CENTRO PAULA SOUZA GOVERNO DO ESTADO DE SÃO PAULO

ETEC ALBERT EINSTEIN

REDES DE COMUNICAÇÃO DE DADOS

(TEORIA)

Prof. Wilson Carvalho de Araújo
Curso Técnico de Eletrônica
Setembro de 2014

Apresentação

Esta apostila aborda de forma básica, mas abrangente, os tópicos para o aprendizado de Redes do curso Técnico de Eletrônica.

Seu conteúdo não segue uma ordem específica: procurei organizar com base em minha experiência pessoal e profissional. Faz parte do meu currículo, atuações como Técnico de Eletrônica, Técnico de Telecomunicações, Programador, Analista de Sistemas, Analista de Redes de Telecomunicações e Professor de Curso Técnico de Eletrônica.

Começou como uma transcrição de minhas aulas de Redes, da lousa para um editor de textos. Em um primeiro momento, figuras eram necessárias e recorri à Internet. Complementei com consulta a artigos da Wikipédia, www.teleco.com.br, www.br-linux.org, www.ubuntu-br.org, Microsoft, Apple, Cisco, RFCs, www.iana.org e artigos de revistas eletrônicas como Veja, Exame e etc. Os conteúdos da Internet foram acessados em setembro de 2014 de forma aberta (sem necessidade de login, senha ou qualquer criptografia) e encontrados por meio de buscas simples em buscadores, como o Google.

Por não ter a pretensão de ser um trabalho acadêmico de graduação ou pós-graduação, me senti livre para escrever da forma como os conteúdos surgiram a se acomodaram, quase uma *brain storm*, mas procurando manter a didática para que os alunos, ou quem quer se a consulte, possam compreender seu conteúdo com a menor necessidade possível de um professor por perto.

Sendo uma versão inicial, esta apostila não tem seus assuntos separados em capítulos. Muita coisa deverá ser reposicionada, revista, incluída ou mesmo excluída, conforme sua utilização em aulas assim o indicar. Conforme novos conceitos surgirem, do ponto de vista do Técnico em Eletrônica (nem sempre o será para o de Informática), seu conteúdo tenderá a ser absorvido gerando novas versões. Assim, esta apostila, não é algo que se finalize e considere pronta: deverá evoluir com minhas aulas e experiências.

Em paralelo, há um conjunto de exercícios de laboratórios, também na forma apostilada, idealizados para uso em máquinas virtuais (ambiente MS-Windows e Linux Ubuntu) e com o simulador *Cisco Packet Tracer*.

Da mesma forma como consultei documentos abertos da Internet, permito que esta apostila seja difundida entre os alunos ou por quem encontre nela interesse.

Prof. Wilson Carvalho de Araújo
Prof.wilson@folha.com.br
Setembro de 2014

Índice

Os Nós e as Linhas

As **Redes** de Comunicação, assim como uma rede de pescador, são constituídas de Nós e Linhas.

Os **Nós** são os equipamentos onde as informações são processadas e é o que realmente caracteriza as diferentes redes (podendo abranger inclusive o equipamento dos usuários na origem e no destino).

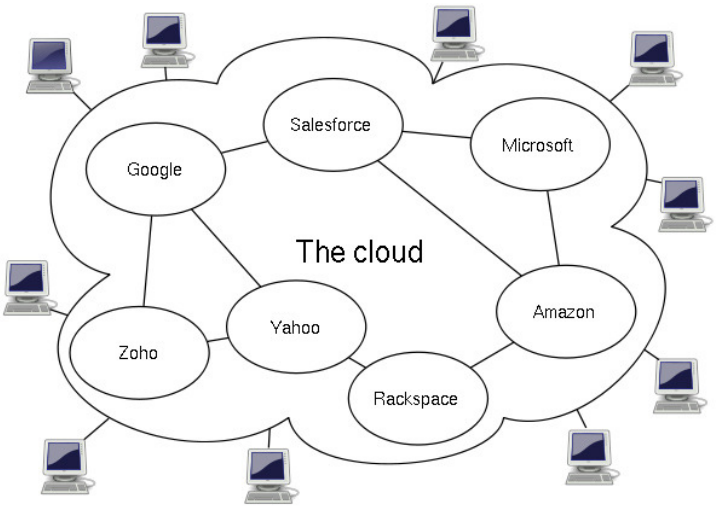
As **Linhas** são os meios de transmissão que interligam cada dois nós adjacentes, passando informações de um nó para outro.

Ao se implantar uma nova rede, os seus nós são específicos, mas as linhas são normalmente "emprestadas" das redes de maior capacidade e ou de maior capilaridade.

Cada novo serviço de comunicações que se desenvolveu, em épocas e por motivações diferentes, evoluiu para uma nova rede de comunicação monosserviço (rede de telegrafia; a rede de telefonia; as redes de TV; etc.).

As redes são acessadas por interesse em um serviço que ela disponibilize. Os equipamentos envolvidos, caminho que a mensagem toma ou como é tratada, pouco interessa ao usuário final da rede; à ele interessa o serviço. Por não se ver/perceber o que há no interior das redes, do ponto de vista do usuário, diz-se que são opacas, como uma nuvem. Assim, para representar uma rede de forma genérica, o fazemos através do desenho de uma nuvem.

Quando se diz que um serviço está "*na nuvem*" (como *cloud computing*), se refere à disponibilidade do serviço em um ambiente externo. Onde está o servidor, qual tecnologia ou técnica utiliza, tipo de equipamento, conexões, etc., não interessam ao usuário.



Redes de Acesso e Backbone

Conceitualmente a UIT (União Internacional das Telecomunicações, ITU para a sigla em inglês) divide as redes de grande porte em **redes de acesso** e **redes de backbone**:

- **Redes de acesso** são aquelas que os usuários se conectam para ter acesso aos serviços. Exemplos: na telefonia fixa, o aparelho telefônico do usuário, a sua linha telefônica e a central

local que atende à essa linha; na telefonia celular, a estação móvel do usuário (aparelho) e a estação rádio base (ERB) que atende a essa estação móvel.

- **Redes de backbone** são as partes de alta capacidade que servem para a interconexão das diferentes redes de acesso. Exemplos: na telefonia fixa, as centrais trânsito (locais ou interurbanas); na telefonia celular, a central de comutação e controle (CCC) e gateways.

Em uma rede de computadores, para se possibilitar o controle de erros (detecção e, por vezes, a correção dos erros) e o controle de fluxo (evitando que um computador mais rápido "entupa" o mais lento) nos enlaces usam-se os chamados **protocolos de comunicação**.

Órgãos de Padronização

A padronização das redes de computadores foi essencial no início da década de 80, e foi um dos principais motivos do grande crescimento observado nas redes. Antes da criação do modelo OSI pela (visto adiante), os sistemas eram todos baseados em soluções proprietárias e não permitiam a interoperabilidade dos fabricantes. Este fato gerava um grande desconforto aos usuários da tecnologia, que ficavam atrelados a soluções de um único fabricante. Se eles decidissem comprar a solução de uma determinada marca, eram obrigados a expandir com a mesma marca, o que era ótimo para o dono da marca e péssimo para o cliente, principalmente na hora de negociar preço.

Os padrões foram criados para permitir que uma solução tecnológica única e padronizada pudesse ser implementada por diferentes fabricantes. Inicialmente os fabricantes acreditavam que a padronização limitava a expansão tecnológica, mas o que aconteceu ao longo dos anos foi que os fabricantes implementavam o padrão e ofereciam a seus clientes, como uma solução de valor agregado, as capacidades avançadas por eles, criadas como um valor agregado.

A padronização em rede de computadores pode ser dividida em dois tipos:

Padronização da indústria: É o tipo de padronização formal. Em geral esses padrões são desenvolvidos por entidades de padronização que funciona como um grande fórum, do qual fazem parte representante das indústrias, dos Governos, dos laboratórios das universidades e dos usuários. É também denominado **Padrão de Direito**. Alguns exemplos são:

- **IEEE** (Institute of Electrical and Electronics Engeneers): Possui engenheiros elétricos e eletrônicos de praticamente todos os países do mundo. Sua meta é promover conhecimento no campo da engenharia elétrica, eletrônica e computação. Um de seus papéis mais importantes é o estabelecimento de padrões para formatos de computadores e dispositivos.

- **ANSI** (American National Standards Organization): É um órgão de padronização criado nos Estados Unidos, em 1918. Possuem aproximadamente 1000 associados entre empresas, organizações, agências de governo e instituições internacionais. A ANSI trabalha em parceria com a IEC. Seu equivalente no Brasil seria a ABNT.

- **IEC** (International Electrotechnical Commission): É uma organização internacional de padronização de tecnologias elétricas, eletrônicas e relacionadas. Alguns dos seus padrões são desenvolvidos juntamente com a Organização Internacional para Padronização (ISO). A sede da IEC, fundada em 1906, é localizada em Genebra, Suíça.

- **EIA** (Electronic Industries Association): É uma organização privada para as indústrias de produtos eletrônicos nos Estados Unidos. A EIA é credenciada pela ANSI para desenvolver padrões e especificações técnicas de componentes eletrônicos, telecomunicações e Internet.

- **TIA** (Telecommunications Industry Association): Associação das indústrias das telecomunicações.

- **ISO** (International Organization for Standardization): É uma organização internacional de padronização que pode ser considerada a maior do mundo. A ISO desenvolve e estabelece padrões nem diversas áreas do desenvolvimento tecnológico e é formada por diversas organizações de diferentes países.

- **UIT (ITU)** - A União Internacional de Telecomunicações (UIT) (em francês: *Union internationale des télécommunications*; em inglês: *International Telecommunication Union*) é a agência da ONU especializada em tecnologias de informação e comunicação. Destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais, a agência é composta por todos os 193 países membros da ONU e por mais de 700 entidades do setor privado e acadêmico. Foi fundada como *International Telegraph Union* (União Internacional de Telégrafos), em Paris, no dia 17 de maio de 1865 e é hoje a organização internacional mais antiga do mundo. Suas principais ações incluem estabelecer a alocação de espéctros de ondas de rádio e organizar os arranjos de interconexões entre todos os países permitindo, assim, ligações de telefone internacionais. É uma das agências especializadas da Organização das Nações Unidas (ONU), tendo sua sede em Genebra, na Suíça, próximo ao principal campus da ONU. Os padrões internacionais que são produzidos pela UIT são denominados **Recomendações** (com a primeira letra em maiúsculo, para diferenciar do significado comum da palavra recomendação).

Padronização de Fato: Trata das tecnologias que acabaram virando padrões porque simplesmente o produto ganhou mercado. Como exemplos há o SNA da IBM, o Windows da Microsoft e o UNIX.

RFC

As **Request for Comments** (*pedido para comentários*) são documentos técnicos desenvolvidos e mantidos pelo **IETF** (*Internet Enginnering Task Force*), instituição que especifica os padrões que serão implementados e utilizados em toda a Internet.

