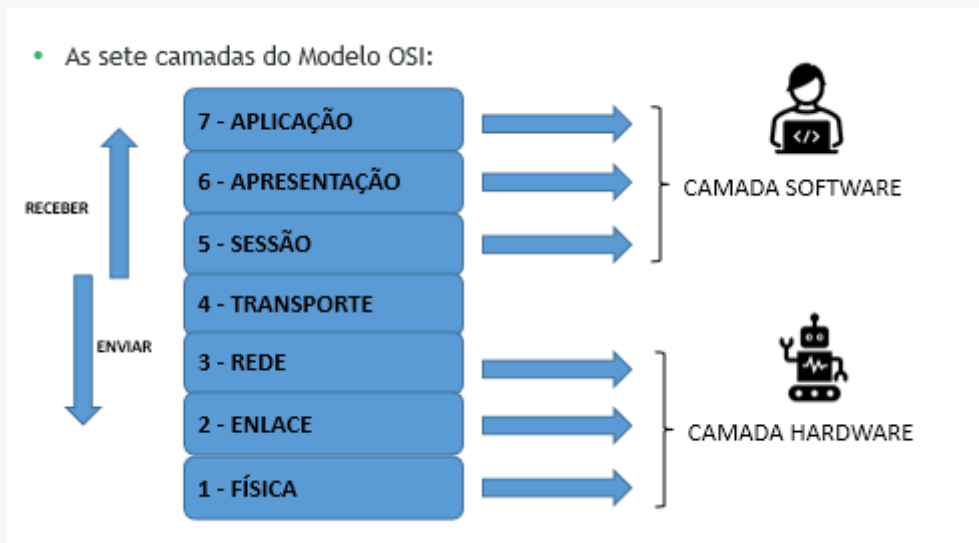
Eis que no meio dos anos 80, a ISSO, que até hoje é considerada uma das maiores entidades de padronização do mundo, publicou um modelo de referência de interconexão de sistemas abertos, no qual carinhosamente a comunidade chamou de modelo de referência OSI.

Atualmente, o modelo OSI é utilizado para fins educacionais. Porém, no ato de sua concepção, seu objetivo principal era o de servir como uma base sólida para o estabelecimento e desenvolvimento de um conjunto amplamente adotado de protocolos conhecidos como “OSI PROTOCOL SUITE” que poderia ser utilizado por qualquer fabricante ou desenvolvedor de sistemas computacionais que permitia fazer com que qualquer dispositivo ou sistema computacional pudesse se comunicar a outros dispositivos e sistemas diferentes em uma rede de computadores. Promovendo assim a interoperabilidade de todo o ecossistema existente.

O modelo de referência OSI é uma arquitetura composta por 7 (sete) camadas, definidas a partir dos seguintes princípios: (a) cada camada possui um nível de abstração separado; (b) cada camada executa uma função definida; (c) as camadas são definidas para criar protocolos padronizados; (d) as camadas facilitam a comunicação na infraestrutura e nos aplicativos e, por fim, (e) cada camada corresponde a uma função específica na comunicação de dados em uma rede de computadores. Desse modo o modelo de referência OSI desenvolvido pela ISO ficou assim:



Figura 19- Modelo de Referência OSI/ISSO.



Ao observarmos o modelo OSI, percebemos que haverá uma espécie de divisão entre as camadas, no qual iremos ter um conjunto de camadas mais próximas do hardware e um outro conjunto de camadas mais próxima do software.

Vamos agora compreender qual a função das 7 (sete) camadas do modelo de referência OSI/ISO, começando da camada mais próxima de nós seres humanos (usuários) e descendo até a última camada, mais próxima das máquinas.

CAMADA	DESCRIÇÃO/FUNÇÃO
(7) APLICAÇÃO	<i>Trata-se da camada mais próxima do usuário e tem como objetivo prover a interface entre a aplicação e a rede, bem como o controle dos serviços e protocolos.</i>
(6) APRESENTAÇÃO	<i>Também denominada como camada de tradução, sua função é a de formatar os dados para que estes possam ser transmitidos na rede. Outras funções tais como: criptografia, descriptografia e compressão de dados são também realizados nessa camada.</i>
(5) SESSÃO	<i>Essa camada tem a responsabilidade por estabelecer, gerir a manutenção e o controle da conexão. Isso inclui os processos de autenticação de sessões estabelecidos pelas aplicações, o sincronismo e o encerramentos das conexões.</i>

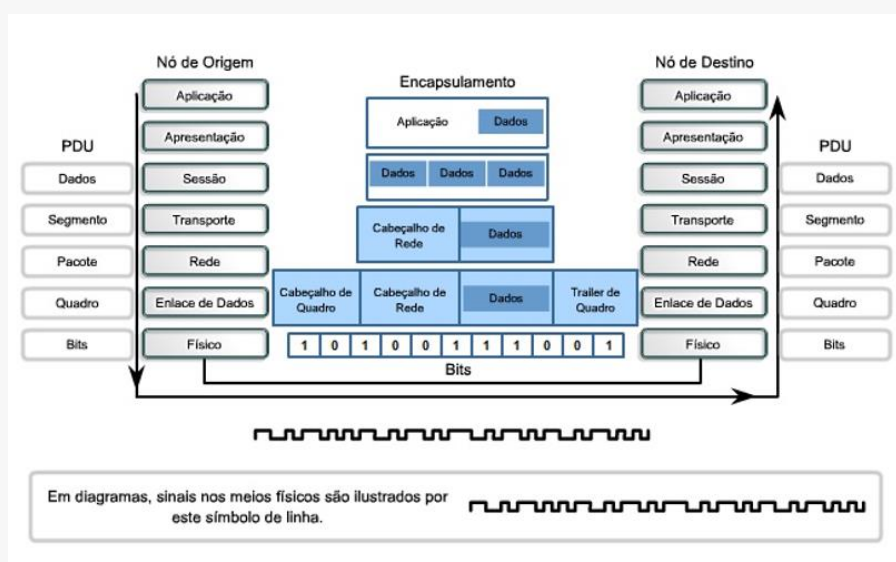
(4) TRANSPORTE	<i>Camada responsável por realizar todos os serviços de comunicação de dados, incluindo a entrega do pacote fim a fim entre a origem e o destino. Durante a realização desses serviços a camada de transporte realiza a segmentação dos pacotes de dados e o controle de fluxo e erros.</i>
(3) REDE	<i>Essa camada tem como responsabilidade realizar o processo de comunicação de dados entre os hosts da rede, bem como implementar os endereços lógicos dos hosts e definir a melhor rota (caminho) a ser seguido pelo pacote durante sua transmissão.</i>
(2) ENLACE	<i>É a camada responsável por entregar “nó a nó” a mensagem. Deve também garantir que a transferência de dados ocorra livre de erros de um nó para outro, além de realizar a tradução do endereço lógico estabelecido da camada superior (rede) para o endereço físico (vice-versa).</i>
(1) FÍSICA	<i>É a camada mais próxima do hardware e tem como responsabilidade realizar a conexão física entre os dispositivos de rede, converter os bits em sinais elétricos, sincronizá-los e por fim transmiti-los de acordo com a interface física existente no dispositivo e o meio (canal) de transmissão/comunicação de dados.</i>

Durante todo o processo de comunicação de dados realizado pelo modelo de referência OSI/ISO, há o que chamamos de processo de encapsulamento e desencapsulamento de pacotes. Ou seja, quando uma informação é transmitida do nó de origem para o nó de destino, ela por sua vez será obrigada a passar por cada uma das 7 (sete) camadas do modelo OSI e em cada camada essa informação será encapsulada e receberá um cabeçalho que irá ter dados referentes a camada.

Esse processo de encapsulamento é realizado até que a informação passe a ser considerada um bit e este seja transmitido pelo meio de comunicação. Do lado contrário (nó de destino) é realizado o processo inverso. Ou seja, o bit vai sendo desencapsulado e assim por diante em cada camada até que seja entregue ao usuário ou aplicação.

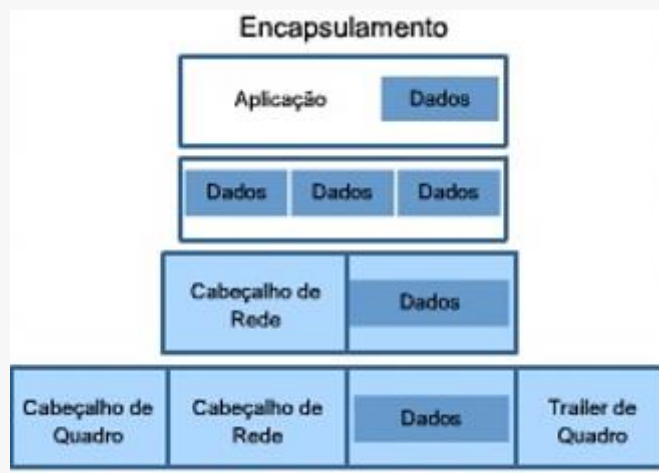
Conforme você irá observar na figura a seguir, as informações durante o processo de encapsulamento e desencapsulamento recebe uma nomenclatura diferente de acordo com a camada em que se encontra. Por exemplo, a informação nas camadas de aplicação e apresentação são nomeadas como PDU; na camada abaixo, “sessão”, o PDU passa a ser conhecido como “dados”; na próxima camada, “transporte”, o dado passa ser nomeado de “segmento”; na camada abaixo, a de rede, o segmento passa a ser conhecido como “pacote”; na camada de enlace o pacote passa a ser reconhecido como “quadro” e, por fim, na última camada, a camada física, o quadro passa a ser reconhecido como “bit”.

Figura 20 - Modelo OSI/Processo de Encapsulamento e Desencapsulamento.



Lembre-se que não podemos esquecer que cada vez que um pacote de dados passa por uma camada ele por sua vez recebe um cabeçalho, ou seja, uma espécie de etiqueta que irá conter informações sobre aquela camada e essa etiqueta é mantida pela próxima camada, que por sua vez acrescenta uma nova etiqueta (cabeçalho) ao pacote.

Figura 21 - Cabeçalho do modelo OSI/ISSO.



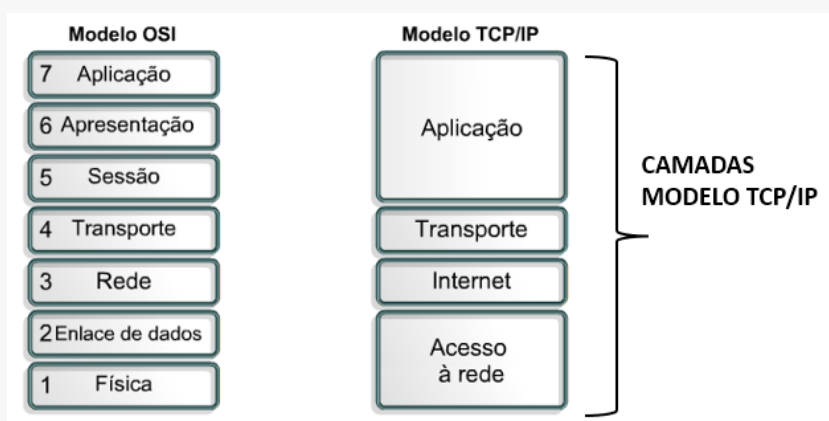
### Modelo de Arquitetura TCP/IP

Pode não parecer, meu jovem Padawan, mas o modelo de arquitetura TCP/IP que é atualmente utilizado em todas as redes de computadores, incluindo a Internet, surgiu bem antes do modelo de referência OSI desenvolvido pela ISO. Ou seja, o modelo de arquitetura TCP/IP surgiu junto com a ARPANET, lá na década 60.

Naquela época os protocolos de comunicação de dados mais relevantes eram o TCP/IP, o NETBEUI, o IPX/SPX, o XNS e o APPLE TALK. Entre esses protocolos, o que representava um conjunto maior de protocolos internos que permitia que vários tipos de equipamentos de diversos desenvolvedores e fabricantes se comunicassem entre si era o nosso queridinho TCP/IP. Isso porque o conjunto de protocolos TCP/IP era estruturado por camadas (é isso mesmo, camadas!!!), na qual cada camada consumia e prestava serviços às camadas adjacentes. Vale ainda ressaltar que cada camada apenas realizava o tratamento das informações que correspondiam à sua função. Isso sem dúvida foi o fator determinante para a escolha do modelo TCP/IP.

Comparando o modelo TCP/IP com o modelo OSI, inicialmente percebe-se que temos duas camadas que foram formadas a partir da fusão de outras camadas do modelo OSI, a saber: a camada de aplicação do modelo TCP/IP que corresponde a fusão das camadas aplicação, apresentação e sessão do modelo OSI) e a camada acesso à rede do modelo TCP/IP que corresponde à fusão das camadas enlace e física do modelo OSI.

Figura 22 - Modelo OSI vs. Modelo TCP.



Observa-se também a nomenclatura das camadas acaba divergindo em comparação com a nomenclatura apresentada no modelo OSI, porém, isso não significa que há uma incompatibilidade entre ambos os modelos e as respectivas funções de cada camada.

Neste contexto, teremos o modelo TCP/IP com as seguintes camadas:

CAMADA	DESCRIÇÃO/FUNÇÃO
(4) APLICAÇÃO	Similar ao modelo OSI, essa camada é a mais próxima do usuário e tem como objetivo prover a interface entre a aplicação e a rede, bem como o controle dos serviços e protocolos. Além de realizar todas as funções que existem na camada de apresentação e sessão do modelo de referência OSI/ISO.
(3) TRANSPORTE	Camada responsável por realizar os serviços de comunicação de dados e entrega dos pacotes “fim a fim” entre a origem e o

	destino. Dentre as funções existentes nessa camada destacam-se a segmentação do pacote e o controle de fluxo e erros. Os principais protocolos presentes nessa camada são o TCP e o UDP.
(2) INTERNET	Tem como responsabilidade realizar a comunicação entre hosts conectados à rede, bem como implementar os endereços lógicos (endereço IP) e definir o melhor caminho (rota) a ser seguido pelo pacote de dados. Principal protocolo dessa camada é o IP.
(1) ACESSO À REDE	Camada responsável por realizar a conexão física entre os dispositivos de rede, converter os bits em sinais elétricos, sincronizá-los e realizar a transmissão de acordo com a interface física presente no dispositivo e o meio de transmissão (canal de comunicação).

Alguns pontos importantes a saber do modelo TCP/IP: na camada de “transporte”, conforme observado, os dois protocolos principais são o UDP e o TCP. Ambos possuem um papel importantíssimo na transmissão dos pacotes. Isso porque, de acordo com a necessidade da origem (emissor) e do destino (receptor), as transmissões de dados poderão ser de dois tipos: (1) transmissões de dados orientadas a conexão ou (2) transmissões de dados não orientadas a conexão. Mas o que seria transmissão de dados orientado a conexão e transmissão de dados não orientado a conexão?

Bem, jovem Padawan, conforme dito anteriormente, os dois principais protocolos da camada de transporte são o UDP e o TCP e cada um deles possui uma missão durante a transmissão de dados em nossa rede.

No caso do protocolo TCP, que é o acrônimo de *Transmission Control Protocol* ou “protocolo de controle de transmissão”, já sabemos que ele é a base de toda a arquitetura de redes, incluindo a Internet junto com o seu irmão o protocolo IP (*Internet Protocol*). Sendo o protocolo TCP um guerreiro muito versátil e robusto, este por sua vez é o mais adequado

para ser utilizado nas transmissões de dados de todos os tipos de redes, incluindo a nossa rede mundial de computadores, a Internet. Isto porque o protocolo TCP é orientado à conexão, ou seja, quando uma conexão é estabelecida entre dois hosts e os pacotes de dados então podem ser transmitidos em ambas as direções, o protocolo TCP possui funções internas que têm como objetivo: (a) verificar o fluxo de dados e erros; (b) garantir que os pacotes de dados sejam entregues na ordem em que foram transmitidos e, (c) caso haja algum erro ou perda de algum pacote de dados durante a sua transmissão, o TCP encarrega-se de enviar novamente o pacote de dados de acordo com as solicitações do destino (receptor).

Essas funções, por mais simples que possam parecer, fazem do protocolo TCP um super protocolo e o queridinho das aplicações e/ou serviços de rede que requerem confiabilidade e segurança, pois não só permitem o total controle na comunicação de dados com relação ao fluxo e erros na transmissão, como também promovem a segurança, integridade e confiabilidade.

Já seu companheiro o protocolo UDP, acrônimo de *User Datagram Protocol*, é totalmente descompromissado com relação ao controle do fluxo de dados, erros, segurança, integridade e confiabilidade. Isto se dá pelo fato de que, diferente do protocolo TCP, o UDP não é orientado à conexão. O que o torna um protocolo mais simples. Porém, esse fato de não ser orientado à conexão não deixa de dar o devido valor ao protocolo UDP, muito pelo contrário!

Existem diversas aplicações e/ou serviços de rede que não necessitam de uma segurança e confiabilidade, e sim de rapidez na transmissão de dados, principalmente aquelas aplicações que realizam a transmissão de vários pacotes de dados interruptamente, como as aplicações de streaming de vídeos ou áudio realizadas por emissoras de TV e rádio, ou aplicações que necessitam realizar consultas/pesquisas em

bases de dados, como por exemplo os serviços de consulta de nomes de domínio como DNS ou de diretórios como o *Microsoft Active Directory*. Nesse caso, essas aplicações/serviços de rede precisam apenas enviar ou receber pacotes de dados, não se preocupando se um ou outro pacote não for recebido. Ou seja, não se preocupam com questões relacionadas a verificação dos dados transmitidos entre a origem e o destino, apenas com a velocidade dessa transmissão de dados.

Basicamente, enquanto o protocolo TCP preocupa-se com a entrega do pacote de dados e com o controle da transmissão, garantindo que a transmissão tenha um começo, meio e fim e que todos os pacotes de dados chegaram certinhos (em ordem) no destino, o protocolo UDP apenas realiza a transmissão de dados sem se preocupar com a garantia que o pacote chegará ao seu destino e considerando que essa conexão seja uma transmissão de dados sem um começo e sem um fim!

Diante do exposto, meu jovem Padawan, se a aplicação ou o serviço de rede requer segurança e confiabilidade o protocolo que será utilizado é o TCP. Agora, se a aplicação ou serviço de rede não necessita de segurança e confiabilidade, apenas agilidade e rapidez no envio dos pacotes de dados, o protocolo que deverá ser utilizado é o UDP. Sendo assim, não existe o bom ou ruim em termos de protocolo e sim a necessidade da aplicação ou do serviço de rede. Afinal, como percebido, cada um dos protocolos (UDP ou TCP) irá atender a uma ou outra necessidade.

Agora, vem a questão, meu jovem Padawan, como o protocolo TCP garante a confiabilidade e a segurança, bem como realiza todos os controles necessários na transmissão dos pacotes de dados? Você já ouviu falar em um processo denominado de “*three-way handshake*”?

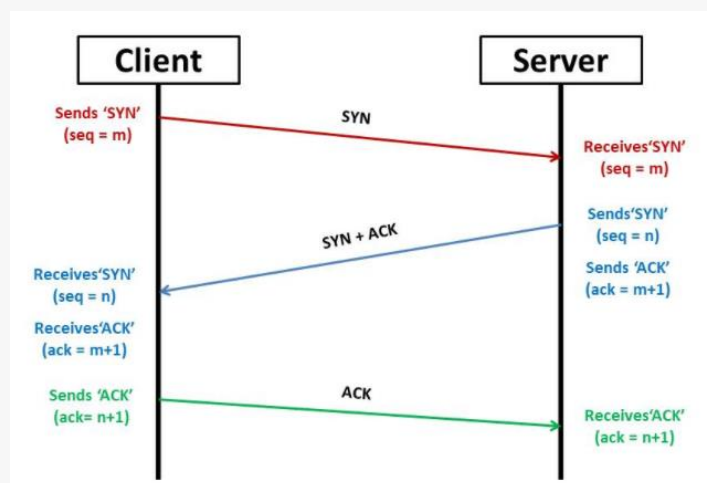
O processo de three-way handshake, ou conhecido na galáxia das redes de computadores como o “processo de aperto de mãos em 3 vias”, é um conjunto definido de atividades (etapas) que ocorrem no protocolo TCP



para criar um canal (link) de comunicação seguro e confiável entre o transmissor e o receptor (origem e destino), incluindo atividades que realizam o controle do fluxo de dados, o controle de erros e o controle de início e fechamento da comunicação entre ambas as partes.

O objetivo do processo three-way handshake é o de estabelecer a conexão entre ambas as partes (origem e destino) antes mesmo que a transmissão dos dados ocorra e garantir que a transmissão ocorra sem erros e de forma segura. Após a transmissão dos dados, não havendo nenhum outro pacote de dados a ser transmitido, o processo de three-way handshake garante que a conexão estabelecida entre ambas as partes possa ser encerrada de maneira correta.

Figura 23 – Processo de Inicialização do Three-way Handshake (protocol TCP).



Para que possamos compreender melhor o processo three-way handshake realizado pelo protocolo TCP na camada de transporte do modelo TCP/IP, observe a figura 23. Nela temos um emissor (*client*) e um receptor (*server*) e, conforme percebe-se, o “cliente” precisa estabelecer uma conexão junto ao “servidor” para aí sim realizar a transmissão dos pacotes de dados. Então o que ocorre, meu jovem Padawan?

Bem, o “cliente” deseja conectar-se ao “servidor”, então ele, “cliente”, envia uma mensagem contendo um sinalizador “SYN” para o

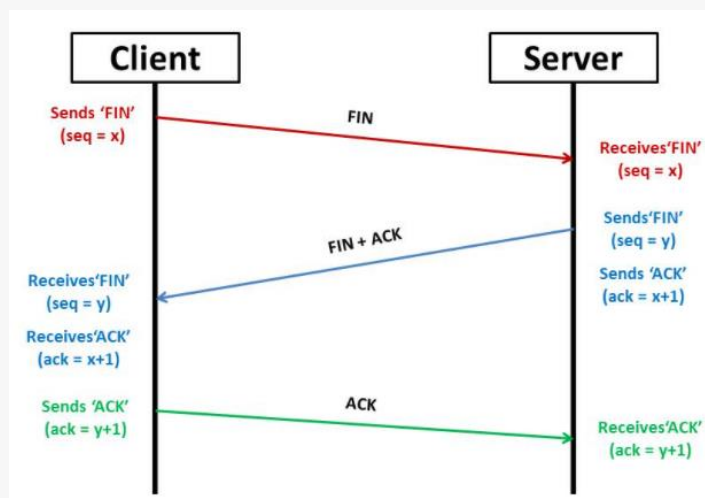
“servidor” como se fosse uma pergunta: *Ei, servidor! Posso me conectar a você?* Ainda nessa mensagem há a existência de outras informações, tais como um número de sequência que pode ser aleatório de 32 bits, o sinalizador “ACK”, o tamanho da janela de transmissão e o tamanho máximo do segmento de dados que será transmitido. Essa é a primeira etapa do processo.

O “servidor”, por sua vez, recebe a solicitação e, se estiver disponível para estabelecer a conexão, responde com uma mensagem de confirmação para o “cliente” com os sinalizadores “SYN” e “ACK”, anunciando ao “cliente” outras informações em conjunto como o tamanho da janela de transmissão e o tamanho máximo do segmento que ele suporta. É como se o “servidor” respondesse ao “cliente”: *Olá, cliente! Estou sim disponível para você!* Essa é a segunda etapa do processo.

O “cliente”, por sua vez, recebe a resposta do “servidor” e envia um sinalizador “ACK”, concluindo assim as etapas do processo de conexão e, enfim, inicia a transmissão dos dados. É como se o “cliente” respondesse ao “servidor”: *Ok servidor, vamos começar a transmitir os dados!* Essa é a terceira e última etapa do processo de estabelecimento de conexão realizado pelo three-way handshake.

Agora, jovem Padawan, tudo que se inicia deve ser terminado, concorda? Então veremos o processo inverso do three-way handshake realizado pelo protocolo TCP na camada de transporte.

Figura 24 - Processo de Finalização do Three-way handshake.



Após a conclusão da transmissão dos dados, o “cliente” envia ao “servidor” um sinalizador “FIN” informando que já transmitiu todos os pacotes de dados. É como se fosse assim: *Ei, servidor! acabei de enviar todos os pacotes de dados.* Essa é a primeira etapa do processo de finalização.

O “servidor”, por sua vez, responde ao cliente com os seguintes sinalizadores “FIN” e “ACK”, confirmando assim que recebeu a mensagem e que está pronto para encerrar a conexão. Exemplo: *Ok cliente, então podemos encerrar a conexão?* Essa é a segunda etapa do processo de finalização.

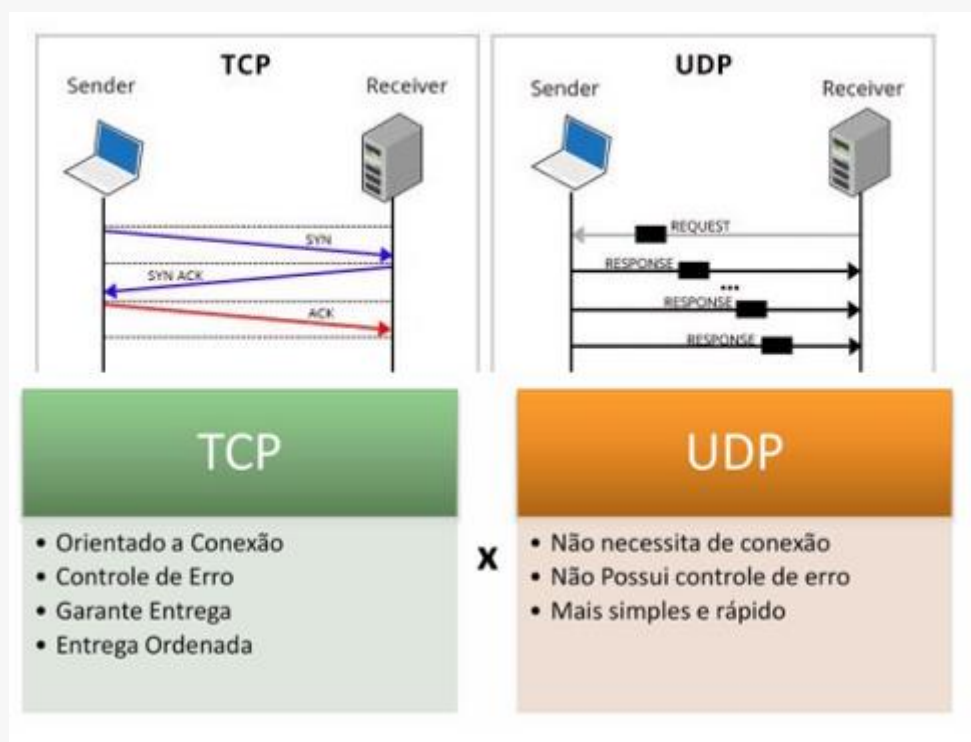
O “cliente” responde ao “servidor” com um sinalizador “ACK”, confirmando assim que a conexão pode ser finalizada. Exemplo: *Sim, servidor!* Essa é a terceira e última etapa do processo de finalização do three-way handshake.

É importante lembrá-lo que durante toda a troca de mensagens, como mencionado anteriormente, há também o envio de diversas outras informações necessárias ao início e ao encerramento da conexão entre o cliente e o servidor. Todas essas informações estarão presentes no cabeçalho das mensagens e podem ser facilmente visualizadas através de

alguma ferramenta de snife de rede, como por exemplo a ferramenta Wireshark.

Aqui, jovem Padawan, apresentamos apenas um resumo entre o protocolo TCP e UDP para que você possa conhecer um pouco mais da “força”.

Figura 25 - TCP vs. UDP.





**XP**e

## > Capítulo 3



## Capítulo 3. Protocolo IP e Endereçamento IP

---

Conforme você já deve ter percebido, meu jovem Padawan, o protocolo IP é um protocolo importantíssimo para as redes de computadores e, em especial, para a maior delas, a Internet. Essa importância é tão grande que faz até compor o nome do modelo de arquitetura utilizado mundialmente nas redes de computadores, o TCP/IP.

Especificado da RFC 791 e publicado, em 1974, pela entidade de padronização IEEE, o protocolo IP, acrônimo de “*Internet Protocol*”, tem como missão principal garantir que os pacotes de dados sejam enviados do transmissor para o receptor de forma bem-sucedida através do endereçamento e fragmentação dos pacotes de dados atuando em conjunto com o protocolo TCP da camada de transporte.

Atualmente existem duas versões do protocolo IP, a versão IPv4 e a versão IPv6. Basicamente, o principal ponto que distingue o protocolo IPv4 do protocolo IPv6 é o espaço de endereçamento de bits que é suportado por cada um deles. No IPv4 esse espaço de endereçamento é de 32bits. Enquanto no IPv6 esse espaço de endereçamento é de 128bits. Porém, é óbvio que existem outras diferenças! Mas antes de falarmos sobre as diferenças, vamos primeiramente compreender o que é endereçamento IPv4 e outros detalhes relacionados ao tema. Preparados, jovens Padawans? Então acionando o hiperespaço rumo a galáxia do IPv4 e Ipv6...