Cada RFC detalha o funcionamento de todos os aspectos do protocolo proposto. A *RFC 3286*, por exemplo, possui todas as especificações necessárias para a implementação do controle de fluxo de dados, também conhecido como *streaming*, e assim permitir que sites como o Youtube funcionem.

Se um padrão se torna obsoleto ou mudanças são necessárias, é gerado um outro arquivo chamado *Request for Change*, onde pessoas que possuem o conhecimento necessário sobre o assunto oferecem soluções para o problema proposto. Caso seja aprovado pelo Comitê, esse documento se torna uma nova RFC, com uma numeração diferente da original (que não é excluída), ficando disponível para consulta.

Existe até uma RFC estabelece como funciona o processo de elaboração e aprovação de uma RFC (*RFC 2826*) para que qualquer pessoa que possa oferecer uma solução para um problema existente possa dar a sua contribuição e, se aprovado, será implementado em toda a Internet com o nome do autor original.

Formas de Conexão

As comunicações em uma rede podem ser orientadas ou não orientadas à conexão.

À semelhança do que ocorre em uma chamada telefônica, na forma **orientada à conexão** a comunicação se dá em três fases: estabelecimento da conexão (tom de discar, discagem, roteamento, tons de supervisão da chamada); transferência de dados (conversação); desconexão (liberação dos recursos utilizados quando os usuários desligam os aparelhos).

Na comunicação **não orientada à conexão** só existe a fase de transferência de dados, pois, como o próprio nome diz, nenhuma conexão é estabelecida (ela já estará disponível, como em uma linha privativa). Neste caso, como não há negociação, não há como indicar (ou negociar) os parâmetros que se querem para esta comunicação; dizendo-se, por isto, que as comunicações não orientadas à conexão são de melhor esforço (*best efort*), sem QoS (*Quality of Service*). Isto não significa que estas comunicações não possuem qualidade e sim que esta qualidade não é controlada.

Há aplicações que exigem comunicações orientadas à conexão como, por exemplo, as transferências de arquivos (que toleram atrasos, mas não toleram erros). Existem outras aplicações que necessitam comunicações não orientadas à conexão como, por exemplo, a troca de informações de um Sistema de Gerência (que privilegiam rapidez, tolerando algum grau de erros).

Comutação por Circuitos e por Pacotes

Comutação é o processo de chaveamento que define como uma mensagem é direcionada por uma ou mais redes. As comunicações podem ocorrer por duas formas de comutação: por **circuitos** ou por **pacotes**.

A **comutação por circuito** é a usada, por exemplo, pelas centrais telefônicas onde se reservam fisicamente os recursos que ficam dedicados aos interlocutores durante todo o tempo da comunicação. Nesta, os dados cursam todo o percurso a uma mesma velocidade, sem nenhum processamento nos nós sendo, portanto, transparente aos protocolos.

Em caso de falhas em um nó ou em um enlace de uma rede comutada por circuitos, as comunicações que usavam esses recursos caem, pois este tipo de rede não tem a capacidade de *re-rotear* (reorientar automaticamente) tais comunicações.

Embora se dê a rede telefônica como exemplo para a comutação de circuitos, também existem redes de dados que usam esta técnica.

A **comutação de pacotes** surge com a comunicação de dados, onde a mensagem inteira pode ser subdividida em pacotes e estes podem trafegar simultaneamente pela rede, embora cada qual em um trecho distinto. Quando os pacotes têm tamanho fixo e relativamente pequeno, chamamos **comutação de células**.

Enquanto a comutação de circuitos é sempre orientada à conexão, a comutação de pacotes pode ser orientada à conexão (quando se usam **circuitos virtuais**) ou não orientada à conexão (quando se usam **datagramas**).

Um **datagrama** é uma unidade de transferência básica associada a uma rede de comutação de pacotes em que a entrega, hora de chegada, e a ordem não são garantidos.

O termo *datagrama* é muitas vezes considerado sinônimo de "*pacote*", mas há algumas diferenças. O termo **pacote** se aplica a qualquer mensagem formatada como um pacote, enquanto o termo **datagrama** é geralmente reservado para os pacotes de um serviço "*não confiável*". Um serviço "não confiável" não notifica o usuário se a entrega falhar.

Diferente das redes comutadas por circuito, as redes comutadas por pacotes, quando congestionadas, degradam os tempos de resposta, mas sempre aceitam uma nova solicitação de comunicação.

A denominação **circuitos virtuais** se dá porque os recursos são reservados apenas logicamente. Estes ainda podem ser do tipo **permanente** (**PVC** – *Permanet Virtual Circuit*) onde o circuito permanece estendido durante toda a comunicação e o caminho por onde passa a informação é fixo, ou do tipo **comutados** (**SVC** – *Switched Virtual Circuit*) onde se deve restabelecer a conexão a cada nova comunicação com a possível escolha de um novo caminho.

No caso dos datagramas, a comunicação não é orientada à conexão e, portanto, não há qualquer reserva de recursos da rede, nem física nem logicamente. Cada pacote passa em cada nó da rede por uma nova decisão de roteamento e, por isso, é possível que pacotes transmitidos primeiro cheguem depois ao destino (sejam entregues fora de ordem) necessitando ser reordenados.

Tipos de Redes

No início de sua popularização (uso civil), as redes existiam principalmente dentro de escritórios (rede local), mas com o passar do tempo a necessidade de trocar informações entre esses módulos de processamento aumentou, dando vez a diversos outros tipos de rede. Assim, as redes passaram a ser categorizadas conforme sua abrangência:

A seguir, temos os principais tipos:

- **LAN – Rede Local**

As chamadas **Local Area Networks**, ou **Redes Locais**, interligam computadores presentes dentro de um mesmo espaço físico. Isso pode acontecer dentro de uma empresa, de uma escola ou dentro da sua própria casa, sendo possível a troca de informações e recursos entre os dispositivos participantes.

- **WLAN – Rede Local Sem Fio**

A **Wireless LAN**, ou **Rede Local Sem Fio** é, como o nome sugere, uma evolução da LAN, onde foram retirados os cabos de interconexão dos equipamentos. Esse tipo de rede é bastante usado tanto em ambientes residenciais quanto em empresas e em lugares públicos.

- **MAN – Rede Metropolitana**

Imaginemos, por exemplo, que uma empresa possui dois escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso existe a **Metropolitan Area Network**, ou Rede Metropolitana, que conecta diversas Redes Locais dentro de algumas dezenas de quilômetros. Através da MAN é possível uma livraria, autopeças, farmácia, etc., consultar a existência do produto desejado em um estoque central ou em outra unidade de vendas (loja).

- **WMAN – Rede Metropolitana Sem Fio**

Esta é a versão sem fio da MAN, com um alcance de dezenas de quilômetros.

- **WAN – Rede de Longa Distância**

A **Wide Area Network**, ou **Rede de Longa Distância**, possui abrangência muito além da **MAN**, como um país, um continente, ou mesmo entre continentes.

- **WWAN – Rede de Longa Distância Sem Fio**

Como versão sem fio da WAN, a WWAN, ou Rede de Longa Distância Sem Fio, alcança diversas partes do mundo. Justamente por isso, a WWAN está mais sujeita a ruídos.

- **SAN – Rede de Área de Armazenamento**

As **Storage Area Networks**, ou Redes de Área de Armazenamento, são utilizadas para fazer a comunicação de um servidor e outros computadores, ficando restritas a isso.

Há outras denominações que surgem conforme a evolução de dispositivos e popularização de aplicações, como:

- **PAN – Rede de Área Pessoal**

As redes do tipo **Personal Area Network**, ou Redes de Área Pessoal, são usadas para que dispositivos pessoais se comuniquem dentro de uma distância bastante limitada. Um exemplo disso são as redes Bluetooth e USB. As redes assim formadas são também denominadas **Piconets**.

- **CAN – Rede de um Campus**

As **Campus Area Networks** são as redes maiores que as redes locais, interligando vários prédios de um campus universitário ou centro empresarial, por exemplo, mas de forma muito menor que uma MAN.

Assim, esta lista apresenta apenas as denominações mais comuns de redes, onde mesmo entre os citados ainda poderíamos descrever as **WPAN** (Wireless PAN) ou **WCAN** (Wireless CAN).

Internet, Intranet, Extranet e VPN

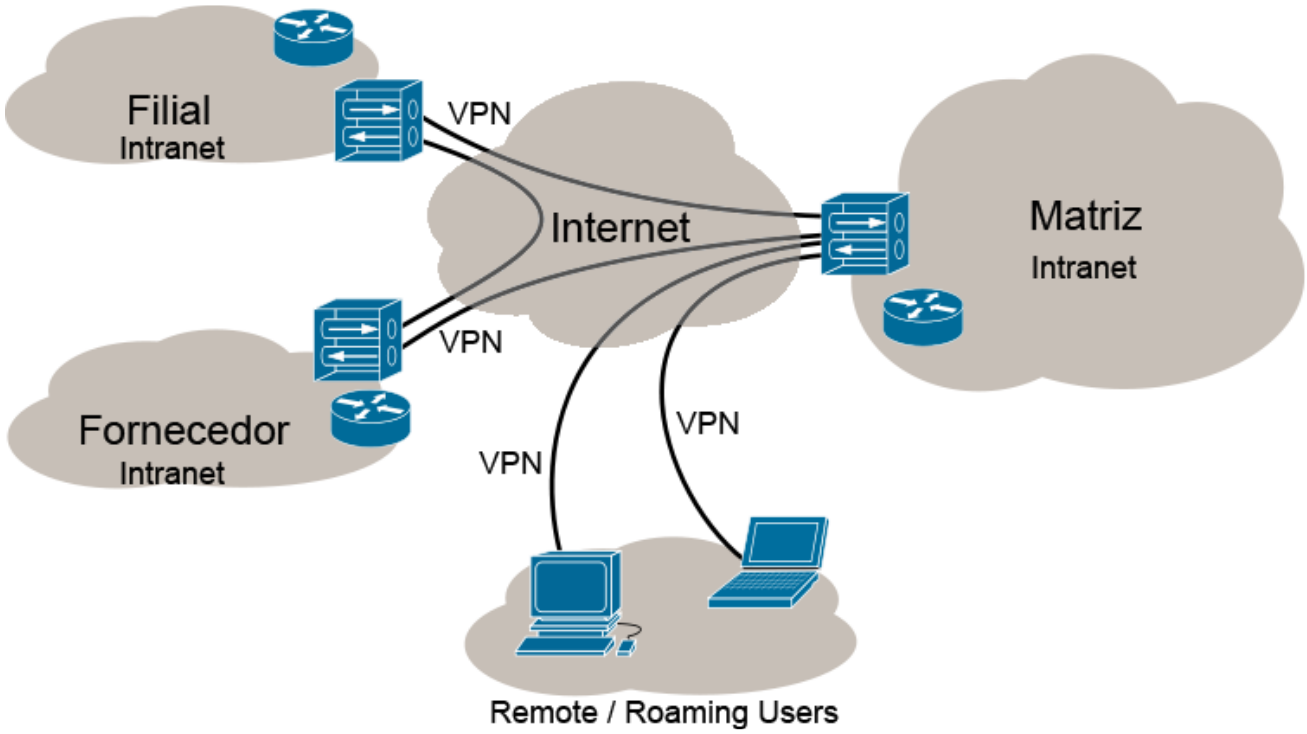
A ***Internet*** é um conglomerado de redes locais espalhadas pelo mundo, o que torna possível a interligação entre os computadores utilizando o protocolo de internet.