### Protocolo e Endereçamento IPv4

O protocolo IPv4 é um protocolo que atua na camada de rede do modelo de referência OSI/ISO e na camada de internet do modelo TCP/IP. Definido e especificado na IEEE - RFC 791, sua principal função é a de fornecer uma conexão lógica entre os dispositivos conectados à rede de computadores, através da identificação de cada um deles por meio de um

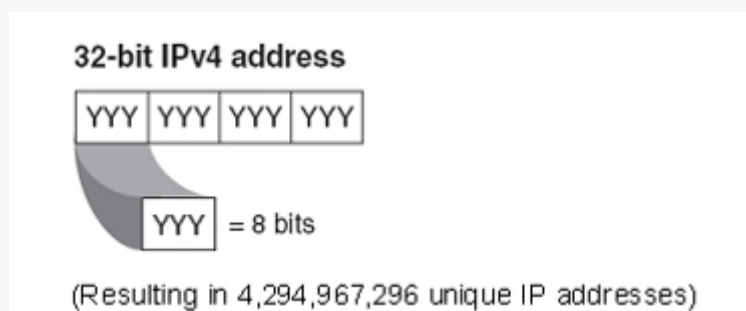
endereçamento lógico denominado de endereçamento IPv4 ou simplesmente: endereço IPv4.

O protocolo IPv4 utiliza endereços de 32 bits para realizar e identificar a comunicação dos dispositivos de rede. Esse endereço IPv4 é apresentado em 5 classes de endereços, a saber: (1) classe A, (2) classe B, (3) classe C, (4) classe D e, por fim, a (5) classe E.

As classes A, B e C possuem um comprimento de bit diferente que são utilizados para endereçar o host da rede. Já os endereços IPv4 da classe D são reservados para multicast e os da classe E são reservados para uso futuro.

O endereçamento IPv4 ao utilizar 32 bits para endereçar dispositivos na rede, significa que ele poderá fornecer  $2^{32}$  endereços IPs. Ou seja, o endereçamento IPv4 pode fornecer aproximadamente 4,29 bilhões de endereços IPs. Daí te pergunto, meu jovem Padawan, você considera essa totalidade de endereços IPs uma quantidade suficiente para atender o universo de dispositivos que temos atualmente e que necessitam estar conectadas a um ou várias redes, incluindo a Internet?

Figura 26 - Protocolo IPv4.



Bem, em uma galáxia não tão distante, até poderia ser! Mas, atualmente, essa quantidade de endereços IPs não é suficiente, principalmente para a rede mundial de computadores – a Internet. O que fez surgir um enorme problema, a escassez de endereços IPs e a solução

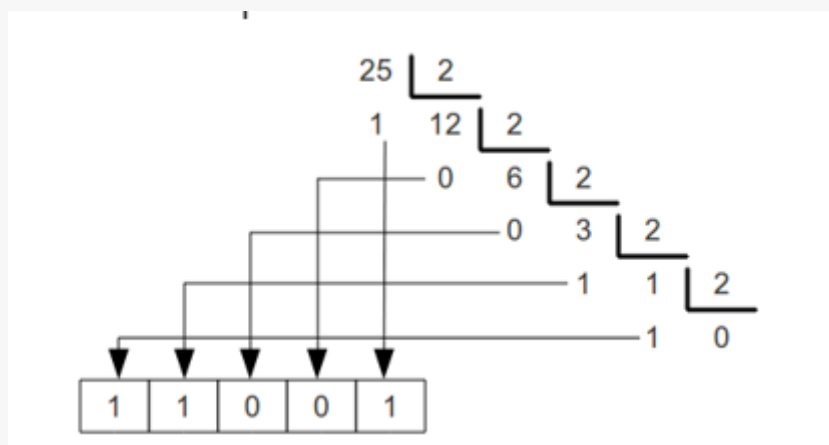
da criação de uma nova versão do protocolo IP, o protocolo IPv6. Mas essa história veremos mais à frente!

Voltando então para o endereçamento IPv4, conforme observado na figura 26, ele é um endereço IP formado por 32 bits e sua notação (escrita) é no formato decimal pontilhado, no qual 4 números são separados por casas. Exemplo: 192.168.120.110.

Porém, sabemos que os dispositivos computacionais conversam na linguagem binária, ou seja, falam e compreendem apenas (0) zeros e (1) uns. Neste sentido, para que o dispositivo computacional compreenda a notação decimal do endereço IPv4, é necessário que seja realizada uma conversão de decimal para binário e vice-versa.

O processo de conversão de números decimais para binário é relativamente simples. Considerando que os números decimais têm com base 10 (dez) casas numéricas, a conversão dever ser realizada para um grupo numérico com apenas 2 (duas) casas com base numérica.

Figura 27 - Conversão Decimal para Binário.

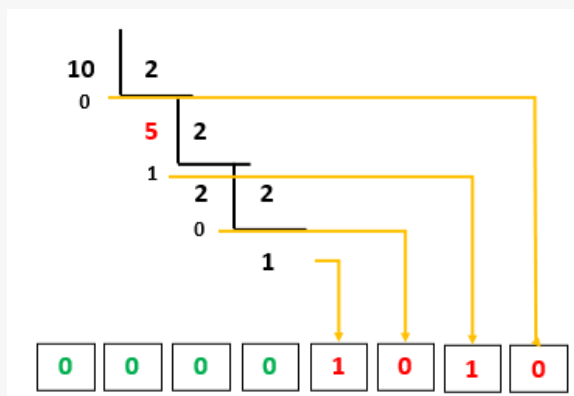


Sendo assim, para realizar a conversão, basta ir dividindo o número decimal que você deseja converter em binário por 2 até que o resultado seja 0 (zero) ou 1 (um).



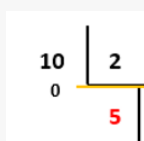
Um jeitinho fácil, meu jovem Padawan, é você realizar o processo de “escadinha” na divisão dos números decimais em 2 para a formação do binário. Para isso vá desenhando uma escadinha cada vez que obtiver o resultado até que a divisão finalize. Observe a figura 28:

Figura 28 - Processo Escadinha - Decimal vs. Binário.

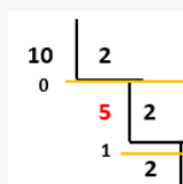


No caso apresentado, estamos convertendo o número 10 (dez) em formato binário. Para isso dividimos o número 10 (dez) por 2 (dois), anotamos abaixo do número 10 (dez) o resto e abaixo do número 2 (dois) o valor correspondente a divisão.

Figura 29 - Representação da divisão.

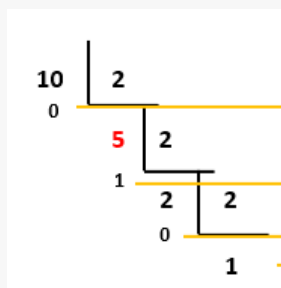


Agora, repetimos o processo, porém vamos realizar a divisão do número 5 (cinco) em 2 (dois). Teremos como resultado o 2 (dois) para dividirmos e o resto 1 (um). Observe:



Repetimos o processo de divisão novamente, mas agora dividindo o número 2 (dois) por 2 (dois). Observa-se que o resultado será 1 (um) resta 0 (zero).

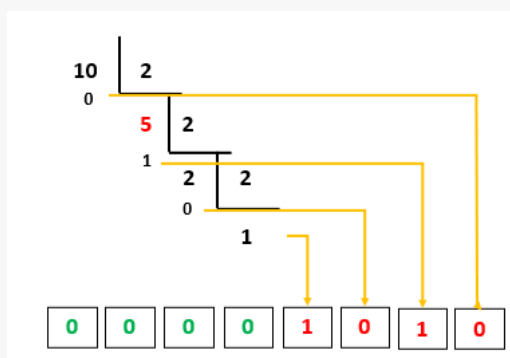
Figura 30 - Resultado da divisão.



Bem, com relação as operações matemáticas, finalizamos, lembrando que temos que obter como resultado da nossa conta 0 (zero) ou 1 (um).

Agora vamos à segunda parte da nossa conversão. Desenhe 8 quadradinhos abaixo da escadinha que você fez e coloque cada um dos “restas” na sequência da direita para esquerda, começando pela primeira divisão realizada. Observe a figura 31:

Figura 31 - Alinhando os "restas" da direita para esquerda.



A conversão do número decimal 10 para binário será 1010. Porém, o bit é formado por 8 (oito) octetos e, sendo assim, teremos que completar os 4 últimos quadradinhos (octetos) com o 0 (zero). Daí o resultado da nossa conversão do número decimal 10 para o binário será: 00001010

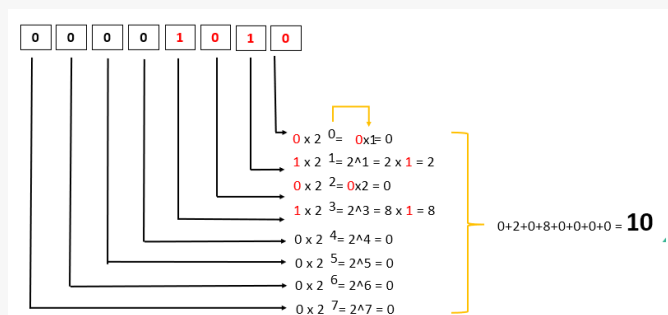
Existem diferentes maneiras de converter um número decimal em binário e é possível utilizarmos uma calculadora científica para fazer essa conversão, como também URLs (sites) na Internet que possuem uma calculadora on-line para a realização da conversão e assim realizarmos uma conversão de um endereço IPv4 em binário e vice-versa, como por exemplo a URL: <https://calculadoraip.com.br/>

Agora, se você deseja converter um número binário em um número decimal, basta realizar o processo inverso. Ou seja, ao invés de dividir por 2 (dois), você irá multiplicar por 2 (dois) e, posteriormente, somar os resultados. Mas, atenção, existem umas “regrinhas” matemáticas que devem ser obedecidas. Por exemplo:

REGRA	CONCEITO
1	Realizar a multiplicação por 2 (dois), sempre elevando a 0, 1, 2 e assim por diante...
2	Resolver primeiramente a potenciação;
3	Todo número elevado a 0 (zero) terá como resultado 1 (um);
4	Todo número multiplicado por 0 (zero) terá como resultado 0 (zero);
5	Todo número elevado a 1 (um) ser ele mesmo.

Na prática, suponha que se deseja converter o número binário 00001010 para decimal, basta seguir a lógica abaixo e as regrinhas. Não tem erro!

**Figura 32 - Conversão de Binário para decimal.**

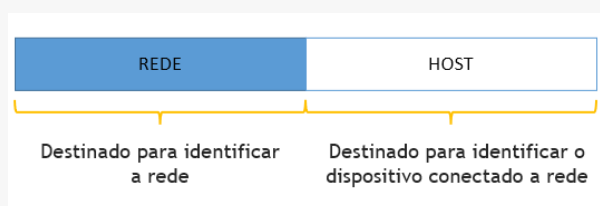


## Classes do Endereçamento IPv4

Assim que o protocolo IP foi padronizado, no início da década de 80, em sua especificação constava que para cada interface de sistema ou dispositivo ligado à rede ou à Internet, um valor único de endereço IP de 32 bits deveria ser associado ao sistema ou dispositivo. Porém, alguns dispositivos, como por exemplo os roteadores, possuem uma ou mais interfaces de conexão à rede e, neste caso, para cada uma das interfaces interligadas à rede um único endereço IPv4 deve ser associado.

Nas classes do IPv4, a primeira parte de um endereço IPv4 identifica a rede em que o dispositivo ou sistema encontra-se. Já a segunda parte identifica o próprio dispositivo ou sistemas na rede. Isto cria uma hierarquia de endereçamentos em dois níveis. Observe (figura 33):

Figura 33 - Hierarquia de endereços IPv4.



Atualmente, a porção destinada à rede é conhecida como “prefixo de rede”. Assim, todos os dispositivos ou sistemas conectados à rede irão compartilhar o mesmo prefixo de rede. Porém, cada um com o seu único (exclusivo) endereçamento IPv4. Ou como denominamos “*host-number*” (número do host).

Vale lembrar que: quaisquer hosts em diferentes redes deverão ter um prefixo de rede diferente, mas poderão ter o mesmo host-number.

Como observamos anteriormente, o endereçamento IPv4 possui 4 classes (A, B, C, D e E). Cada uma dessas classes “fixa” a fronteira entre o prefixo de rede e o host-number em diferentes pontos entre os 32 bits que compõe o endereço Ipv4. Observe a seguir:

Figura 34 - Classes IPv4.

**Classes IPv4**

CLASSE	FAIXA END. IP	MASC. SUB REDE	NOTAÇÃO CIDR	Nº REDES	Nº. IPs	Nº. IPs POR REDE
A	10.0.0.0 A 10.255.255.255	255.0.0.0	/8	126	16.777.216	16.777.216
B	172.16.0.1 A 172.31.255.254	255.255.0.0	/16	16.382	1.048.576	65.534
C	192.168.0.0 A 192.168.255.255	255.255.255.0	/24	2.091.150	65.535	256
D	224 A 239	MULTICAST	-	-	-	-
E	240 A 255	EXPERIMENTAL	-	-	-	-

Octetos:

255 . 255 . 255 . 255

Classe A: [Rede] ● [Host] ● [Host] ● [Host]

Classe B: [Rede] ● [Rede] ● [Host] ● [Host]

Classe C: [Rede] ● [Rede] ● [Rede] ● [Host]

Ao observarmos as classes do endereçamento IPv4, notamos a presença de um outro elemento ainda não estudado por nós que são as “máscaras de sub-rede” do endereçamento IPv4, e é justamente isso que vamos conhecer a seguir, jovens Padawans!

### Máscara de Sub-Redes no IPv4

A máscara de sub-rede, ou também conhecida como “*netmask*”, é um número de 32 bits utilizado para que um endereço IPv4 possa realizar a separação de quais partes do endereçamento correspondem à rede, à sub-rede e, por fim, aos hosts. Ou seja, trata-se de uma segmentação realizada dentro de uma rede, o que proporciona a divisão de uma grande rede em diversas redes menores, tornando assim a rede mais eficiente em termos de fluxo, tráfego e desempenho, além de proporcionar uma melhor administração e/ou gerenciamento.

Bem, jovem Padawan, para que possamos segmentar uma rede maior em outras redes menores, precisamos dividir o número (endereço) da máscara dessa rede maior utilizando valores que estejam entre 0 até 255. E para realizarmos essa tarefa iremos utilizar as máscaras de sub-rede.

Como referência de máscaras de sub-rede, apresentamos a seguinte tabela:

Tabela 1 - Máscara de Sub-Redes.