Uma ***intranet*** é uma rede corporativa que está protegida atrás de firewalls e utiliza tecnologias de Internet. Mesmo utilizando o mesmo protocolo TCP/IP que a Internet, elas operam como redes privadas com acesso limitado. Apenas empregados com senhas e códigos de acesso podem acessá-las. As intranets estão limitadas às informações relacionadas com a empresa (informação pertinente, proprietária e sensível). Firewalls protegem intranets de acessos externos não autorizados. A intranet ainda possibilita o uso de mais protocolos de comunicação, não somente o HTTP usado pela internet, geralmente utilizado em servidores locais instalados na empresa.

Uma ***extranet*** é uma "*extended intranet*". As transmissões das *extranets* são realizadas via Internet porém oferecendo privacidade e segurança através da criação de canais seguros de transmissão de dados denominados de túneis. Estes túneis utilizam criptografia e algoritmos de autenticação.

As *extranets* troca de informações de forma segura entre as intranets das corporações e dos seus parceiros, fornecedores e clientes.

A **VPN** (*Virtual Private Network*) é o conceito que permite conectar dois hosts ou mesmo duas redes utilizando a Internet, mas de forma segura e protegida. A VPN possibilita a criação dos túneis que interligam as intranets (para formação de extranets) ou de conexão simples à intranet mas com privacidade e segurança de comunicação.



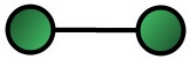
Conexão de intranets, formando extranets, pela Internet, com o uso de VPNs.

Topologia de Redes

A topologia de uma rede indica como os equipamentos estão interligados entre si. Quando faz referência à conexão entre as máquinas, é denominada **topologia física**. Quando diz respeito a forma como os equipamentos trocam informações entre si, é denominada topologia lógica.

- **Peer-to-peer**

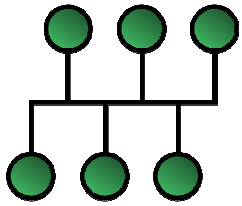
Do inglês par-a-par ou simplesmente **ponto-a-ponto**, com sigla **P2P**, é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. As redes P2P podem ser configuradas em casa, em Empresas e ainda na Internet. Todos os pontos da rede devem usar programas compatíveis para ligar-se um ao outro. Uma rede peer-to-peer pode ser usada para compartilhar músicas, vídeos, imagens, dados, enfim qualquer coisa com formato digital.



A topologia ponto a ponto é a mais simples. Une dois computadores, através de um meio de transmissão qualquer. Dela podemos formar novas topologias, incluindo novos nós em sua estrutura.

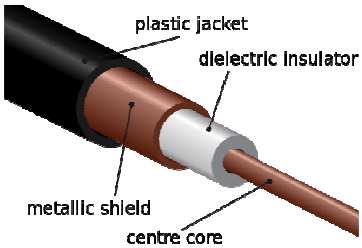
- **BUS**

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



Para contornar o problema de colisões existem mecanismos como o protocolo **CSMA/CD** (*Carrier Sense Multiple Access / Colision Detect*). Nele, o equipamento "escuta" a rede; caso algum outro nó esteja fazendo sua transmissão ele espera um tempo para então voltar a escutar e verificar se a rede está livre. Outra característica é que, se quando o canal estiver ocioso e o nó for transmitir e outro o fizer no mesmo momento, o CSMA/CD realiza a detecção de colisão, fazendo com que os dois parem a transmissão e esperem tempos aleatórios e distintos para voltar a escutar a rede e tentar nova transmissão.

Essa topologia utiliza cabos coaxiais. Para cada barramento existe um único cabo, que vai de uma ponta a outra. O cabo é seccionado em cada local onde um micro será inserido na rede. Com o seccionamento do cabo formam-se duas pontas e cada uma delas recebe um conector BNC. No micro é colocado um "T" conectado à placa que junta as duas pontas. Embora ainda existam algumas instalações de rede que utilizam esse modelo, é uma tecnologia obsoleta. Existe uma forma um pouco mais complexa dessa topologia, denominada barramento distribuído, no qual o mesmo começa em um local chamado raiz e se expande aos demais ramos (Ligados a um conector). A diferença entre este tipo de barramento e o barramento simples é que, neste caso a rede pode ter mais de dois pontos terminais.



cabo coaxial


conector BNC

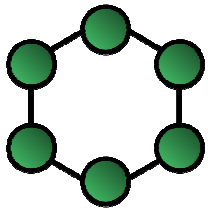

conector BNC T

- **Line**

A topologia linear coloca um link de duas vias entre um computador e outro. No entanto, isso era caro nos primeiros dias da computação, uma vez que cada computador (exceto os que estão em cada extremidade) necessitava de dois receptores e dois transmissores.

- **Ring**

A topologia de **rede em anel** (**ring**) consiste em estações conectadas através de um circuito fechado, em série (anel). O anel não interliga as estações diretamente, mas consiste de uma série de repetidores ligados por um meio físico, sendo cada estação ligada a estes repetidores. É uma configuração em desuso, exceto para backbones.



Redes em anel são capazes de transmitir e receber dados em configuração unidirecional. O projeto dos repetidores é mais simples e torna menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em seqüência ao destino, pois sendo unidirecional evita o problema do roteamento.

Numa rede em anel cada estação está conectada a apenas duas outras estações, quando todas estão ativas. Uma desvantagem é que se, por acaso apenas uma das máquinas falhar, toda a rede pode ser comprometida, já que a informação só trafega em uma direção, que no caso é circular.

Há um atraso de um ou mais bits em cada estação para processamento de dados. A cada estação inserida, há um aumento de retardo (***delay***) na rede. É possível usar anéis múltiplos para aumentar a confiabilidade e o desempenho.

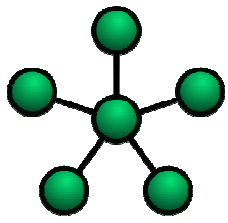
Em termos práticos, nessas redes a fiação, que geralmente é realizada com cabos coaxiais, possui conectores BNC em formato de "T", onde uma das pontas é conectada ao computador anterior e a outra levará a informação adiante, para a máquina seguinte.

Em uma rede em anel, cada nó tem sua vez para enviar e receber informações através de um ***token*** (ficha, em inglês). Caso o token esteja vazio, a máquina que deseja transmitir o preenche com os dados. Caso o token esteja preenchido e não forem destinatárias, repassam a mensagem adiante e aguardam um token vazio. As máquinas que recebem a mensagem verificam se é endereçada à elas, Caso seja, retiram o conteúdo do token (mensagem) e entregam o token vazio à máquina seguinte.

Somente o nó com o token pode enviar informações. Todos os outros nós devem esperar o token chegar. Com a evolução, passou-se a utilização uma topologia híbrida,ou seja, utiliza-se cabos de rede RJ45 e um hub (vistos mais adiante) que faz a topologia anel lógica no seu interior. Pode-se ligar entre 30 a 50 computadores com taxas de transferência de 50 Mbps.

- **Star**

A topologia estrela (**star**) é caracterizada por um elemento central que gerencia o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada nó, resultando daí a designação *estrela*.



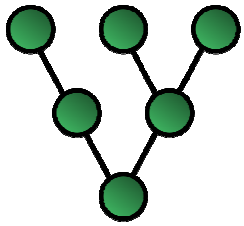
Na topologia estrela todas as conexões partem de um ponto centralizado, normalmente um hub ou switch.

Toda informação enviada de um nó para outro é enviada primeiro ao dispositivo que fica no centro da estrela, os dados não passam por todos os hosts. O concentrador encarrega-se de encaminhar o sinal para as estações solicitadas.

Existem também redes estrela com conexão passiva (similar ao barramento), na qual o elemento central nada mais é do que uma peça mecânica que atrela os enlaces entre si, não interferindo no sinal que flui por todos os nós, da mesma forma que o faria em redes com topologia barramento. Mas este tipo de conexão passiva é mais comum em redes ponto-a-ponto lineares, sendo muito pouco utilizado já que os dispositivos concentradores (HUBs, Switches, e outros) não apresentam um custo tão elevado se levarmos em consideração as vantagens que são oferecidas.

Como este tipo de topologia possui um concentrador, caso um equipamento apresente problemas, a rede permanece estável. Porém, um problema no equipamento que é o centro da estrela pode paralisar a rede.

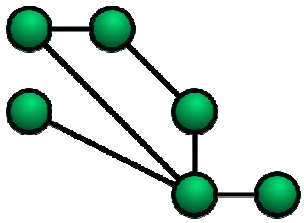
- **Tree**



Uma topologia em árvore é uma rede, que, pela sua configuração de suas interligações, se assemelha a uma árvore, no sentido em que as suas ramificações tendem a convergir para uma raiz, ou uma origem (como por exemplo, em árvore genealógica). Introduz-se, portanto, a noção de raiz e descendência.

Nas redes em árvores devem ser tomados cuidados adicionais, pois cada ramificação significa que o sinal deverá se propagar por dois caminhos diferentes. A menos que estes caminhos estejam perfeitamente casados, os sinais terão velocidades de propagação diferentes e refletirão os sinais de diferentes maneiras. Em geral, redes em árvore, trabalham com taxas de transmissão menores do que as redes em barramento comum.

- **Mesh**



Na rede em malha (**mesh**), cada nó pode se comunicar com vários outros. Na figura ao lado, temos uma rede mesh parcial, onde as máquinas comunicam com várias outras, mas não todas. Caso as conexões sejam entre todos os nós é denominada Fully Connected.

Esta topologia é muito utilizada em várias configurações, pois facilita a instalação e configuração de dispositivos em redes mais simples, já que são vários os caminhos possíveis por onde a informação pode fluir da origem até o destino.

Neste tipo de rede, o tempo de espera é reduzido e eventuais problemas não interrompem o funcionamento da rede. Um problema encontrado é em relação às interfaces de rede, já que para cada segmento de rede seria necessário instalar, em uma mesma estação, um número equivalente de placas de rede. Uma vez que cada estação envia sinais para todas as outras com frequência, a largura da banda de rede não é bem aproveitada.

Ainda no que diz respeito às conexões de rede, podemos citar as seguintes técnicas de formação de topologias:

- **Daisy-Chain**

Exceto para redes conectadas em estrela, a maneira mais fácil de adicionar mais computadores em uma rede é por encadeamento (Daisy-Chaining), ou seja, ligar cada computador em série com o próximo. Se a mensagem se destina a um computador distante no caminho da linha, cada sistema a retransmite em sequência, até que ela chegue ao seu destino. Uma rede encadeada (Daisy-Chained) pode assumir duas formas básicas: **linear e anel**.

- **Ad Hoc**

Ad hoc é uma expressão latina que significa "*para esta finalidade*" ou "*com este objetivo*". Geralmente se refere a uma solução destinada a atender a uma necessidade específica ou resolver um problema imediato - e apenas para este propósito, não sendo aplicável a outros casos. Portanto, tem um caráter temporário. Em um processo *ad hoc*, nenhuma técnica de uso geral é empregada, pois as fases variam a cada aplicação, conforme a situação assim o requeira. O processo nunca é planejado ou preparado antecipadamente.

Tecnicamente, as redes *ad hoc* são um tipo de rede que não possui um nó ou terminal especial - geralmente designado como ponto de acesso - para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos. Assim, uma rede de computadores ad hoc é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas dos terminais vizinhos. Um dos protocolos usados para redes *ad hoc* sem fio é o OLSR (*Optimized Link State Routing*).

Geralmente, numa rede *ad hoc* não há topologia predeterminada, nem controle centralizado. Redes *ad hoc* não requerem uma infraestrutura tal como um *backbone* ou pontos de acesso configurados antecipadamente. Os nós (ou nodos) se comunicam com conexão física entre eles, criando uma rede *on the fly*, na qual alguns dos dispositivos da rede fazem parte dela apenas durante a sessão de comunicação - ou, no caso de dispositivos móveis ou portáteis, enquanto estão a certa proximidade do restante da rede.

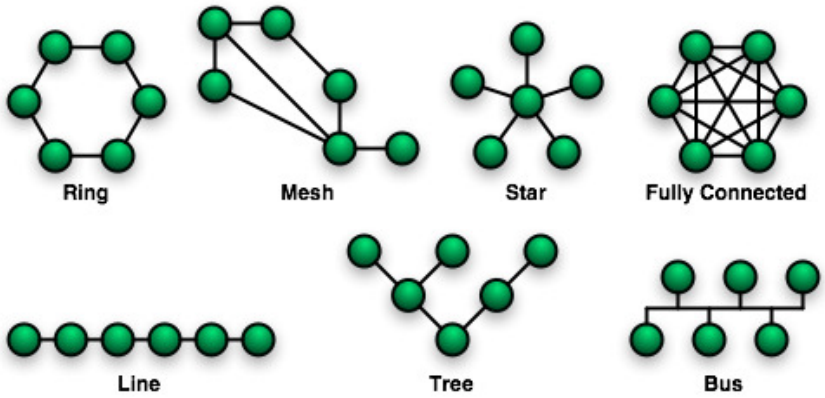
No modo *ad hoc* o usuário se comunica diretamente com outros, como em P2P. Este modelo, pensado para conexões pontuais, só recentemente passou a prover mecanismos robustos de segurança, por conta do fechamento de padrões mais recentes (802.11i).

- **Rede Mista ou híbrida**

Numa topologia híbrida, o desenho final da rede resulta da combinação de duas ou mais topologias de rede. A combinação de duas ou mais topologias de rede permite-nos beneficiar das vantagens de cada uma das topologias que integram esta topologia. Embora muito pouco usada em redes locais, uma variante da topologia em malha, a malha híbrida, é usada na Internet e em algumas WANs. A topologia de malha híbrida pode ter múltiplas ligações entre várias localizações, mas isto é feito por uma questão de redundância, além de que não é uma verdadeira malha porque não há ligação entre cada um e todos os nós, somente em alguns por uma questão de *backup*.

- **Resumindo:**

A figura seguinte ilustra resumidamente os principais tipos de topologias de redes.



Exemplos de Topologias de Redes

Formas de Endereçamento de Mensagens

Denomina-se **domínio de difusão** como sendo um segmento lógico de uma rede de computadores em que um computador ou qualquer outro dispositivo conectado à rede é capaz de se comunicar com outro sem a necessidade de utilizar um dispositivo de roteamento.

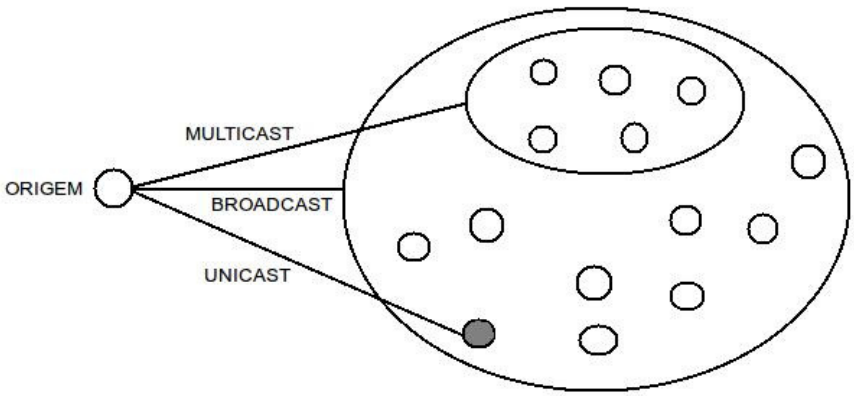
Existem, basicamente, três formas de endereçamento que podem ser implementadas em uma rede: **unicast**, **multicast** e **broadcast**.

No endereçamento **unicast**, a origem envia uma mensagem para apenas um destinatário, ou seja, apenas um dispositivo receberá a mensagem.

No endereçamento **broadcast**, a origem envia uma mensagem para todos os dispositivos da rede. Nesta situação, diz-se que a mensagem atingiu todos os hosts de seu **domínio de difusão**, sendo por isso, muitas vezes denominado **domínio de broadcast**. É importante ressaltar que uma mensagem de broadcast não sai da rede (não atinge outras redes, fica restrita ao domínio da rede).

Switches e *Hubs* encaminham pacotes de broadcast (*routers* não) e por isso formam somente um domínio de broadcast. Já um roteador (*router*) não encaminha broadcasts e por isso cada porta dele forma um domínio de broadcast.

No endereçamento **multicast**, a origem envia uma mensagem para um grupo de dispositivos chamado grupo multicast. O grupo multicast é um subconjunto dos dispositivos que formam a rede, ou seja, vários recebem a mensagem, mas não todos.



O Host

Por definição, **host** é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos. Essas máquinas são responsáveis por oferecer recursos, informações e serviços aos usuários ou clientes. Por essa abrangência, a palavra pode ser utilizada como designação para diversos casos que envolvam uma máquina e uma rede, desde computadores pessoais a roteadores.

Servidores de hospedagem de sites também podem ser considerados hosts. Esses serviços contam com uma máquina central, o host, que fica conectada 24 horas por dia, enquanto armazena e envia os dados das páginas para a Internet. Essa máquina é responsável pelo armazenamento de todos os arquivos contendo os códigos das páginas que se encontram online.

O termo pode ainda ser usado para indicar outras formas de rede que não a Internet. Um roteador que controla a rede onde diversas máquinas se conectam por meio de um número de IP, por exemplo, também pode ser considerado um host.

Arquiteturas de Redes

Arquitetura de rede é como se designa um conjunto de camadas e protocolos de rede. A especificação de uma arquitetura deve conter informações suficientes para permitir que um implementador desenvolva o programa ou construa o hardware de cada camada, de forma que ela obedeça corretamente ao protocolo adequado

O Modelo OSI da ISO

O Modelo OSI (*Open System Interconnection*) é um modelo de referência da ISO (*International Standards Organization*), criado em 1970 e formalizado em 1983, idealizado para viabilizar uma solução aberta para redes de Comunicação. O modelo OSI se tornou referência para a maioria das arquiteturas de redes atuais. As sete camadas do RM-OSI (Reference Model OSI) são:

- **Camada 7 - Aplicação**: A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizados para promover uma interação entre a máquina-usuário (máquina destinatária e o usuário da aplicação). Esta camada também disponibiliza os recursos (protocolo) para que tal comunicação aconteça, por exemplo, ao solicitar a recepção de e-mail através do aplicativo de e-mail, este entrará em contato com a camada de Aplicação do protocolo de rede efetuando tal solicitação (POP3 ou IMAP).

- **Camada 6 - Apresentação**: A camada de Apresentação, também chamada *camada de tradução*, converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado na transmissão desse dado, ou seja, um formato entendido pelo protocolo usado. Trata a sintaxe (disposição dos diferentes campos pelos *flags* de delimitação) e a semântica (significado dos campos como compressão de dados ou criptografia) – para que os *bits* transmitidos tenham o mesmo significado na origem e no destino;

- **Camada 5 - Sessão**: A camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma comunicação, definindo como será feita a transmissão de dados,

pondo marcações nos dados que serão transmitidos. Se porventura a rede falhar, os computadores reiniciam a transmissão dos dados a partir da última marcação recebida pelo computador receptor. Resumidamente, organiza o diálogo fim-a-fim (*half-duplex*, *full-duplex*, etc...).

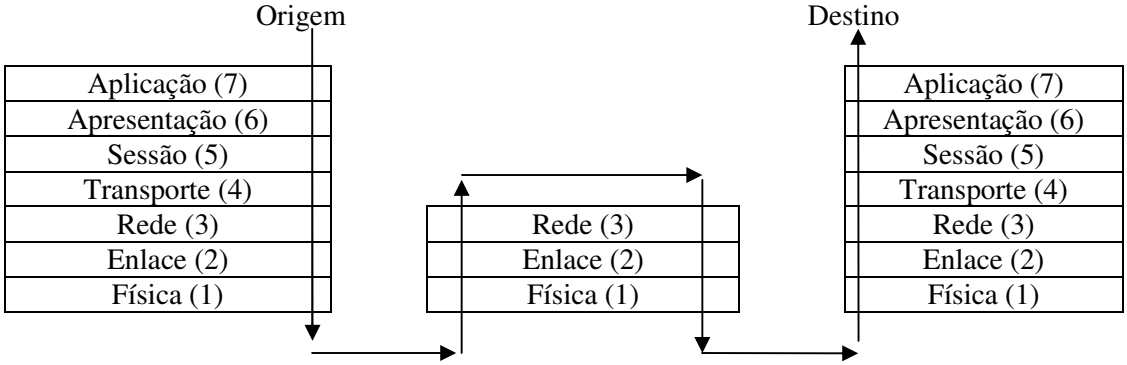
- **Camada 4 - Transporte**: Garante a integridade fim-a-fim dos "bits" (Controle de Erros e Fluxo fim-a-fim). A camada de transporte é responsável por receber os dados enviados pela camada de sessão e segmentá-los para que sejam enviados a camada de rede, que por sua vez, transforma esses segmentos em pacotes. No receptor, a camada de Transporte realiza o processo inverso, ou seja, recebe os pacotes da camada de rede e junta os segmentos para enviar à camada de sessão. Isso inclui controle de fluxo, ordenação dos pacotes e a correção de erros, tipicamente enviando para o transmissor uma informação de recebimento, garantindo que as mensagens sejam entregues sem erros na sequência, sem perdas e duplicações. A ISO define o protocolo de transporte para operar em dois modos: *orientado a conexão* e *não-orientado a conexão*.