HOST	REDE	MASC. SUB-REDE	CIDR
1	256	255.255.255.255	/32
2	128	255.255.255.254	/31
4	64	255.255.255.252	/30
8	32	255.255.255.248	/29
16	16	255.255.255.240	/28
32	8	255.255.255.224	/27
64	4	255.255.255.192	/26
128	2	255.255.255.128	/25
256	1	255.255.255.0	/24

Observe que na tabela apresentada há a presença de uma coluna identificada como “CIDR” ou conhecido como notação CIDR. Esta notação “CIDR” é um método utilizado em implementações de redes e sub-redes que possibilita otimizar a distribuição de endereços IPv4, além de melhorar o processo de roteamento entre as redes. A sigla CIDR é o acrônimo de “*Classes Interdomain Routing*”.

Seguindo adiante... Em uma máscara de sub-rede, os bits referentes à rede serão representados pelo número 1 (um) e os bits referentes a hosts serão representados pelo número 0 (zero). Por exemplo:

Supondo que o endereço da máscara de sub-rede seja da classe “C” do endereço IPv4 – 192.168.1.120/24, este seria representado da seguinte forma:

Tabela 2 - Representação Máscara Sub-Rede.

END. IP	192.168.1.1	11000000.10101000.00000001.01111000
MÁSCARA	255.255.255.0	11111111.11111111.11111111.00000000
REDE	192.168.1.0	11000000.10101000.00000001.00000000
BROADCAST	192.168.1.255	11000000.10101000.00000001.11111111
END. IP HOST INICIO	192.168.1.1	11000000.10101000.00000001.00000001
END. IP HOST FINAL	192.168.1.254	11000000.10101000.00000001.11111110

Lembre-se que os números 1 (um) – em vermelho representa a rede e os números 0 (zero) representam o host! Bem, vamos supor que você precisa saber qual é a máscara de sub-rede do endereço IPv4 10.10.20.45/26 e quantos hosts poderia ter essa rede?

Então, será necessário realizar uma operação matemática para responder a essa pergunta. Mas, para facilitar, vamos em primeiro lugar descobrir os números de hosts possíveis nessa rede. Para isso, eleve a potência de 2 (dois) ao número de hosts apresentados na máscara e do total retire 2 (dois). Veja, o endereço IPv4 é: 10.10.20.45/26 ou:

ENDEREÇO IP	10.10.20.45	BINÁRIO	00001010.00001010.00010100.00101101
MÁSCARA	/26		11111111.11111111.11111111.11000000

Lembre-se: REDE = 1 e HOST = 0

Agora conte o número de 0 (zeros) que você tem em binários. Observe que o total de 0 (zeros) será 6!

.11000000

Então, eleve a potência de 2. Exemplo:  $2^6 = X$

O resultado será 64. Deste resultado, realize a subtração de 2. Ex.:  $64 - 2 = X$ .

O resultado será 62 e, sendo assim, este será o número total de hosts na referida rede. Mas por que subtrair por 2? Porque, seja qual for a classe de rede a ser utilizada, o primeiro endereço IP representa o endereço da rede e o último endereço IP representa o endereço de broadcast. Firmando o conceito, imagine que sua rede é 192.168.0.1/24 a 192.168.0.254/24, o total de hosts dessa rede seria 254 hosts. Isto porque o primeiro endereço IP, que seria 192.168.0.0/24, é destinado para representar a rede e por isso não pode ser utilizado para identificar um host. E o último endereço IP, 192.168.0.255/24, será utilizado para representar o broadcast e por esse motivo também não pode ser alocado em um host. É importante lembrar que o número 0 (zero) entra na contagem como um dígito. Logo de 0 a 255 teremos 256 números.

Agora que já sabemos parte da resposta que é a quantidade de hosts possíveis na rede (62 hosts). Vamos descobrir quantas redes teremos. O primeiro passo é transformar o endereço IP 10.10.20.45 que está em representado em formato decimal para o formato binário. Isso já aprendemos.

ENDEREÇO IP	10.10.20.45	BINÁRIO	00001010.00001010.00010100.00101101
MÁSCARA	/26		11111111.11111111.11111111.11000000


Agora, faça uma tabelinha de 8 (oito) colunas e em cada coluna, começando da esquerda para direita, vá inserindo os múltiplos de 8. Exemplo: 128, 64, 32, 16, 8, 4, 2, 1. Veja como irá ficar:

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



Insira uma linha abaixo dessa tabela e coloque cada número 1 (um) de cada octeto binário abaixo de cada um dos números, sempre da direita para a esquerda.

ENDEREÇO IP	10.10.20.45	BINÁRIO	00001010.00001010.00010100.00101101							
MÁSCARA	/26		11111111.11111111.11111111.11000000							



Todos bits do octeto apresentam "1"

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

Observe que cada número 1 (um) representa um valor. Então some os valores representados nas colunas que têm o número 1 (um) abaixo. Exemplo: a coluna 128 tem o número 1, então soma. A coluna 64 tem o número 1, então soma, e assim por diante. Veja como será a soma:  $128+64+32+16+8+4+2+1$ . O resultado obtido com a soma dos números será: 255. Sendo assim, nosso primeiro octeto representará: 255 (.) ← não podemos esquecer do ponto que separa os octetos! Repita o processo com os demais octetos que irão representar a rede.

ENDEREÇO IP	10.10.20.45	BINÁRIO	00001010.00001010.00010100.00101101			
MÁSCARA	/26		11111111.11111111.11111111.11000000			

Resultado encontrado anteriormente

Encontre os demais resultados de cada sequência de octetos binários

Se você, jovem Padawan, encontrou como resultado: 255.255.255.192, significa que sua conta está certinha! E será essa a nossa máscara de sub-rede para o endereço IP 10.10.20.45

A representação dessa máscara de sub-rede poderá ser realizada de duas formas. A primeira mais tradicional será: Endereço IPv4:

10.10.20.45 → Máscara de Sub-Rede: 255.255.255.192 ou da segunda forma, utilizando a notação CIDR: 10.10.20.45/26

Para facilitar a notação CIDR, basta encontrar na tabela 3 a máscara de sub-rede correspondente ao CIDR.

Tabela 3 - Máscara Sub-Rede e CIDR.

HOST	REDE	MASC. SUB-REDE	CIDR
1	256	255.255.255.255	/32
2	128	255.255.255.254	/31
4	64	255.255.255.252	/30
8	32	255.255.255.248	/29
16	16	255.255.255.240	/28
32	8	255.255.255.224	/27
64	4	255.255.255.192	/26
128	2	255.255.255.128	/25
256	1	255.255.255.0	/24

No caso, a nossa máscara de sub-rede é 255.255.255.192, logo, na representação CIDR será /26.

Bem, já temos a máscara de sub-rede que é 255.255.255.192 ou /26 (CIDR) e o número de hosts dessa sub-rede que é 62 hosts. Agora, qual seriam os endereços IPs reservados para a rede e para broadcast nessa sub-rede: 10.10.20.45/26 ou IP: 10.10.20.45 NETMASK: 255.255.255.192? É, jovem Padawan, que a força esteja com você. Afinal, agora você vai precisar!

Então, tudo parte do princípio BINÁRIO e, sendo assim, você vai precisar converter tudo em binário e depois seguir todos os passos anteriores.

Observe a seguir como ficarão os resultados:

ENDEREÇO IP	10.10.20.45	BINÁRIO		00001010.00001010.00010100.00101101			
MÁSCARA	/26			11111111.11111111.11111111.11000000			
10	10	20	45				
00001010	00001010	00010100	00101101				
255	255	255	192				
11111111	11111111	11111111	11000000				
00001010	00001010	00010100	00000000 → todos os bits de hosts permanecem zerados				
10	10	20	0 → Endereço IP da Rede				
00001010	00001010	00010100	00111111 → todos os bits de hosts mudam para 1				
10	10	20	63 → Endereço IP de Broadcast				
128	64	32	16	8	4	2	1
0	0	1	1	1	1	1	1

$32+16+8+4+2+1 = 63$

Conversão do endereço IP 10.10.20.45 de decimal para binário.

Conversão da máscara de sub-rede: 255.255.255.192 de decimal para binário.

Observe que os 2 primeiros bits da máscara de sub-rede estão citados como 1 (um). Lembrando da regra que o primeiro endereço IP é destinado para rede e o último é destinado para broadcast. Vamos ter como endereço IP da rede: 10.10.20.0

Agora, mude todos os bits de hosts (apresentados como 0 (zero)) para 1 e converta de binário para decimal. Observe que o resultado será 63. Sendo assim, iremos ter como último endereço IP de nossa rede (o endereço de broadcast) o IP: 10.10.20.63

Ufa! jovem Padawan... Essa foi difícil ou não? Bem, para você que está buscando o caminho da força, como meu antigo mestre Yoda sempre dizia:

“Exercitar, deve você. Pois só assim aprenderá!”

Agora, vamos exercitar mais um pouco. Responda:

- Quantas sub-redes seria possível ter na rede 192.168.1.0/27?
- Quantos hosts cada uma das sub-redes acima teria?

Bem, para que possamos responder a essas duas perguntas, precisamos primeiramente identificar quantos bits foram reservados para a

sub-rede. Para isso descubra a máscara de sub-rede e converta ela em binário.

ENDEREÇO IP	192.168.1.0	BINÁRIO	11000000.10101000.00000001.00000000
MÁSCARA	/27		11111111.11111111.11111111.11100000

Pronto. Agora, observe que teremos 5 (cinco) bits 0 (zero) reservados para hosts. Logo será:  $2^5 = 32$  hosts. Mas lembre-se que deles temos que subtrair 1 para rede e 1 para broadcast. Então teremos:  $32 - 1 - 1 = 30$  hosts.

Observe que o último octeto da direita para esquerda possui 3 bits representados pelo número 1 (um). Lembrando que os bits representados pelo número 1 (um) correspondem à rede, então teremos:  $2^3 = 8$  ← este será o número de sub-redes desta rede. Agora como ficaria a faixa de endereçamento IPv4 de cada sub-rede? Observe:

Sub-Rede	Faixa de Endereçamento IPv4 192.168.1.0/27 classe C
1	192.168.1.0 a 192.168.1.32
2	192.168.1.33 a 192.168.1.64
3	192.168.1.65 a 192.168.1.96
4	192.168.1.97 a 192.168.1.128
5	192.168.1.129 a 192.168.1.160
6	192.168.1.161 a 192.168.1.192
7	192.168.1.193 a 192.168.1.224
8	192.168.1.225 a 192.168.1.256

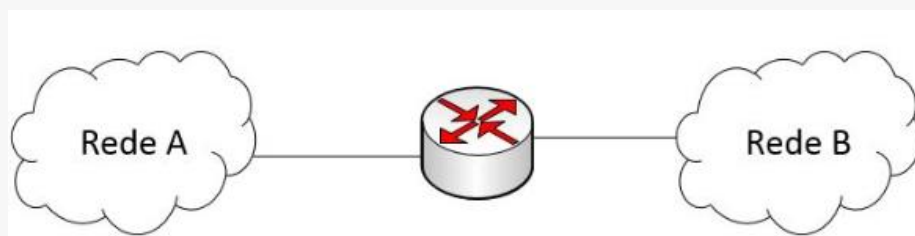
Partindo do ponto que a máscara de sub-rede permite um total de 8 sub-redes nessa rede, e cada uma dessas sub-redes terá no máximo 32 hosts, sendo o primeiro endereço IP destinado à rede e o último destinado a broadcast, basta agora você ir criando a sequência de endereços IPs de acordo com a quantidade de sub-redes até que se alcance o número máximo, que é 256.

## Roteadores e Rotas

Um roteador (*router*, em inglês) é um equipamento de rede que efetua o encaminhamento de pacotes de dados entre redes de computadores distintas. Esses pacotes de dados são encaminhados de um roteador para outro até que atinjam o dispositivo de destino, ou sejam descartados. Os roteadores efetuam a leitura dos pacotes IP, podendo analisar o conteúdo de seus cabeçalhos e então tomar decisões baseando-se nos lados lidos e os protocolos de transmissão implementados em suas configurações.

Os roteadores são conectados em redes distintas, efetuando a conexão entre essas redes, em contraste com um Switch, que efetua a conexão de dispositivos finais, como computadores e notebooks, dentro de uma mesma rede.

Figura 35 - Roteador como elemento central interligando duas redes distintas.

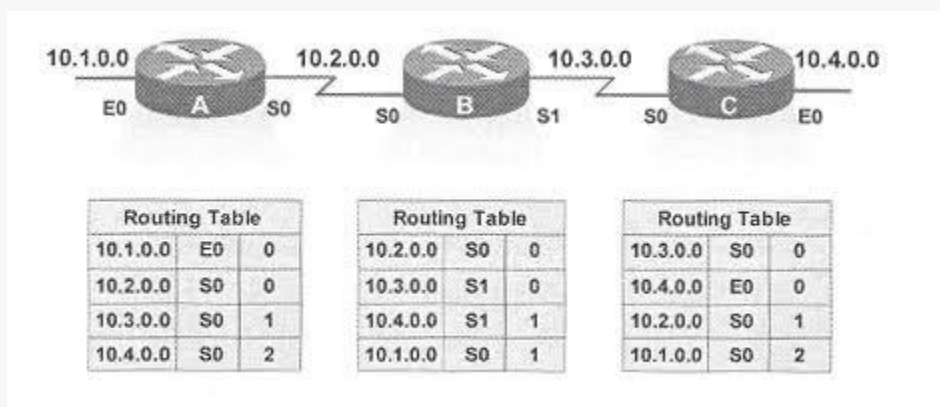


Os roteadores mantêm domínios de broadcast separados para cada rede que conectam, desta forma isolando-as. Assim, dados direcionados à rede local por um host qualquer permanecem nesta rede local, não sendo encaminhados para as outras redes que estejam conectadas ao roteador.

Por exemplo, na figura 35, se um host na rede A enviar um pacote a outro host na mesma rede A, o roteador não encaminhará o pacote para a rede B, o pacote permanece no domínio de broadcast a que pertence. Agora, se um host na rede A enviar um pacote para um host localizado na rede B, o roteador irá encaminhar o pacote de uma rede para outra, efetuando assim seu roteamento.

Os roteadores dependem de uma tabela de roteamento para identificar para onde um pacote de dados deve ser encaminhado. As tabelas de roteamento contêm informações sobre o destino, próximo salto, interface, métricas e rotas, que podem ser usadas para guiar o pacote de dados através das linhas de comunicação e em direção ao seu destino.

Figura 36 - Exemplo Tabela Roteamento.



Existem dois métodos pelos quais as tabelas de roteamento são atualizadas e mantidas em ordem. Isto pode ser feito de forma dinâmica ou estática.