- **Camada 3 - Rede**: Define o roteamento (rotas até o destino) e promove o controle de congestionamento da rede enquanto se mantém a qualidade de serviço requerido pela camada de transporte. A camada de rede realiza roteamento de funções. **Roteadores** operam nesta camada, enviando dados em toda a rede estendida e tornando por exemplo, a *Internet* possível.

- **Camada 2 - Enlace**: A camada de ligação de dados também é conhecida como de enlace ou link de dados. Esta camada detecta e, opcionalmente, corrige erros que possam acontecer no nível físico. É responsável por controlar o fluxo (recepção, delimitação e transmissão de quadros) e também estabelece um protocolo de comunicação entre sistemas diretamente conectados. Os **switches** operam nesta camada.

- **Camada 1 - Física**: Adéqua a interface dos computadores à Rede (a conexão física). A camada física define especificações elétricas e físicas dos dispositivos. Em especial, define a relação entre um dispositivo e um meio de transmissão, tal como um cabo de cobre ou um cabo de fibra óptica. Isso inclui o layout de pinos, tensões, impedância da linha, especificações do cabo, temporização, hubs, repetidores, adaptadores de rede, adaptadores de barramento de host e etc. A camada física, a camada mais baixa do modelo OSI, diz respeito à transmissão e recepção do fluxo de bits brutos não-estruturados em um meio físico. Ele descreve as interfaces elétricas óptica, mecânicas e funcionais para o meio físico e transporta sinais para todas as camadas superiores. Os **hubs** operam nesta camada.

A figura seguinte ilustra a comunicação entre origem e destino envolvendo três nós, utilizando o modelo OSI.



Caminho físico em uma comunicação envolvendo três nós.

Os Protocolos utilizados em cada camada adicionam bits aos pacotes promovendo o ***Overhead***.

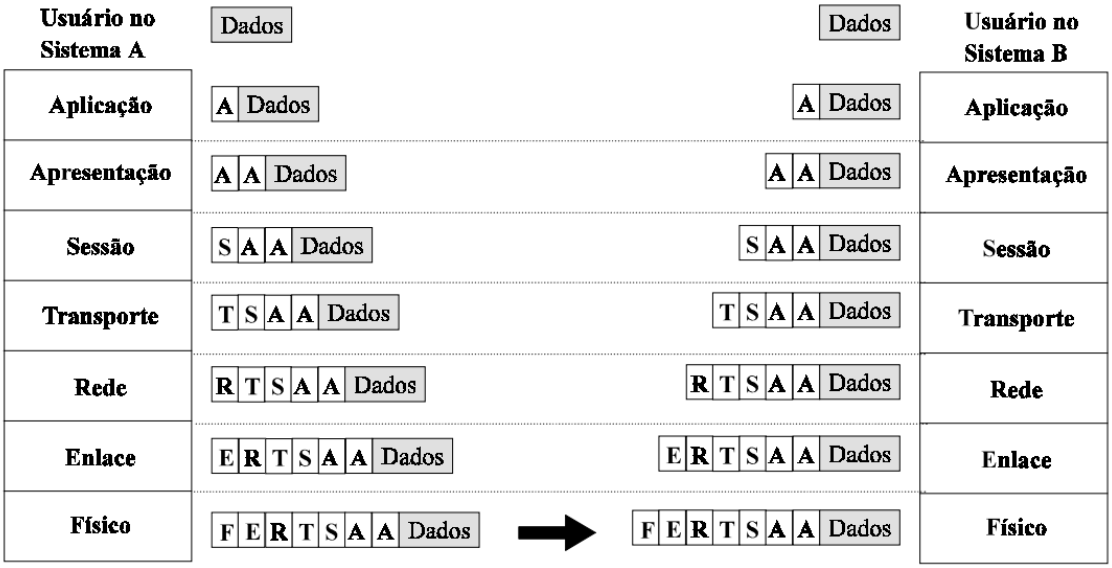


Ilustração da inclusão de bits em cada camada (*Overhead*).

Para não confundir **quadro** e **pacote**, podemos simplificar com as seguintes definições:

- **Quadro**: (ou **frame**) é a menor estrutura de informação transmitida através de uma rede local. Possui o endereço de origem e destino **físico** (da placa de rede), toda a estrutura do pacote e o *checksum* (código usado para verificar a integridade de dados transmitidos).

- **Pacote**: são transportados no interior dos quadros, possuindo: endereço lógico de destino, endereço lógico de origem (da rede) e os dados.

O modelo TCP/IP

O RM-OSI é excelente por motivos didáticos, mas não existe em uso comercial uma rede mundial totalmente OSI (com as sete camadas implementadas). Existe outro modelo para a implementação de uma solução aberta de redes de comunicação e que efetivamente está sendo usado: é a arquitetura **TCP/IP**, o modelo usado na **Internet**.

Pode-se dizer que a história do que hoje se conhece por Internet começa no dia 04/07/1957 quando a União Soviética lançou o Sputnik 1, o primeiro satélite artificial a orbitar o globo terrestre.

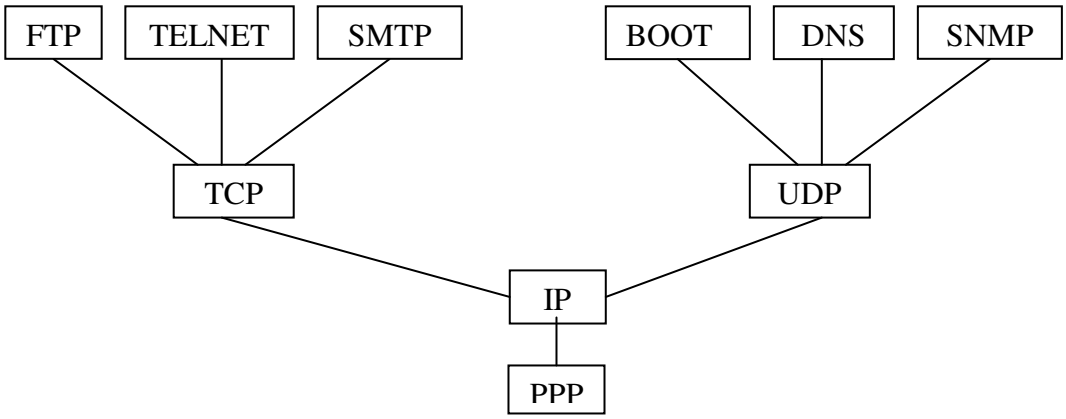
Uma das respostas americanas foi a criação da **ARPA** (*Advanced Research Projects Agency*) dentro do **DoD** (*Department of Defense*), com a finalidade de manter os Estados Unidos na liderança da ciência e da tecnologia aplicadas às atividades militares.

Em 1962, Paul Baran, da Rand Co., publicou "*On Distribuited Communications Networks*" a defesa da idéia de se criarem redes que sobrevivessem à destruição parcial dos seus nós e enlaces.

Uma rede assim não poderia ser uma rede de circuitos, mesmo que de circuitos virtuais, pois, após o estabelecimento das conexões (dos circuitos) a informação dos endereços de origem e destino é perdida (tal qual numa chamada telefônica).

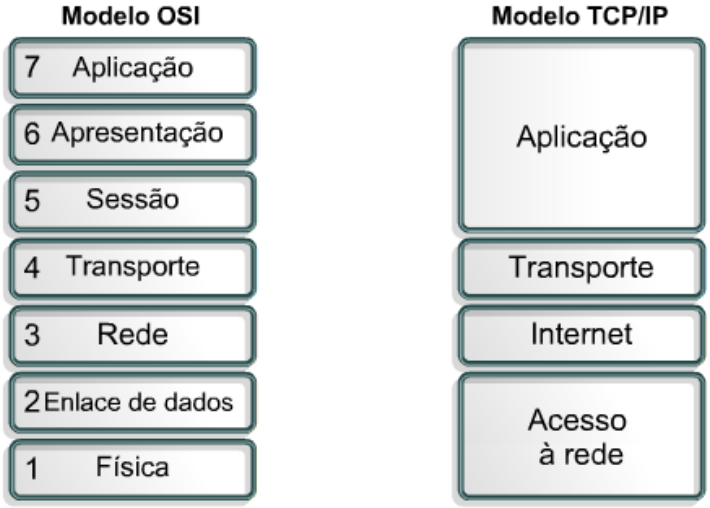
Uma rede de circuitos não têm a capacidade de re-rotear as comunicações afetadas; uma rede de datagramas sim, já que cada datagrama "per si" é roteado de forma independente dos demais.

O **TCP** (*Transfer Control Protocol*) e o **IP** (*Interconnection Network Protocol*) são dois protocolos independentes – o IP é sempre usado nesta arquitetura, o TCP nem sempre. Mas quando se cita o TCP/IP não se está falando dos dois protocolos e sim da **arquitetura** que, além destes dois, possui dezenas de outros protocolos.



As quatro camadas e alguns protocolos da arquitetura IP.

A figura seguinte ilustra a comparação entre as funções das camadas dos modelos OSI e o TCP/IP.

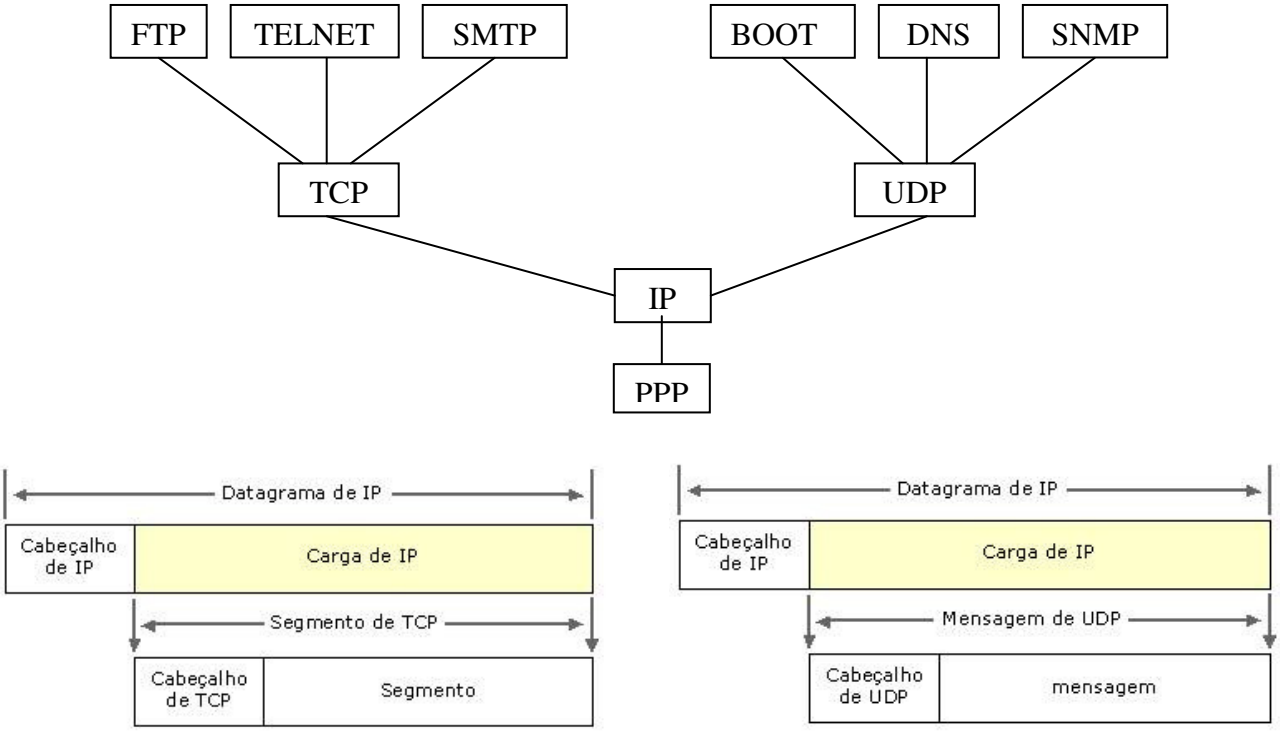


A camada "*Internet*" também é conhecida como "**Inter Rede**".

- **OBS**: O modelo TCP/IP foi definido originalmente, pela RFC 871, como tendo **três camadas**. Na RFC 1122 (1989) especificou-se um modelo de **quatro camadas**. Mais recentemente (RFC 1188, RFC 1377 e RFC 1663) foi apresentado um modelo de **cinco camadas** que divide a camada "acesso à rede" (vide figura acima) em "enlace de dados" e "física" (como no modelo OSI).

Portas de comunicação

Como vimos, o TCP/IP usa o IP para endereçar as mensagens (camada de rede). Na camada de transporte, estas mensagens podem trafegar na forma orientada a conexão (TCP – *Transfer Control* Protocol) ou não orientada a conexão (UDP – *User Datagram Protocol*).



O **TCP** é o protocolo mais usado, fornece garantia na entrega de todos os pacotes e opera na forma **orientada a conexão**. No estabelecimento da conexão entre emissor e receptor existe uma negociação denominada de *Three Way Handshake* (SYN, SYN-ACK, ACK). Após o aceite (ACK) é feita a transmissão dos pacotes. Ao final da transmissão a conexão é desfeita.

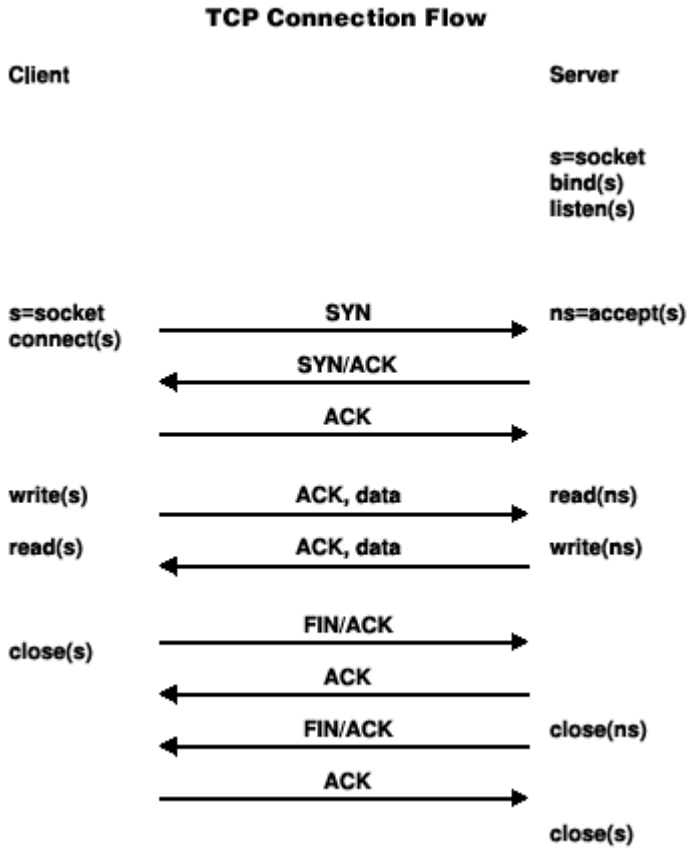
O protocolo TCP/IP permite o uso de pacotes com até 64 kbytes, mas normalmente são usados pacotes com até 1500 bytes, que é o tamanho máximo de um frame Ethernet.

Para cada pacote recebido, a estação envia um pacote de confirmação e, caso algum pacote se perca, ela solicita a retransmissão. Cada pacote inclui 4 bytes adicionais com um código de **CRC** (*Cyclic redundancy check*), que permite verificar a integridade do pacote. É através dele que o cliente sabe quais pacotes chegaram danificados.

Depois que todos os dados são transmitidos, o servidor envia um pacote "FIN" que avisa que não tem mais nada a transmitir. O cliente responde com outro pacote "FIN" e a conexão é oficialmente encerrada.

Este procedimento garante a integridade da comunicação. Porém toda esta formalidade torna as transferências mais lentas, já que via TCP, para cada conexão é necessário adicionar um total de 9 pacotes.

A figura a seguir ilustra o fluxo de informações na troca de dados usando TCP.



O **UDP** é um protocolo mais simples e por si só não fornece garantia na entrega dos pacotes. Esse processo de garantia de dados deve ser realizado pela aplicação em si (que usa o protocolo UDP) e não pelo protocolo. Por ser mais simples, é mais rápido que o TCP.

Assim como no TCP, são usados pacotes de até 1500 bytes (o protocolo permite o uso de pacotes com até 64 kbytes, mas, assim como no caso do TCP eles são raramente usados devido ao limite de tamanho dos frames Ethernet), contendo os bits adicionais de verificação. A estação pode verificar a integridade dos pacotes, mas não tem como perceber se algum pacote se perdeu, ou solicitar a retransmissão de um pacote corrompido. Se um pacote se perde, fica por isso mesmo.

Um exemplo típico de uso do UDP é o *streaming* de vídeo e áudio via web, uma situação onde se privilegia a velocidade e não a confiabilidade.

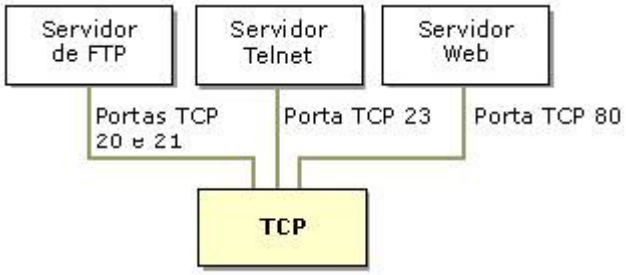
Outra aplicação comum são os servidores DNS (*Domais Name Server*). Sempre que se acessa um site, a solicitação do endereço IP referente ao *domínio* do site e a resposta do servidor são enviadas via UDP, para ganhar tempo.

Na prática, é raro encontrar algum programa que utilize unicamente pacotes UDP para outros serviços além do envio de mensagens curtas. Mesmo no caso do streaming de vídeo, é comum usar uma porta TCP para estabelecer a conexão e enviar informações de controle, deixando o UDP apenas para o envio dos dados.

Em uma comparação simplista podemos resumir na seguinte tabela:

TCP	UDP
Serviço orientado por conexão: Uma sessão é estabelecida entre os hosts.	Serviço sem conexão: Não há sessão entre os hosts.
Garante a entrega através do uso de confirmações e entrega seqüenciada dos dados.	Não garante ou confirma a entrega ou seqüência os dados.
Os programas que usam TCP têm garantia de transporte confiável de dados.	Os programas que usam UDP são responsáveis por oferecer a confiabilidade necessária ao transporte de dados.
TCP é mais lento, necessita de maior sobrecarga e pode oferecer suporte apenas à comunicação ponto a ponto.	UDP é rápido, necessita de baixa sobrecarga e pode oferecer suporte à comunicação ponto a ponto e ponto a vários pontos.

Cada programa trabalha com um protocolo/serviço específico, ao qual está associado um número denominado **Port** (porta). Assim, enquanto o IP permite endereçar redes e hosts, o número de porta permite identificar o protocolo/serviço ao qual a mensagem é endereçada.



Atuação de portas TCP

Exemplos de portas TCP

nº	Descrição
20	Servidor FTP (canal de dados)
21	Servidor FTP (canal de controle)
23	Servidor Telnet
53	Transferências de zona DNS
80	Servidor da Web (HTTP, Hypertext Transfer Protocol, protocolo de transferência de hipertexto)
139	Serviço de sessão de NetBIOS

Exemplos de portas UDP

nº	Descrição
53	Consultas de nomes DNS
69	Trivial File Transfer Protocol (TFTP)
137	Serviço de nomes de NetBIOS
138	Serviço de datagrama de NetBIOS
161	Simple Network Management Protocol (SNMP)
520	Routing Information Protocol (RIP, protocolo de informações de roteamento)

Para obter uma lista atualizada e completa de todas as portas conhecidas e registradas atualmente, consulte o seguinte endereço web:

http://www.iana.org/assignments/port-numbers

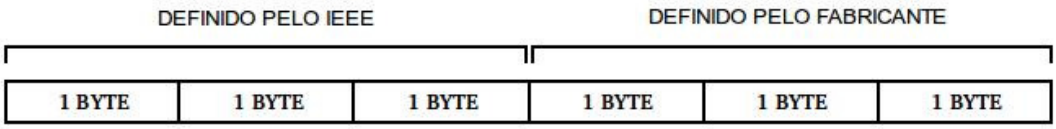
O Endereço Físico – MAC Address

O **MAC** (*Media Access Control*) é um endereço físico associado à interface de comunicação (**NIC** – *Netwok Interface Card*), que conecta um dispositivo à rede. O MAC é um endereço "único", não havendo duas portas com a mesma numeração, e usado para controle de acesso em redes de computadores. Sua identificação é gravada em hardware, isto é, na memória ROM da placa de rede de equipamentos como desktops, notebooks, roteadores, smartphones, tablets, impressoras de rede, etc. Assim, em tese, uma interface de rede tem um código que a identifica como sendo única.