O método estático envolve a atualização manual das tabelas de roteamento. Por outro lado, os roteadores dinâmicos trocam automaticamente informações com dispositivos através de diferentes protocolos de roteamento. Com base nessas informações, as tabelas de roteamento são automaticamente atualizadas.

Todos os roteadores executam a função básica de receber e enviar dados entre a Internet e os dispositivos locais conectados a uma rede. No entanto, há diferentes tipos de roteadores que existem com base em como eles se conectam aos dispositivos ou como funcionam dentro de uma rede. Especificamente, os tipos de roteadores comumente disponíveis incluem:

- *Router* – Um roteador B também é conhecido como roteador de ponte. Ele é um dispositivo de rede que executa tanto como uma

ponte quanto como um roteador. Tanto uma ponte quanto um roteador conectam redes, entretanto, a ponte de rede envolve conectar duas redes separadas para permitir que elas funcionem como uma única rede coesa. Considerando que um roteador fornece uma conexão que ainda mantém ambas as redes como redes privadas individuais;

- *Core Router* – Um roteador core estabelece uma conexão de rede e facilita a transmissão de dados dentro da rede privada. Os roteadores do tipo “core” funcionam dentro do núcleo ou dentro da rede e não podem enviar ou receber dados fora dela. A distribuição de dados está limitada à rede, uma vez que este tipo de encaminhador é incapaz de realizar o intercâmbio de informações com outros sistemas;
- *Roteador de Borda* – Um roteador de borda é responsável pelas transferências de dados de condução entre várias redes. Ao contrário do roteador core, o roteador edge não facilita o intercâmbio de pacotes de dados dentro de uma rede privada, mas, em vez disso, gerencia a transmissão de dados para outros sistemas de rede separados;
- *Roteador virtual* – Geralmente, um roteador virtual consiste em um software que permite que um dispositivo funcione como um roteador físico padrão. É capaz de funcionar com o uso de um Protocolo de Redundância de Roteador Virtual (VRRP).
- *Roteador sem fio* – Um roteador sem fio ainda mantém uma conexão com fio com o modem onde recebe sinais de dados da Internet. No entanto, não há necessidade de uma conexão com fio do roteador para os dispositivos que estão conectados à rede. Um roteador sem fio usa antenas que enviam ondas de rádio ou infravermelho que carregam os pacotes de dados. O exemplo mais

comum de um roteador sem fio são os roteadores [Wi-Fi](#) de casa, que são largamente usados em escritórios e casas residenciais.

Figura 37 - Esquema de interligação de Roteadores de Borda.



Jovem Padawan, acredito que até aqui você percebeu que a principal função de um roteador é a de interligar redes distintas e encaminhar os pacotes de dados entre elas. Bem, a esse encaminhamento de pacotes de dados realizados pelo roteador denominamos de “encaminhamento de pacotes IP” e o processo deste encaminhamento é conhecido como “roteamento de pacotes IP”.

O roteamento de pacotes IP é o processo pelo qual os roteadores escolhem um caminho (rota) pelo qual o pacote de dados irá passar. Esse caminho (rota) é definido através de um protocolo conhecido como “protocolo de roteamento”.

No algoritmo de roteamento, que está presente no protocolo de roteamento, existe dois níveis, a saber: o primeiro denominado de IGP (*Interior Gateway Protocol*) que é utilizado de forma interna à rede; já o segundo é o EGP (*External Gateway Protocol*) que por sua vez é utilizado de forma externa à rede.

Cada um dos dois níveis, por sua vez, terá internamente vários outros protocolos, tais como: RIP, IPX, OSPF, BGP, EIGRP, IGRP e CIDR, e

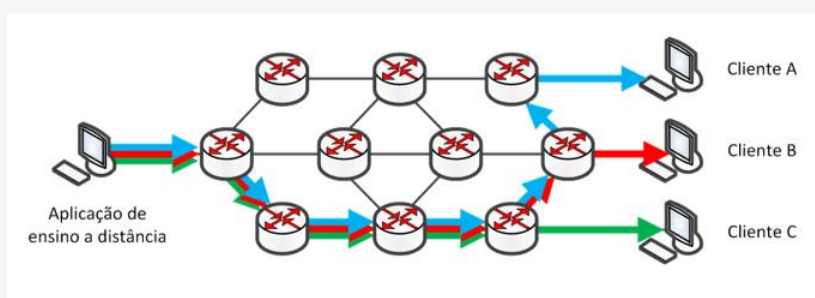


cada um deles irá realizar funções específicas de acordo com o propósito de desenvolvimento.

Bem, seja qual for o modelo de roteador utilizado, qualquer um irá implementar um protocolo de roteamento baseado na maior coincidência. Ou seja, irá implementar um algoritmo de direcionamento que servirá para realizar o encaminhamento de pacotes IP de uma rede a outra.

*LONGEST MATCH* é uma rota com prefixo de rede estendido, utilizado para descrever o maior número possível de possibilidades de destino menor. Roteadores que utilizam o algoritmo longest match, o fazem para direcionar o tráfego de pacotes IP de forma mais eficiente.

Figura 38 - Algoritmo Longest Match.

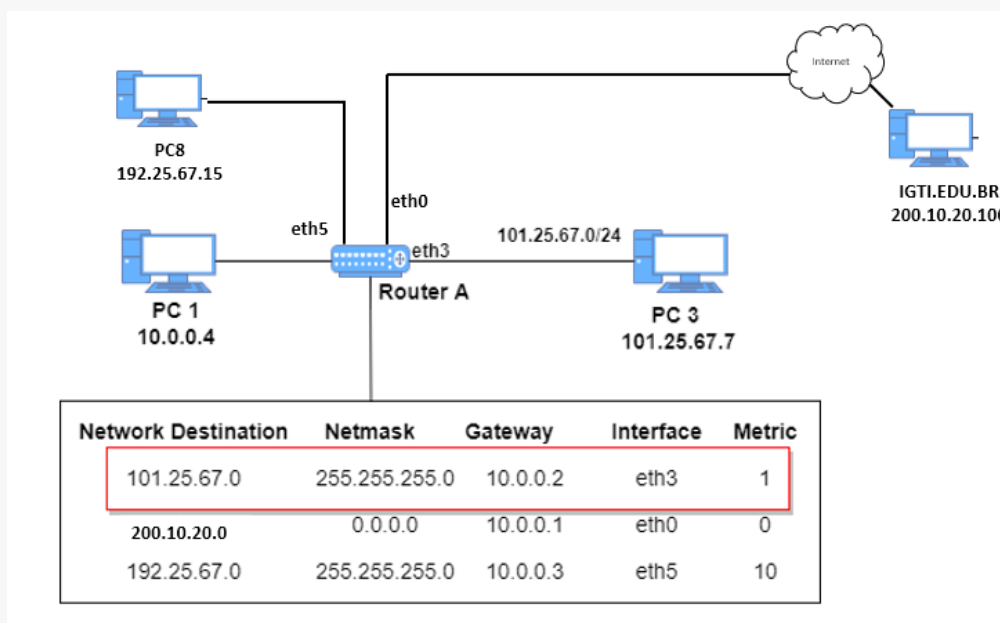


Falando um pouco mais, meu jovem Padawan, sobre tabela de roteamento, além do que já estudamos anteriormente, ela será composta por outras informações, tais como: origem da rota, rede de destino, distância administrativa, métrica, next-hop, data/hora da rota e interface de saída. Essas informações são essenciais para que o pacote siga a diante em seu caminho, ou melhor rota até o destino.

Em toda tabela de roteamento irá existir uma rota padrão, ou seja, uma rota específica que irá descrever o caminho padrão que o pacote de dados IP deverá seguir caso não encontre nenhuma outra rota (caminho) na tabela de roteamento. A rota padrão na tabela de roteamento será representada da seguinte forma: 0.0.0.0/0 na versão IPv4, e ::/0 na versão IPv6. Atenção! É regra, todo o roteador deve em sua tabela de roteamento

ter essa rota padrão, pelo qual o pacote de dados seguirá caso não encontre outra.

Figura 39 - Representação de uma tabela de roteamento.



De acordo com a figura 39, se o host PC8 deseja enviar um pacote de dados para o host igti.edu.br, o pacote então seguirá pela rota padrão que está configurada para sair na interface eth0 do roteador. Agora se o host PC8 desejar enviar um pacote para o host PC3, o pacote então seguirá na rota que está configurada para sair na interface eth3 do roteador.

### Protocolo IPv6

Como visto anteriormente, para que um novo dispositivo ou sistema se conecte à rede ou à Internet, é preciso que ele receba um endereço lógico único e exclusivo. E é essa a função do protocolo IPv4. Porém, apesar de fornecer cerca de 4.29 bilhões de endereços IP e com a crescente demanda a cada dia de centenas de milhares de dispositivos e sistemas necessitando interconectar à rede e, em especial, à Internet, infelizmente o total de endereços IPs fornecidos pelo IPv4 esgotou! É isso mesmo, meu jovem Padawan, não há como fornecer mais endereços IPv4.

Sabendo que esse fato iria acontecer, especialistas, pesquisadores, desenvolvedores, fabricantes e entidades de padronização de diversas partes da galáxia, se uniram para buscar uma solução ao problema de escassez de endereços IPv4. O resultado dessa união fez surgir então uma nova versão do protocolo IP, no qual passou a ser conhecida como protocolo IPv6.

A criação do protocolo IPv6 parte da ampliação dos números de bits para endereçamento. Ou seja, o que a turma fez foi passar de 32 bits que era o número máximo na versão IPv4 para 128 bits na versão IPv6.

É obvio, jovem Padawan, que não foi só essa mudança, mas essa é a mais significativa e importante. Isto porque, agora, com a versão IPv6, ao invés de termos 4.29 bilhões de endereços IPs que poderiam ser alocados em dispositivos ou sistemas, passamos a ter a marca de (vamos lá, o número é enorme...) 340.282.366.920.938.463.374.607.431.768.211.456 (ufa! Confesso que nem sei expressar esse número na unidade de medidas). Ou seja, temos  $2^{128}$ , isto representa aproximadamente 79 octilhões de vezes a quantidade de endereços IPv4.

Se você, meu jovem Padawan, não considera esse número o suficiente, observe que teremos aproximadamente 55 octilhões de endereços IPs por ser humano na terra, se considerarmos uma população mundial de 6 bilhões de habitantes. E aí, agora é suficiente?!

Figura 40 - Comparação entre IPv4 vs. IPv6.

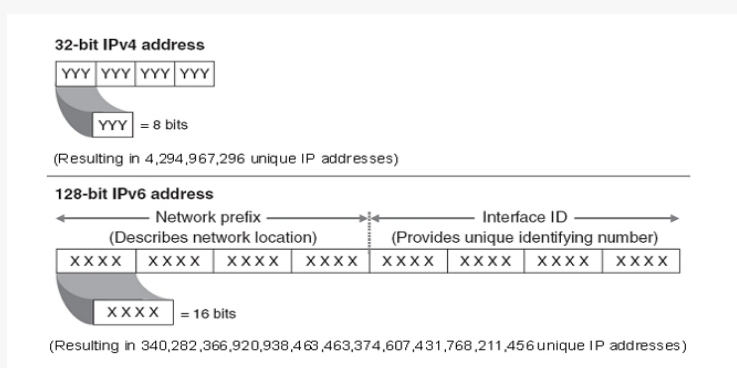
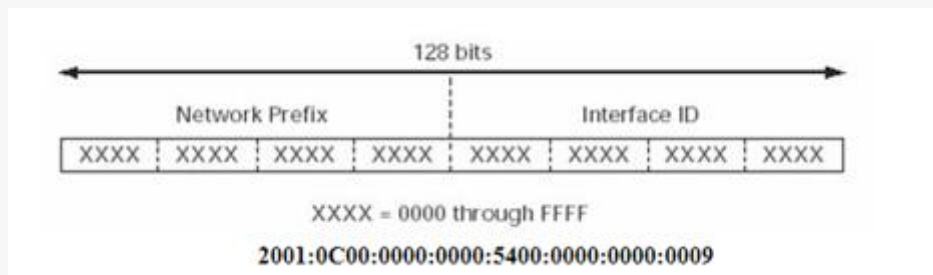


Figura 41 - IPv6.

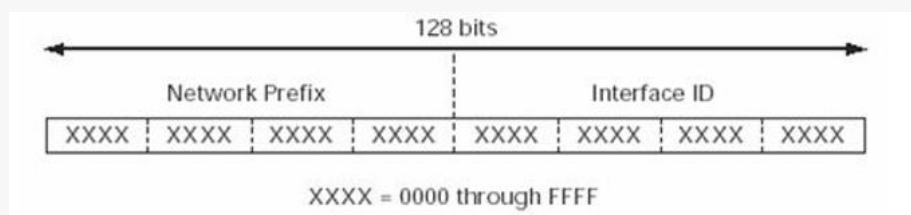


Observa-se na figura 41 que o endereço IPv6 é representado por 8 grupos de 16 bits separados por "." (ponto) e escritos no formato hexadecimal (0-F). Isso permite que seja utilizado no endereçamento IPv6 caracteres maiúsculos e minúsculos, podendo ainda ser aplicada algumas regras para abreviar e facilitar a escrita de grandes endereços, como por exemplo a regra que permite omitir o 0 (zero) a esquerda de cada bloco de 16 bits ou a regra que permite substituir uma sequência longa de 0 (zeros) por :: ← ponto sobre ponto.

A princípio pode parecer confuso, mas as regras facilitam, e muito, a administração e manutenção de uma rede que utiliza o protocolo IPv6 no dia a dia.

Outro ponto importante é com relação aos prefixos de rede. No IPv6 o prefixo de rede continua da mesma forma que no IPv4, inclusive utilizando a notação CIDR. Sendo assim, para o IPv6, os endereços serão representados da seguinte forma: 64 bits para identificar rede e máscara de sub-rede e 64 bits para representar os hosts. Observe:

Figura 42 - Representação de Rede, Sub-Rede e Hosts no IPv6.



Com relação aos tipos de endereços existentes no protocolo IPv6, teremos: (a) UNICAST – endereço que identifica uma única interface de maneira que um pacote de dados enviado a um endereço do tipo unicast é entregue a uma única interface; (b) ANYCAST – reconhece um conjunto de interfaces. Neste caso o pacote de dados é encaminhado a um endereço do tipo anycast, que por sua vez é uma interface pertencente a um conjunto de interfaces mais próximas da origem. A ideia por trás do anycast é a de uma comunicação um-para-um-de-muitos; (c) MULTICAST – similar ao anycast, com a ressalva que um pacote de dados é enviado a um endereço multicast e, entregue a todas as interfaces associadas a esse endereço multicast. A ideia aqui é a de comunicação um-para-muitos.

Já com relação as questões de rota e roteamento, o protocolo IPv6 segue os mesmos princípios e lógicas do IPv4. Porém, com uma tecnologia superior em termos de desenvolvimento, velocidade, controle de fluxo e erros, escolha de rotas e demais outras. Afinal, o IPV6 é uma evolução do IPv4.

Apesar de todas as vantagens oferecidas pelo protocolo IPv6, principalmente na questão de fornecer muito mais endereços IP (muito mais mesmo), o IPv6 ainda é um, vamos dizer, “bebê” que está começando a “engatinhar” na galáxia das redes. Isso porque sua oficialização ocorreu relativamente a pouco tempo, em 2012, e há um universo gigantesco de dispositivos e sistemas existentes antes da criação do IPv6 e que precisam se adequar a essa nova tecnológica de protocolo IP, sem contar que, como toda tecnologia nova, leva-se um tempo até que tudo se acerte.



**XP**e

## > Capítulo 4



## Capítulo 4. Dispositivos de Interconexão

---

Seja qual for o tipo ou topologia de rede de computadores que será implementado em sua casa ou na organização onde trabalha, sempre haverá a necessidade de inserção de dispositivos e/ou sistemas que realizem a interconexão entre todos os outros dispositivos e/ou sistemas presentes na rede.

A todos esses dispositivos nomeamos de “dispositivos de interconexão” e, como o próprio nome sugere, a função principal de qualquer um deles é justamente o de realizar a interconexão entre todos os outros dispositivos e/ou sistemas presentes na rede. Porém, é óbvio que cada tipo ou modelo servirá para um determinado propósito e terá várias funções ou funcionalidades na rede.

Para começar, vamos falar um pouco sobre os GATEWAYS.

Os gateways podem ser encontrados na forma de appliance (hardware) ou software (aplicativo). Porém, podemos ainda sim transformar um computador (PC ou Servidor) em um gateway.

Bem, podemos considerar um gateway como um nó de rede utilizado nas redes de telecomunicações e nas redes de computadores para interligar duas redes com diferentes protocolos de transmissão (essa ideia lembra o roteador, concorda – jovem Padawan? Mas não é!). O gateway age como um ponto de entrada e saída para uma rede e obrigatoriamente todos os pacotes de dados devem passar ou se comunicar com ele antes de serem roteados pelo roteador.

Como sabemos, 99% das redes existentes atualmente utilizam o protocolo TCP/IP e, sendo assim, todos os pacotes IP deverão passar pelo gateway, exceto aqueles que estão entre nós no mesmo segmento da LAN.

No jargão técnico da galáxia de redes de computadores é comum os analistas denominarem o gateway como gateway padrão e isto dá na mesma em termos de conceito e funcionalidades.

Como principal vantagem da utilização de um gateway podemos citar a simplificação da conectividade entre a rede LAN e outra, como por exemplo a WAN ou Internet.

Em um ambiente organizacional, um gateway pode exercer diversas funções, tais como a função de servidor proxy ou até mesmo a função de um firewall. Mas como funciona um gateway?

Bem, seja qual for a rede, ela por sua vez terá um limite que irá limitar a comunicação com qualquer outro dispositivo ou sistema que esteja diretamente interconectado a ela. Por conta disso, se a rede em questão desejar se comunicar com dispositivos e/ou sistemas, nós ou outras redes fora desse limite, ela por sua vez irá exigir a implementação e funcionalidade de um gateway.

No geral, um gateway pode ser considerado uma junção entre um roteador e um modem e, na maioria dos casos, sua implementação ocorre na extremidade da rede, ou seja, na borda da rede e ali ele fica gerenciando todos os pacotes de dados que são direcionados internamente ou externamente na rede.

Daí, quando a rede LAN, por exemplo, deseja se comunicar com a rede WAN para enviar um pacote de dados, esse pacote é repassado ao gateway que, em seguida, o redireciona para o roteador ou para a rota (no caso dele estar atuando como um roteador) que possui o melhor caminho que o pacote poderá seguir, além de realizar o armazenamento do registro de todas as informações sobre a rede de destino, rota, o tipo de pacote de dados, a origem e o destino, o host transmissor, dentre outras que fazem parte da administração e gerenciamento.



Por fim, podemos concluir que os gateways são no geral conversores de protocolos, permitindo assim a compatibilidade e a interoperabilidade entre dois protocolos, podendo atuar em qualquer uma das camadas do modelo OSI/ISO ou TCP/IP.

Apenas a título de curiosidade, podemos encontrar gateways especificados para diversas funções. A saber: gateway de armazenamento em nuvem; gateway de API, gateway de IOT; gateway proxy; gateway firewall; gateway VoIP; gateway de mídias e muitos outros tipos.

Agora, vamos pular os roteadores. Pois, afinal, já falamos deles anteriormente. E vamos para os SWITCHS!

Bem, um switch é um dispositivo de rede de alta velocidade que tem como objetivo receber pacotes de dados e redirecioná-los para o seu destino em uma LAN. No geral, operam na camada 2, e alguns modelos mais sofisticados operam na camada 3. Nesse contexto, poderemos encontrar switches L2 e switches L3 (o “L” significa “*layer*” ou, traduzindo, “camada”) e, sendo assim, suportam praticamente todos os protocolos presentes nessas camadas (2 e 3).

Um switch L2 pode ser também entendido como “bridge” e sua função neste caso é a de enviar os quadros contendo os pacotes de dados entre nós ou segmentos de uma LAN. Podemos comparar um switch como um policial que realiza o controle do trânsito dos carros (pacotes de dados) em uma rede LAN. Já um switch L3 possui como vantagem a função “roteamento” e com isso consegue interligar uma rede LAN com outra qualquer. Mas, atenção! Não é porque ele tem a função roteamento que ele pode ser considerado um roteador. São coisas distintas!

Uma coisa muito bacana com relação aos switches é que temos modelos de switch que possuem a função de gerência e daí chamamos eles de switch gerenciáveis. Essa função de gerência permite os analistas de

redes e equipes de TI terem um controle maior de todo o tráfego da rede que passa pelo switch, através de uma interface administrativa que no geral é uma aplicação web – isto significa que pode ser acessado por qualquer browser.

Além de funções de controle e administração, os switches gerenciáveis também permitem a criação de VLANs, ou seja, redes locais virtuais. Isso é bem útil para organizações que desejam segmentar a suas redes para realizar um controle maior em termos de acesso, troca de pacotes, controle de broadcast, entre outros.

Apenas para título de curiosidade, temos, vamos dizer assim, um parente mais velhinho dos switches que é o hub. Um hub é simplesmente um dispositivo que conecta todos os nós de um único segmento de rede LAN e, neste sentido, não possui nenhuma das funções de um switch.

Na galáxia de redes, os mestres *Jedi* e *Lords Sith* costumam referenciar os hubs como equipamentos “burros” que somente têm a capacidade de interligar hosts de uma mesma e única rede LAN e não conseguem controlar questões relacionadas a fluxo de dados, domínio de broadcast e assim por diante. Neste contexto, os switches são considerados mais inteligentes, justamente por possuírem muitas outras funções e funcionalidades que um hub não possui, além de atuarem de outras camadas do modelo OSI e TCP/IP.

Aproveitando que citamos VLANs, meu jovem Padawan, vamos dar um pulinho nesse planeta chamado VLAN...

### VLANs – Redes Locais Virtuais

Existem inúmeras definições para uma rede local virtual, como pode ser observado na bibliografia.

- Varadarajan as define como "estruturas capazes de segmentar, logicamente, uma rede local em diferentes domínios de broadcast". (data)
- Já Molinari diz que "uma rede virtual é um grupo de estações e servidores que se comunica independentemente de sua localização física ou topologia, como se fosse um único domínio broadcast, ou uma rede lógica." (data)

De acordo com as definições apresentadas, a implantação de VLANs possibilita a partição de uma rede local em diferentes segmentos lógicos (criação de novos domínios broadcast), permitindo que usuários fisicamente distantes (por exemplo, um em cada local ou andar da empresa) estejam conectados à mesma rede.

Como fatores motivadores à criação de VLANs em uma infraestrutura de TI no ambiente corporativo, imagine uma empresa cujo crescimento acelerado impossibilitou um projeto ordenado de expansão, que possua uma dezena de departamentos conectados a uma rede local interna. Ao contrário do que se pensa, os funcionários de cada departamento estão espalhados pelos andares da sede. Como organizar um domínio para cada setor da empresa? Uma solução possível seria a segmentação da rede interna em redes virtuais, uma para cada departamento.

Outro exemplo é a formação de grupos temporários de trabalho. Hoje em dia é comum o desenvolvimento de projetos envolvendo diversos setores de uma empresa, como marketing, vendas, contabilidade e comercial. Durante o período do projeto, a comunicação entre seus membros tende a ser alta. Para conter o tráfego broadcast, pode-se implementar uma VLAN para esse grupo de trabalho.

Os exemplos anteriores mostram que as VLAN proporcionam uma alta flexibilidade a uma rede local. Isto é ideal para ambientes corporativos, onde a todo momento ocorrem mudanças de empregados, reestruturações internas, aumento do número de usuários, entre outras situações. Entre os benefícios proporcionados pela implantação de redes virtuais, podemos citar:

- Controle do tráfego broadcast – as VLANs apresentam um desempenho superior as tradicionais redes locais, principalmente devido ao controle do tráfego broadcast. Tempestades de quadros broadcast (*broadcast storms*) podem ser causadas por mal funcionamento de placas de interface de rede, conexões de cabos malfeitas e aplicações ou protocolos que geram este tipo de tráfego, entre outros. Em redes onde o tráfego broadcast é responsável por grande parte do tráfego total, as VLANs reduzem o número de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede. De um outro ponto de vista, em uma rede local segmentada, os domínios de broadcast são menores. Isto porque cada segmento possui um menor número de dispositivos conectados, comparado ao existente na rede sem segmentação. Com isso, trafegam menos quadros broadcast tanto em cada segmento, quanto em toda rede;
- Segmentação lógica da rede – como visto anteriormente, redes virtuais podem ser criadas com base na organização setorial de uma empresa. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isto proporciona uma segmentação lógica da rede;
- Redução de custos e facilidade de gerenciamento – grande parte do custo de uma rede se deve ao fato da inclusão e movimentação

de usuários dela. Cada vez que um usuário se movimenta é necessário um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores. Em uma VLAN, a adição e movimentação de usuários pode ser feita remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade;

- Independência da topologia física – VLANs proporcionam independência da topologia física da rede, permitindo que grupos de trabalho, fisicamente diversos, possam ser conectados logicamente a um único domínio broadcast;
- Maior segurança – as redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais proteção e segurança a estes. O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Desta forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim "*domínios de segurança no acesso a recursos*".

Por fim, os dispositivos em uma rede local virtual podem ser conectados de três maneiras diferentes, sendo:

- Enlace tronco (*Trunk Link*) – todos os dispositivos conectados a um enlace deste tipo, incluindo estações de trabalho, devem, obrigatoriamente, ter suporte a VLANs. Todos os pacotes de dados transmitidos em quadros em um *trunk link* possuem um rótulo VLAN;
- Enlace de Acesso (*Access Link*) – um enlace de acesso conecta um dispositivo sem suporte à VLAN a uma porta de um switch. Todos

os pacotes de dados transmitidos em quadros neste tipo de enlace, obrigatoriamente, não devem possuir rótulo;

- Enlace Híbrido (*Hybrid Link*) - este é uma combinação dos dois enlaces anteriores. Em um enlace híbrido são conectados tanto dispositivos com suporte a VLANs, quanto os sem. Num enlace desta natureza pode haver quadros com (*tagged frames*) e sem rótulo (*untagged frame*), mas todos os quadros para uma VLAN específica têm de ser com rótulo VLAN ou sem rótulo.



**XP**e

## > Capítulo 5



## Capítulo 5. Elementos de Integração

---

A década de 80 sem dúvida foi uma daquelas décadas das quais quem viveu (eu) jamais esquecerá. Isto porque, na ocasião, várias revoluções, tais como: políticas, sociais, econômicas, culturais, científicas e até tecnológicas aconteceram de uma forma muito ampla e dinâmica, fazendo com que as pessoas, sociedades e organizações mudassem conceitos, paradigmas, culturas, pensamentos etc.

Do lado das tecnologias e da computação essas revoluções foram extremamente marcantes. Como exemplo podemos citar a rede mundial de computadores – a Internet – que passou a ser utilizada por todos nós. Naqueles anos as redes de computadores se tornaram cada vez mais comuns dentro das organizações e junto com a Internet causaram um frenesi nas empresas de telecomunicação e informática. Para se ter uma ideia do que estamos contando a você, meu jovem Padawan, só na área das telecomunicações, na época, as empresas investiram pesado na abordagem de cabos e equipamentos, espalhando cabos e equipamentos em todos os lugares e cantos do planeta.

E é aí que entra aquela famosa frase dita pelos astronautas Jack Swingert e Jim Lovell da missão Apollo 13 ao centro de comando da Nasa na Terra:

“OK, HOUSTON WE HAVE A PROBLEM!”

Com a necessidade constante e imposta pelas organizações em querer estarem conectadas à Internet para a realização de seus negócios e a cada dia uma nova tecnologia de telecomunicação e computação era lançada, a ausência de uma padronização nos sistemas, dispositivos, tecnologias e cabos de telecomunicação utilizados na época passou a ser realmente um grande problema para todos – desenvolvedores, fabricantes,



empresas de telecomunicação, organizações etc., deixando assim todos com uma grande “dor de cabeça”!

É por isso então que temos as “entidades padronizadoras”! Na ocasião, a entidade heroína foi a EIA (*Electronic Industries Association*) que em conjunto com a outra salvadora a TIA (*Telecommunications Industry Association*) desenvolveram uma proposta de solução ao problema da falta de padronização, principalmente relacionada a utilização de cabos em redes de telecomunicações e redes de computadores, no qual como resultado gerou a primeira versão de uma norma internacional de padronização, logo no finalzinho dos anos 80 início dos anos 90, levando assim a paz para toda a galáxia das telecomunicações e redes!

Nomeada de EIA/TIA – 568, a normatização criada tinha como objetivo: (a) implementar um padrão genérico de cabeamento a ser utilizados nas telecomunicações (voz e dados) por qualquer fornecedor; (b) estruturar um sistema de cabos intra e inter prédios que pudesse ser utilizado por qualquer produto de qualquer fornecedor e, por fim, (c) estabelecer critérios técnicos de desempenho para sistemas distintos de cabos de telecomunicação (voz e dados).