Um host pode ter várias interfaces de rede, tendo um MAC para cada interface (NIC).

O endereço **MAC** é formado por um conjunto de seis bytes separados por dois pontos (":") ou hífen ("-"), sendo cada byte representado por dois algarismos na forma hexadecimal, como por exemplo: "00:19:B9:FB:E2:58". Cada algarismo em hexadecimal corresponde a uma sequência de quatro bits, desta forma, os 12 algarismos que formam o endereço totalizam 48 bits.

Há uma padronização dos endereços MAC administrada pela **IEEE** (*Institute of Electrical and Electronics Engineers*) que define que os três primeiros bytes, denominados **OUI** (*Organizationally Unique Identifier*), são destinados a identificação do fabricante - eles são fornecidos pela própria IEEE. Os três últimos bytes são definidos pelo fabricante, sendo este responsável pelo controle da numeração de cada placa que produz.



Apesar de ser único e gravado em hardware, o endereço MAC pode ser alterado através de técnicas específicas.

O endereço físico (**MAC**) de interface de rede (**NIC**) em um computador com Windows pode ser verificado pelo comando ***ipconfig /all*** **e**xecutado em janela de prompt de comandos. Em sistemas baseados em Unix e Linux, pode-se utilizar o comando ***ifconfig*** em janela de terminal. Estes comandos mostram, além do endereço físico, o endereço lógico das interfaces de redes.

O **endereço lógico** é um endereço que é atribuído pelo gestor da rede (de forma manual ou automática) que permite a comunicação entre redes (nível 3 – Rede – do modelo OSI). Em uma rede TCP/IP, o endereço lógico é o **Endereço IP**.

O MAC é responsável pelo controle de acesso ao meio propriamente dito, além da construção do quadro, endereçamento e detecção de erro.

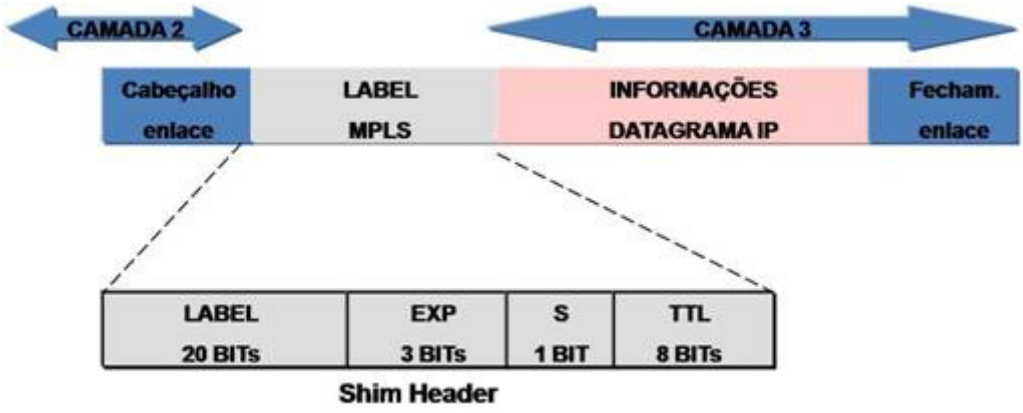
.

O Endereço lógico – IP Address

O **endereço IP** é uma forma de endereçamento lógico que permite endereçar hosts e redes. As primeiras versões foram usadas para desenvolvimento em ambientes de teste. A versão estável e que tornou a Internet possível foi a versão 4 (**IPv4**).

O **IPv5** (*Internet Protocol*, versão 5) foi uma pequena modificação experimental no IPv4 para trafegar voz e vídeo sobre *multicast*. Foi uma versão experimental do protocolo ST (*Stream Protocol*), que foi primeiramente definido em 1979 em IEN 119 (*Internet Experiment Note*), e revisto na RFC 1190 e na RFC 1819. Nunca foi introduzido ao público geral, mas atualmente muitos de seus conceitos estão presentes no protocolo MPLS.

No contexto das redes de computadores e telecomunicações, o **MPLS** (*Multi Protocol Label Switching*) é um mecanismo de transporte de dados pertencente à família das redes de comutação de pacotes. O MPLS é padronizado pelo IETF (*Internet Engineering Task Force*) através da RFC-3031 e opera numa camada OSI intermediária às definições tradicionais do Layer 2 (Enlace) e Layer 3 (Rede), pelo que se tornou recorrente ser referido como um protocolo de "Layer 2,5".



O **IPv6** é a versão mais atual do Protocolo de Internet. Originalmente oficializada em 6 de junho de 2012, é fruto do esforço do IETF para criar a "nova geração do IP" (IPng: Internet Protocol next generation), cujas linhas mestras foram descritas por *Scott Bradner* e *Allison Marken*, em 1994, na RFC 1752. Sua principal especificação encontra-se na RFC 2460.

O protocolo está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "**pilha dupla**" (***dual stack***), por algum tempo. Em longo prazo, o IPv6 tem como objetivo substituir o IPv4, que suporta cerca de 4 bilhões ($4x10^9$) de endereços IP, contra cerca de $3,4x10^{38}$ endereços do novo protocolo (enquanto o IPv4 conta com 32 bits de endereçamento, o IPv6 conta com 128 bits de endereçamento).

IPv4

O endereço **IPv4** (*Internet Protocol versão 4*) é formado por uma sequência de 32 bits que identificam redes e hosts. Para facilitar a interpretação e manuseio, os 32 bits são representados em quatro grupos (octetos), convertidos para decimal e separados por pontos.

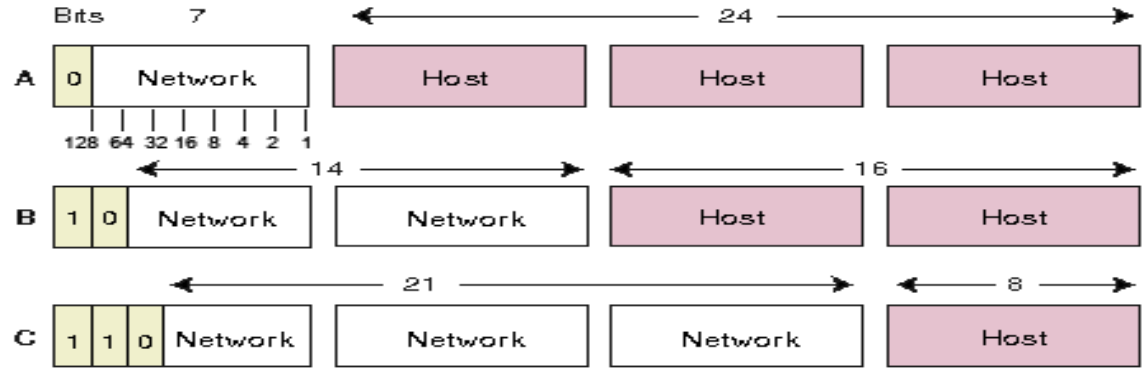
Exemplo:

sequencia de 32 bits	11000000101010000000000000000001
octetos	11000000 10101000 00000000 00000001
representação em decimal	192 . 168 . 0 . 1

Originalmente, o espaço do endereço IP foi dividido em poucas estruturas de tamanho fixo chamados de "classes de endereço". As três principais são a classe A, classe B e classe C. Examinando os primeiros bits de um endereço, o software do IP consegue determinar rapidamente qual a classe, e logo, a estrutura do endereço.

- Classe A: Primeiro bit é 0 (zero)
- Classe B: Primeiros dois bits são 10 (um, zero)
- Classe C: Primeiros três bits são 110 (um, um, zero)
- Classe D: (endereço multicast): Primeiros quatro bits são: 1110 (um, um, um, zero)
- Classe E: (especial reservado): Primeiros quatro bits são 1111 (um, um, um, um)

A figura seguinte mostra o arranjo para as classes A, B e C.



A tabela, a seguir, contém o intervalo das classes de endereços IPs:

Classe	Gama de Endereços	Redes	Hosts por Rede
A*	1.0.0.0 até 126.0.0.0	126	16 777 214**
B	128.0.0.0 até 191.255.0.0	16 384	65 534**
C	192.0.0.0 até 223.255.255.0	2 097 152	254**
D	224.0.0.0 até 239.255.255.255		Multicast
E	240.0.0.0 até 255.255.255.254		Reservada para testes pela IETF

Observações:
* Os endereços de rede 0 e 127 são reservados a loopback e não acessam a rede física.
** Em cada classe, dois endereços de hosts que são reservados:
Quando todos os bits que endereçam o host estão zerados, o endereço se refere à própria rede.
Quando todos os bits que endereçam o host estão em 1, trata-se de broadcast (todos os hosts da rede).

Há blocos de endereços **IP** que são **reservados** para uso em redes privativas e não são roteados pela Internet.

Classe A = 10.0.0.0
Classe B = 169.254.0.0 (*Zeroconf*)
Classe B = 172.16.0.0 a 172.31.0.0
Classe C = 192.168.0.0

Zeroconf (ou ***Zero Configuration Networking***) é um conjunto de técnicas que criam de forma automática uma rede IP sem necessitar de configuração ou servidores. Isto permite usuários inexperientes conectarem computadores, impressoras de rede e outros dispositivos e aguardar que o

funcionamento da rede se estabeleça automaticamente. Sem o Zeroconf, um usuário precisaria configurar serviços especiais, tais como DHCP e DNS, ou configurar manualmente cada computador para acessar a rede.

Historicamente a primeira tentativa de implementação deste tipo de serviço foi realizada pela ***Apple*** com o *AppleTalk*, ainda nos anos 80. Com esta facilidade, que já existia nos *Macs*, o usuário podia simplesmente ligar dois computadores numa rede que eles já estariam aptos a se comunicar.

A **RFC 3330** define um bloco de endereço, 169.254.0.0/16, para o uso especial no endereçamento de conexão local para redes IPv4. No IPv6, cada interface, seja através de atribuições de endereços estáticos ou dinâmicos, também recebe um endereço de link local automaticamente no bloco fe80 :: / 10.

Esses endereços são válidos apenas no link, como um segmento de rede local ou ponto a ponto, que um host está conectado. Esses endereços não são roteáveis e como endereços privados não pode ser a origem ou o destino dos pacotes que atravessam a Internet.

Quando o bloco de endereços IPv4 foi reservado, não existiam normas para os mecanismos de auto configuração de endereços. Preenchendo o vazio, a ***Microsoft*** criou uma implementação que é chamada de IP privado automático (*APIPA - Automatic Programmed IP Address*).

Quando um computador com o windows não encontra o DHCP, usará um endereço classe B com configuração 169.254.x.x, onde "x.x" (parte do IP referente ao host) será definido em função do hardware, ou seja, utilizando o endereço físico (MAC).

Com essa operação, mesmo que não haja DHCP na rede, as máquinas passarão a compor a rede 169.254.0.0 e terão conectividade entre si, embora não acessem outras redes.