Logo, a nova norma EIA/TIA-568 apresentou benefícios que foram percebidos por todos rapidamente, dentre os quais destacamos: (a) diminuição dos custos financeiros e operacionais relacionados à implementação de cabos – afinal, antes da norma em uma organização poderia ser encontrado diversos tipos de cabos e cada um para uma determinada função, por exemplo: cabos só para o tráfego de voz, outros para serem somente usados para dados, outros para som e assim por diante... imagine a quantidade de cabos encontrados em uma única organização naquela época. Com a norma todos esses serviços, dados, voz, som etc., que necessitavam de cabos específicos, passaram a utilizar um único tipo de cabo para tudo; (b) interoperabilidade entre diferentes

fabricantes e fornecedores – afinal todos tinham uma referência técnica a ser seguida para a produção de cabos, e (c) aumento da capacidade de transmissão, desempenho, integridade e velocidade.

Talvez o benefício mais significativo da norma EIA/TIA-568 foi a introdução do conceito de um sistema de cabeamento estruturado que poderia ser utilizado por qualquer empresa e indústria.

Esse conceito baseia-se na disposição de uma rede de cabos, com interligação e integração de serviços de dados e voz, que facilmente poderiam, com base no conceito, ser redirecionados por caminhos diferentes dentro de uma mesma infraestrutura, provendo um caminho de transmissão entre pontos da rede distintos.

### Cabeamento Estruturado

Então, pensar em um sistema de cabeamento estruturado é pensar em “organização” e talvez essa seja a palavra mais certa para definir o que é um sistema de cabeamento estruturado de rede. Isto porque um sistema de cabeamento estruturado é uma abordagem organizada para a implementação de uma infraestrutura de cabeamento, independentemente do tamanho da organização, seja ela pequena, média ou grande, o modelo de negócio que ela atua ou simplesmente se o desejo for implementar uma infraestrutura de cabeamento em sua casa.

Conceitualmente falando, um sistema de cabeamento estruturado é definido como a organização da infraestrutura de cabeamento de telecomunicações (voz e dados) de um prédio ou campus, havendo ainda vários componentes menores padronizados.

Em um sistema de cabeamento estruturado irá existir uma infraestrutura criada por um conjunto de patch panel, racks, armários de telecomunicações, cabos, conectores e vários outros elementos que

permitirão a conexão dos mais variados dispositivos de rede ou telecomunicações.

Todo esse conjunto estará disposto em algumas áreas do prédio, que serão denominadas de acordo com o seu papel no sistema de cabeamento estrutura. Como exemplo, uma dessas áreas é a sala de equipamentos de telecomunicação ou SET que tem como função abrigar todos os equipamentos e dispositivos de telecomunicação.

Com relação aos benefícios de um sistema de cabeamento estruturado, são muitos, começando pelo benefício da organização de toda a infraestrutura de telecomunicações. Porém, além desta podemos citar ainda: disponibilidade dos dispositivos, sistemas e recursos da rede, otimização e padronização de toda a infraestrutura de cabeamento, integridade, confiabilidade, gerenciamento e manutenção, escalabilidade, dentre outras.

Mas, afinal, meu jovem Padawan, por que uma organização deve pensar em implementar um sistema de cabeamento estrutura em sua infraestrutura?

Para começar, imagine essa situação:

Figura 43 - Infraestrutura Desorganizada.



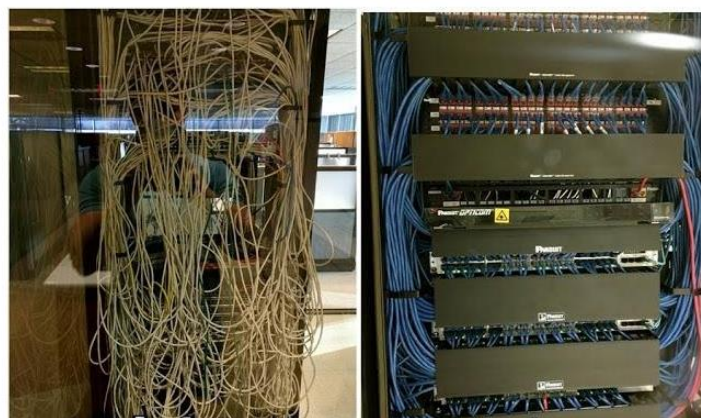
Pergunta: será que os dispositivos, sistemas, serviços e recursos de redes e telecomunicação funcionam de forma eficiente em organizações que possuem a sua infraestrutura de cabos similar à figura 43?

Se você respondeu sim, é bem provável que você esteja sendo otimista, concorda? Possa até considerar que todos os dispositivos, sistemas, serviços e recursos dessa rede estejam funcionando, mas com eficiência, infelizmente acredito que não!

O que precisamos realmente entender que uma infraestrutura de cabeamento desorganizada e sem padronização com certeza trará perdas de comunicação de dados, operacionais e até financeiras em alguns casos. Em uma pesquisa realizada pelo *Real Decisions Institut* a pedido de um dos maiores fabricantes de cabos e soluções para cabeamento estruturado a Furukawa, apontou que mais de 70% dos problemas com a rede são decorrentes do cabeamento. Por isso é que precisamos implementar um sistema de cabeamento estruturado, seguindo um modelo de padronização e melhores práticas.

E como transformar uma infraestrutura de cabeamento desorganizada e sem nenhuma padronização em um sistema de cabeamento estruturado organizado e padronizado (figura 44)?

Figura 44 - Antes e Depois - Cabeamento Estruturado.

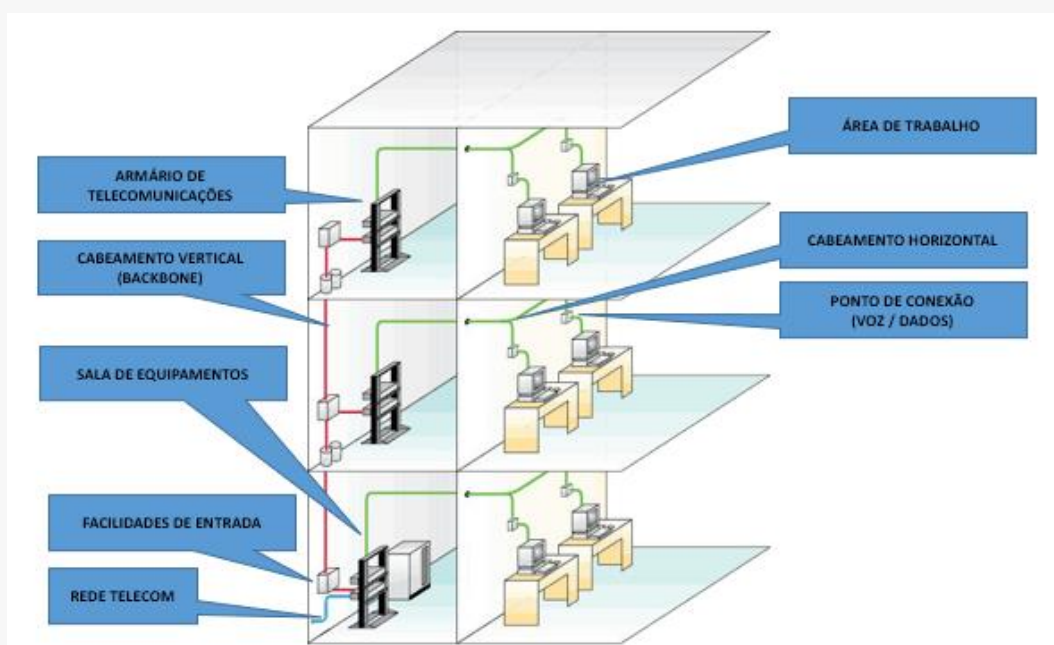


O primeiro passo é buscar no mercado uma empresa especializada em implementação de um sistema de cabeamento estruturado, que seja credenciada no CREA e, o principal, que possua credibilidade no mercado.

Posteriormente, observe, questione e avalie – todos os aspectos técnicos fornecidos pela empresa contratada, fique atento se ela está seguindo as normas e padrões técnicos estabelecidos por uma entidade de padronização (EIA, TIA, ABNT etc.).

Utilize sempre materiais – cabos, conectores, patch panel, patch cords etc., - de primeira linha. Ou seja, de fabricantes reconhecidos no mercado e que prezam por fornecer produtos com qualidade e principalmente de acordos/certificados com as normas e padrões utilizados em um sistema de cabeamento estruturado.

Figura 45 - Sistema de Cabeamento Estruturado.



Na figura 45 podemos observar o esquema de um sistema de cabeamento estruturados. Perceba que existem diversos elementos que compõe esse sistema e cada qual irá exercer um papel.

Entre os elementos apresentados, destacam-se a SET – Sala de Entrada de Telecomunicações – destinada a receber todos os equipamentos, circuitos e cabos fornecidos pela operadora de telecomunicações. No geral, essa sala também é conhecida como “facilidade de entrada ou rede Telecom”. É importante frisar que por melhores práticas e segurança da informação a SET não deve conter os servidores da organização. Isto porque, normalmente, a SET é um local que pode ocorrer um fluxo de entrada de terceiros, ou seja, de técnicos da operadora de telecomunicação, instaladores de cabos, eletricitas e demais equipes terceirizadas que não pertencem ao quadro de colaboradores da organização.

Outro ponto importante a ser observado na figura 45 é o backbone, ou seja, a “espinha dorsal” da comunicação de dados. O backbone é responsável por realizar a interconexão da comunicação de dados entre todos os armários de telecomunicação.

Por fim, temos os armários de telecomunicação que têm a função de distribuir o cabeamento horizontal nas áreas de trabalho que por sua vez irão conter os pontos de conexão onde serão conectados diversos tipos de dispositivos de rede, tais como: computadores, laptops, telefones IPs, impressoras etc., além dos dispositivos de voz, tais como aparelhos telefônicos convencionais, fax-modem, equipamentos de teleconferência ou videoconferência, IoTs, dentre outros.



Figura 46 - Exemplo de um projeto de Cabeamento Estruturado.



A figura 46 representa um exemplo de um projeto de um sistema de cabeamento estruturado. Observe que antes mesmo de colocar a “mão na massa” o desenho técnico do projeto deve ser criado. Nesse desenho técnico, ou também conhecido como planta técnica do projeto, irá conter todas as informações técnicas do sistema de cabeamento estruturado, tais como: quantidade de pontos de conexão de dados/voz, padrão técnico dos cabos, tubulações de passagem de cabos, racks e patch panel, dentre outros.

É importante lembrá-lo, meu jovem Padawan, que o projeto técnico do sistema de cabeamento estruturado deve ser criado por um engenheiro devidamente qualificado e credenciado no CREA – Conselho Regional de Engenharia e Agronomia do estado onde será realizada a obra. Porém, esse engenheiro não irá realizar tudo sozinho, ele irá precisar do auxílio de todos os envolvidos. Ou seja, da equipe de manutenção técnica da organização, da equipe de TI e, por fim, de demais outras pessoas ou equipes envolvidas.


## Cabos e Conectores

Na implementação de um sistema de cabeamento estruturado será necessário a implementação de vários pontos de conexão. Esses pontos devem conter elementos que estejam de acordo com as especificações técnicas dispostas nas normas e/ou padrões.

Na comunicação de dados, os cabos e conectores são importantíssimos. Isso porque, além de conduzir os bits que estão em sinais elétricos para que a comunicação de dados ocorra, são também responsáveis por garantir a qualidade e eficiência de toda a comunicação.

Cabos e conectores fora do padrão ou especificação técnica, de baixa ou má qualidade, com uma crimpagem ruim etc., são muitas das vezes a causa de mais de 80% dos problemas de comunicação de dados em uma rede de computadores e podem trazer para a organização diversos tipos de problemas, tais como: perda da eficiência da comunicação, falhas de comunicação entre os dispositivos, serviços e recursos de rede, indisponibilidade da rede, dentre outros. E, com certeza, problemas operacionais e até prejuízos financeiros e de reputação da marca ou nome da empresa perante os clientes podem acontecer.

As redes de computadores e telecomunicações podem conter diversas mídias de cabos, sendo os mais comuns:

<i>CABO</i>	<i>DESCRIÇÃO</i>
<b>COAXIAL</b> 	Criado na década de 30, trata-se de um cabo que possui um núcleo de fio de cobre envolvido por uma malha metálica trançada que tem como função isolar e proteger o fio central contra diversos problemas relacionados a interferência eletromagnética, tensão etc. Sua capacidade de transmissão de dados pode chegar até 10Mbps. No geral são usados por operadoras de telecomunicação, por operadoras de televisão, em algumas redes de computadores (muito poucas), antenas de



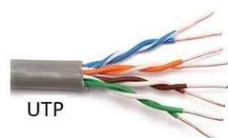
## *SERIAL e PARALELO*



## *USB*



## *PAR TRANÇADO*



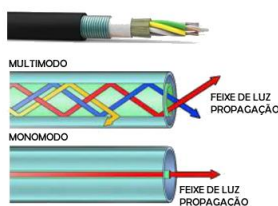
TV. Os principais conectores utilizados nesse tipo de cabo são: RCA e BCN.

Muito utilizados no passado (anos 80 e 90) quando ainda não havia o padrão ethernet, esses modelos de cabo atendiam redes e equipamentos se utilizavam de interfaces seriais e paralelas e possuíam como taxa de transferência menos que 1Mbps. Atualmente são considerados cabos obsoletos, principalmente por conta não só do desenvolvimento do padrão ethernet, mas também por causa da tecnologia USB (universal serial bus). Dentre os principais tipos de conectores, citamos: DB9 e DB25.

Acrônimo de Universal Serial Bus, esse tipo de cabo surgiu logo após a criação do padrão USB, em 1996. De lá para cá várias versões foram desenvolvidas e a cada uma delas as taxas de transmissão foram aumentando. Para se ter uma ideia, a primeira versão “USB 1.0” realizava uma taxa de transmissão de 1.5Mbps. Já a versão atual “USB 3.2” pode realizar uma transmissão de dados a 20Gbps. No geral, são utilizados para interligar dispositivos computacionais de I/O (entrada e saída), tais como: impressoras, scanner, mouse, teclado etc. Porém, podem também ser utilizados nas redes de computadores com a adição de adaptadores USB/Ethernet, seja na opção com fio ou sem fio (wireless). Com relação a conectores, existem diversos tipos, sendo os mais comuns: A, B, C, Micro B, Micro, Mini e Lightning.