Devido ao poder de mercado da Microsoft, o APIPA foi implantado em milhões de máquinas e assim tornou-se um **padrão de fato** na indústria. Muitos depois a IETF definiu um padrão formal para essa funcionalidade, a RFC 3927, intitulada de configuração dinâmica de endereços IPv4.

O endereçamento **IPv6** contém 128 bits e não possui classes específicas.

O equipamento que permite interligar redes é o *router*. Quando interliga uma rede interna (de IP interno/privado) à rede externa (de IP público, como a Internet), é um ***router gateway***. Quando representa a saída padrão da rede interna para o exterior, é um ***default gateway***.

Os números de IP interno da rede (como 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16) nunca poderiam ser passados para a Internet pois não são roteados nela. Sendo assim, os pedidos teriam de ser gerados com um IP global do router. Mas quando a resposta chegasse ao router, seria preciso saber a qual dos computadores presentes na LAN pertenceria aquela resposta.

A solução encontrada foi fazer um mapeamento baseado no IP interno e na *porta* local do computador. Com esses dois dados, é gerado um número de 16 bits usando a tabela *hash* (tabela de dispersão), este número é então escrito no campo da *porta* de origem e o pacote é enviado.

Quando o router recebe a resposta faz a operação inversa, procurando na sua tabela uma entrada que corresponda aos bits do campo da porta. Ao encontrar a entrada, é feito o direcionamento para o computador correto dentro da rede privada.

Este processo é denominado **NAT** (*Network Address Translation*).

Esta foi uma medida de reação face à previsão da exaustão do espaço de endereçamento IPv4, e rapidamente adaptada para redes privadas também por questões econômicas (no início da Internet os endereços IP alugavam-se, quer individualmente quer por classes/grupos).

Por reconhecer apenas os protocolos de transporte *TCP* e *UDP*, não é possível estabelecer uma conexão que não utilize um desses protocolos.

O número gerado pela tabela de *hash* tem apenas 16 bits, o que faz com que esta técnica permita pouco mais de 65000 conexões ativas. Dependendo das dimensões da rede e do número de pedidos feitos pelos computadores desta rede, o limite pode ser facilmente atingido.

As entradas no NAT são geradas apenas por pedidos dos computadores de dentro da rede privada. Sendo assim, um pacote que chega ao router vindo de fora e que não tenha sido gerado em resposta a um pedido da rede, ele não encontrará nenhuma entrada no NAT e este pacote será automaticamente descartado, não sendo entregue a nenhum computador da rede. Isso impossibilita a entrada de conexões indesejadas e o NAT acaba funcionando como um *firewall*.

Loopback
Um *loopback* é um canal de comunicação com apenas um ponto final. Qualquer mensagem transmitida por meio de tal canal é imediatamente recebida pelo mesmo canal.

O *Internet Protocol* define uma rede *loopback*. No IPv4, deve ser a rede 0 ("*a própria rede*") e um endereço de loopback para o computador atual - 0.0.0.0 - ("*este computador nesta rede*").

Por razões de mau uso deste endereço (em particular o uso do endereço 0 para *broadcast*) levou ao uso do endereço 127.0.0.1 como "*endereço de loopback*".

Atualmente a maioria das implementações do IPv4 usa o IP 127.0.0.1 como o endereço de loopback padrão; alguns chegam a não aceitar o valor correto 0.0.0.0.

A maior parte das implementações do IP aceita uma interface de loopback. Qualquer tráfego que um computador envie em uma rede loopback é endereçada ao mesmo computador. O endereço IP mais usado para tal finalidade é 127.0.0.1 no IPv4 e **::**1 no IPv6. O **nome de domínio** padrão para tal endereço é *localhost*.

O **nome de domínio** foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Sem ele, teríamos que memorizar uma sequência grande de números.

Em sistemas *Unix* e *Linux*, a interface *loopback* é geralmente chamada de **lo** ou **lo0**.

Máscaras de Subrede

Uma máscara de subrede, também conhecida como ***subnet mask*** ou ***netmask***, é um número de 32 bits usado com um IP para separar a parte correspondente à rede pública, à subrede e aos hosts.

Uma **subrede** é uma divisão de uma rede de computadores - é a faixa de endereços lógicos reservada para uma organização. A divisão de uma rede grande em menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede. No IPv4 uma subrede é identificada por seu endereço base e sua máscara de subrede.

Os 32 bits das **Máscaras de Subrede** são divididos em duas partes: um primeiro bloco de 1s (uns) seguido por um bloco de 0s (zeros). Os 1s (uns) indicam a parte do endereço IP que pertence à rede e os 0s (zeros) indicam a parte que pertence ao host. A **máscara de rede padrão** acompanha a classe do endereço IP:

Classe A	=	11111111 00000000 00000000 00000000
Classe B	=	11111111 11111111 00000000 00000000
Classe C	=	11111111 11111111 11111111 00000000

Assim como o endereço IP, a máscara de subrede, por razões de facilidade de manuseio, é dividida em quatro octetos convertidos para decimal e separados por pontos.

Classe A	=	255. 0 . 0 . 0
Classe B	=	255.255. 0 . 0
Classe C	=	255.255.255. 0

Embora normalmente as máscaras de subrede sejam representadas em notação decimal, é mais fácil entender seu funcionamento usando a notação binária. Para determinar qual parte de um endereço é o da rede e qual é o do host, um dispositivo deve realizar uma operação "AND".

Exemplo:

	Endereço decimal	Binário
Endereço completo	192.168.5.10	11000000 10101000 00000101 00001010
Máscara da subrede	255.255.255.0	11111111 11111111 11111111 00000000
Porção da rede	192.168.5.0	11000000 10101000 00000101 00000000

Uma rede ***classful*** é uma rede que possui uma máscara de rede 255.0.0.0 (classe A), 255.255.0.0 (classe B) ou 255.255.255.0 (classe C).

O **CIDR** (*Classless Inter-Domain Routing*) foi introduzido em 1993 como um refinamento para a forma de condução de tráfego pelas redes IP. Permite flexibilidade acrescida possibilitando a divisão de endereços IP em redes separadas. Com isso promove um uso mais eficiente para os endereços IPv4. O CIDR está definido no RFC 1519.

A notação *standard* para o intervalo de endereços CIDR começa com o endereço de rede. Isto é seguido por um caracter e de um prefixo que define o tamanho da rede em questão (o prefixo é, na verdade, o comprimento em bits 1 da máscara de sub-rede).

Exemplo:

IP = 192.168.0.0
Netmask = 255.255.255.0 → 11111111.11111111.11111111.00000000

Contamos, neste caso, 24 bits 1 da esquerda para direita, temos então: 192.168.0.0 /24
Na notação padrão, teremos então:

Classe A	→	ip/8
Classe B	→	ip/16
Classe C	→	ip/24

O **CIDR** usa máscaras de comprimento variável, o **VLSM** (Variable *Length Subnet Masks*) para alocar endereços IP em sub-redes de acordo com as necessidades individuais e particulares da rede. Assim a divisão de rede/host pode ocorrer em qualquer fronteira de bits no endereço.
Como as distinções de classes normais são ignoradas, o novo sistema foi chamado de ***routing* sem classes**. Isto levou a o sistema original passar a ser chamado de ***routing* de classes**.

Com o CIDR, se são necessários apenas 1000 endereços, por exemplo, poderia ser usada uma máscara /22 (que permite o uso de 1022 endereços), em vez de uma faixa de classe B inteira, como seria necessário anteriormente.

Outra mudança é que as faixas de endereços não precisam mais iniciar com determinados números. Uma faixa com máscara /24 (equivalente a uma faixa de endereços de classe C) pode começar com qualquer dígito e não apenas com de 192 a 223.

Um exemplo do VLSM seria um endereço como 72.232.35.108/29

Na notação decimal separado por pontos, a máscara será: 255.255.255.248

Nesse caso, teríamos 29 bits do endereço dedicados a endereçar a rede e apenas os 3 últimos bits destinados ao host. Convertendo o endereço para binário temos o endereço:

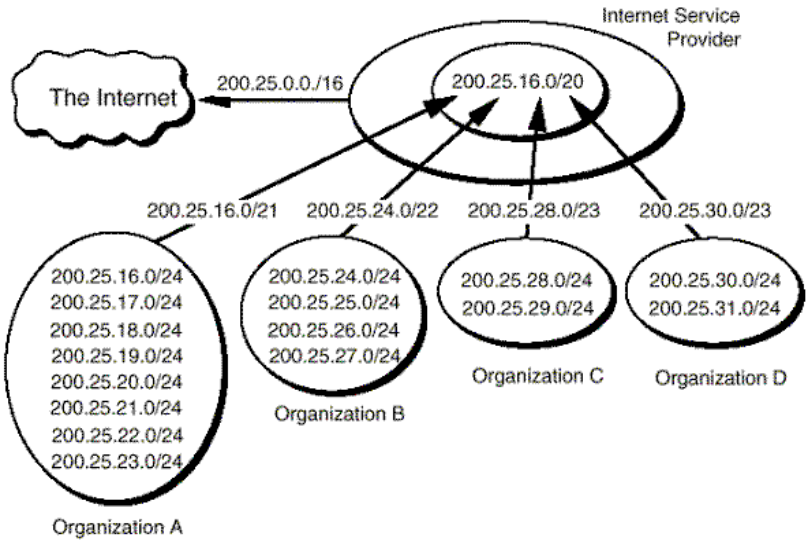
(binário) 01001000 11101000 00100011 01101100

Onde:
01001000 11101000 00100011 01101 é o endereço da **rede** (29 bits da esquerda para a direita);
100 (últimos 3 bits) é o endereço do **host** dentro dela. Neste caso, o equipamento utiliza o 4º endereço de host dentro desta rede.

Fazendo a operação lógica AND entre o endereço IP e a máscara, encontramos o endereço de rede: **72.232.35.104**. O broadcast desta rede será: **71.232.35.111**

O CIDR permite também que várias faixas de endereços contínuas sejam agrupadas em faixas maiores, de forma a simplificar a configuração. Por exemplo, é possível agrupar 8 faixas de endereços com máscara 255.255.255.0 (classe C) contínuas em uma única faixa com máscara /21 que oferece um total de 2045 endereços utilizáveis (descontando o endereço da rede, endereço de broadcast e o endereço do gateway).

Este agrupamento permite uma redução significativa do número de routes, prevenindo a "explosão da tabela de routing". Assim, é possível que uma única entrada na tabela de roteamento especifique a rota de vários endereços de rede individuais.



Exemplo de aplicação do VLSM na simplificação de tabelas de roteamento

Para simplificar o trabalho do administrador de redes, na Internet, há disponível várias ferramentas que atuam como calculadoras de endereçamento IP, com conversão para a notação binária, decimal, hexadecimal e octal.

A