Esse tipo de cabo é o mais utilizado em redes de computadores. Possui 4 pares de fios de cobre trançados para a par e foram desenvolvidos para atender o protocolo ethernet. Atualmente existem diversas categorias para esse tipo de cabo, dentre as quais destacam-se CAT5 e CAT5e sendo as mais utilizadas. A variação na taxa de transmissão também é de acordo com a categoria do cabo que será utilizado. Por exemplo, na CAT3 chega-se a 10Mbps ou 10BASE-T. Já nas CAT5 e CAT5e essa velocidade de taxa de transmissão pode ir de 100Mbps (100BASE-T) até 10Gbps (10GBASE-T). Existem ainda outras

## FIBRA ÓPTICA



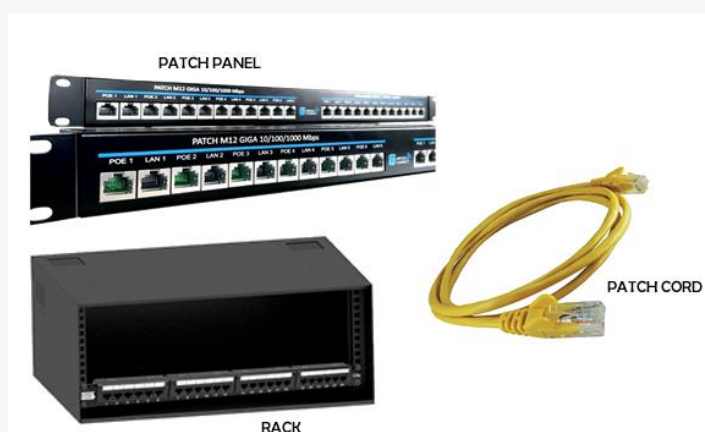
categorias, tais como: CAT6, CAT7 e CAT8, esta última podendo realizar a taxa de transmissão em até 25GBps (25GBASE-T). Os trançados nos pares são necessários para proteger a comunicação dos dados, ajudando a isolar problemas elétricos e reduzir ruídos de fontes externas. Podemos encontrar esse tipo de cabo em 2 modelos: UTP e STP, a diferença está na presença de uma malha metálica protetora que exerce a função de blindar o cabo, como se fosse um escudo protetor. Somente os cabos do tipo STP possuem essa blindagem. Por fim, com relação aos conectores o utilizado para as redes que possuem um sistema de cabeamento estruturado é o conector RJ45 (macho ou fêmea) e em telefônica convencional RJ11.

Entre os tipos de cabos, este é sem dúvida o mais eficiente em diversos aspectos, velocidade, taxa de transmissão, desempenho etc. A comunicação de dados (e voz) neste tipo de cabo acontece através de um feixe de luz em uma fibra da espessura de um fio de cabelo. Este tipo de transmissão é denominado de modos de propagação, neste sentido existem 2 modos de propagação: (1) multimodo – no qual os feixes de luz podem circular de mais de uma maneira ou forma, chegando todos ao mesmo tempo. Uma fibra multimodo pode realizar mais de mil modos de propagação da luz e são empregadas em curtas distâncias com limite de 2km. (2) monomodo ou modo único – neste caso o feixe de luz é propagado de um único modo, podendo realizar uma transmissão paralela ao eixo da fibra. Por fim, a fibra monomodo é ideal para realizar a comunicação de dados em altas taxas de transferência (40Gbps) e longas distâncias de 80km ou mais com a inserção de repetidores de sinais. Com relação aos tipos de conectores, há uma variedade, sendo os mais comuns: ST, SC, LC, E2000, FC, MTRJ, UM e MPO-MTP.

Algumas curiosidades com relação a cabos: diversos especialistas em redes de computadores costumam utilizar o termo “patch cable” para referenciar qualquer tipo de cabo de rede; Em redes de computadores que possuem um sistema de cabeamento estruturado, serão encontrados

armários de telecomunicação (estudado anteriormente) e neles poderá haver racks contendo patch panel – trata-se de um hardware similar a uma régua que pode conter até 96 portas de conexão do tipo RJ45, sendo os mais comuns os de 24 e 48 portas. Seu principal objetivo é a organização dos cabos ethernet do tipo UTP ou STP e nessa organização os analistas de rede utilizam cabos do tipo: patch cords – cabos ethernet tipo UTP ou STP fabricados de forma industrial e com comprimentos que podem variar entre 0,50cm a 2mts.

Figura 47 - PATCH PANEL, RACK e PATCH CORD.



Com relação a conectores, acredito, meu jovem Padawan, que você já percebeu que existem diversos e modelos que se encaixam perfeitamente no tipo de cabo no qual foi projetado. É importante lembrá-lo que os conectores são tão importantes quanto os cabos. Um conector com um crimpagem ruim irá causar problemas de conexão na rede.

Em uma rede de computadores do tipo LAN, iremos encontrar conectores do tipo RJ45 (macho e fêmea) para serem utilizados em cabos do tipo CAT5 e CAT5e nos modelos UTP e STP. Porém, ainda é possível, na mesma rede, encontrarmos outros tipos de conectores utilizados em cabos de fibra óptica, USB e até no formato serial e paralelo.

Um ponto importante a saber sobre os conectores é que as crimpagem entre o cabo e o conector deve seguir um padrão ou norma. No

caso das redes de computadores do tipo ethernet e que utilizam cabos CAT5, CAT5e e assim por diante, os padrões utilizados são o EIA/TIA 568-A ou EIT/TIA 568-B. A única diferença existente entre os dois padrões 568-A e 568-B está na crimpagem dos fios no conector RJ45, no resto ambos são idênticos.

O padrão EIA/TIA 568-A possui compatibilidade retroativa para esquemas de fiação USOC de um par ou dois pares. Já o padrão EIA/TIA 568-B possui a mesma compatibilidade do 568-A, porém para um único par.

Com relação à crimpagem das posições dos fios (pares), que é a única diferença existente entre ambos os modelos, no EIA/TIA 568-A as posições dos pares no conector RJ45 ficam na seguinte ordem:

<i>CRIMPAGEM/PINAGEM</i>	<i>FIOS (PARES)/ CORES</i>
<i>PINO 1</i>	Listras brancas e verdes
<i>PINO 2</i>	Verde
<i>PINO 3</i>	Listras branca e laranja
<i>PINO 4</i>	Azul
<i>PINO 5</i>	Listras branca e azul
<i>PINO 6</i>	Laranja
<i>PINO 7</i>	Listras branca e marrom
<i>PINO 8</i>	Marrom

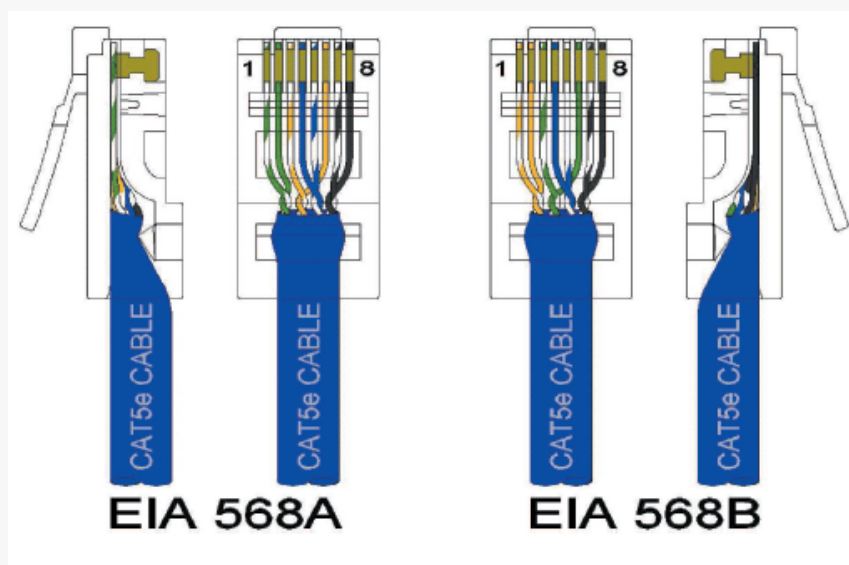
Com relação ao padrão EIA/TIA 568-B, as posições são:

<i>CRIMPAGEM/PINAGEM</i>	<i>FIOS (PARES)/ CORES</i>
<i>PINO 1</i>	Listras brancas e laranja
<i>PINO 2</i>	Laranja

<i>PINO 3</i>	Listras brancas e verde
<i>PINO 4</i>	Azul
<i>PINO 5</i>	Listras brancas e azul
<i>PINO 6</i>	Verde
<i>PINO 7</i>	Listras brancas e marrom
<i>PINO 8</i>	Marrom

Observe que a diferença, conforme comentado, entre ambos os padrões é a mudança de posicionamento junto a pinagem em 2 pares, o par que contém as cores: verde/listras brancas e verdes e o par que contém as cores: laranja e listras brancas e laranja.

Figura 48 - Esquema Crimpagem: 568-A vs. 568-B.



Com relação à comunicação de dados, cada um dos pinos do conector RJ45 irá exercer uma função, a saber:

<i>PINAGEM</i>	<i>FUNÇÃO</i>
<i>PINO 1</i>	+TD (transmissão dados)
<i>PINO 2</i>	- TD (transmissão dados)
<i>PINO 3</i>	+RD (recepção dados)
<i>PINO 4</i>	NULL

<i>PINO 5</i>	NULL
<i>PINO 6</i>	- RD (recepção dados)
<i>PINO 7</i>	NULL
<i>PINO 8</i>	NULL

Um detalhe importante com relação à crimpagem de um cabo ethernet UTP ou STP com o conector RJ45 é o padrão de crimpagem e, nesse contexto, poderemos realizar a crimpagem de três formas: (1) crimpagem direta – nesse formato ambas as extremidades do cabo possuem a crimpagem no mesmo padrão, ou seja, ambas as pontas do cabo recebem, por exemplo, a crimpagem no padrão EAI/TIA 568-A. A crimpagem direta é utilizada para interligar dispositivos finais na rede, como exemplo um PC a um Switch; (2) crimpagem cruzada ou cross-over – nesse padrão as extremidades do cabo recebem padrões diferentes, ou seja, uma ponta do cabo recebe a crimpagem EIA/TIA 568-A e a outra ponta recebe a crimpagem EAI/TIA-568-B. A crimpagem cruzada é utilizada quando há a necessidade de ligar dois dispositivos de rede de forma direta, sem a utilização de um concentrador (Switch ou HUB), exemplo: 2 PCs; (3) crimpagem rollover – nessa crimpagem os pinos no conector possuem posições opostas em cada extremidade do cabo. Essa forma é totalmente diferente das duas anteriores e é projetada para criar uma interface com o dispositivo ao invés de transportar dados.

Figura 49 - Exemplos de Conectores Ethernet.



Figura 50 - Exemplos de conectores - Fibra Óptica.



Figura 51 - Exemplo de conectores coaxial.



**FERRAMENTAS ESSENCIAS  
PARA CRIMPAGEM DE REDES**

**DESCRIÇÃO/FUNÇÃO**



ALICATE PARA CRIMPAR CONECTORES RJ11 E RJ45

ALICATE DE TERMINAÇÃO/INSERÇÃO – PUNCH DOWN –  
USO EM PATCH PANEL PARA CRIMPAGEM DE CABOS





TESTADOR DE CABO DE REDE – RJ11 E RJ45 – UTILIZADO PARA REALIZAR TESTES DE CRIMPAGEM EM CABO ETHERNET UTP E STP

LOCALIZADOR/TESTADOR DE CABOS – AUXILIA NA LOCALIZAÇÃO, IDENTIFICAÇÃO DE PONTOS DE CONEXÃO ENTRE A ÁREA DE TRABALHO E O PATCH PANEL, ALÉM DA POSSIBILIDADE DE REALIZAR TESTES DE CRIMPAGEM.

ALICATE DESCASCADOR UNIVERSAL – AUXILIA NA DECAPAGEM DE CABOS.

Vale lembrar, meu jovem Padawan, que aqui apresentamos algumas ferramentas essenciais para realizarmos a crimpagem e manutenção física em um sistema de cabeamento estruturado. É óbvio que além das apresentadas é necessário possuir outras, tais como alicates de corte de fios, etiquetadoras para realizarmos a identificação dos pontos, ferramentas guias passa fio, sondas e muitos mais.

Outra ferramenta muito importante para um sistema de cabeamento estruturado é a ferramenta scanner para validação e certificação da rede. Esse tipo de ferramenta permite realizar um teste completo em todo o cabeamento estruturado, possibilitando identificar problemas como rompimento de vias, conectores com falha de crimpagem, diagnósticos relacionados a interferência de ruídos, campos eletromagnéticos, medição de taxas de transferência, perdas de inserção,



conversas cruzadas, medição de comprimento e distância, detecção de energia sobre o cabo (POE) e muitos outros testes. No geral, esse tipo de ferramenta possui um custo alto, devido a possibilidades de testes, diagnósticos e resolução de problemas que ela oferece, além da emissão de laudos que atestam e certificam que o sistema de cabeamento estruturado está totalmente em conformidade com uma norma ou padrão técnico.

Figura 52 - Kit Certificador de Redes.



## Referências

---

ABNT. Associação Brasileira de Normas Técnicas, c2022. Página inicial. Disponível em: <<https://www.abnt.org.br>>. Acesso em: 30 ago. 2022.

COMER, Douglas E. Redes de Computadores e Internet. 2. ed. São Paulo: Bookman, 2001.

DANTAS, Mário. Tecnologia de Redes de Comunicação e Computadores. Rio de Janeiro: Axcel Books, 2002.

IEEE. Advancing Technology for humanity – The world's largest technical professional organization for the advancement of technology, c2022. Página inicial. Disponível em: <<https://www.ieee.org>>. Acesso em: 30 ago. 2022.

VPN Tunneling Protocols. Microsoft Docs, c2022. Disponível em: <[http://technet.microsoft.com/en-us/library/cc771298\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771298(WS.10).aspx)>. Acesso em: 30 ago. 2022.

MORINOTO, Carlos Eduardo. Redes: guia prático. Porto Alegre: Sul Editores, 2008.

MORINOTO, Carlos Eduardo. História das redes. Guia do Hardware. Disponível em <<https://www.guiadohardware.net/tutorias/história-redes>>. Acessado em 30 ago. 2022.

PINHEIRO, José Mauricio. Guia completo de cabeamento de redes. Rio de Janeiro: Campus, 2003.

SOARES, Luís Fernando; LEMOS, Guido; COLCHER, Sérgio. Redes de computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

SPONH, Marco Aurélio. Desenvolvimento e análise de desempenho de um "Packet Session Filter. Porto Alegre – RS: CPGCC/UFRGS, 1997.

SPURGEON, Charles E. Ethernet: o guia definitivo. Tradução de Daniel Vieira. São Paulo: Campus, 2000.

TANENBAUM, Andrew. S. Redes de Computadores. 4. ed. Rio de Janeiro: Editora Campus (Elsevier), 2011.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. Building internet firewalls. 2. ed. O'Reilly Media, 2000.

COMO funcionam as redes virtuais privadas. Cisco, 13 out. 2008. Disponível em: <[https://www.cisco.com/c/pt\\_br/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html](https://www.cisco.com/c/pt_br/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html)>.

Acesso em: 30 ago. 2022.

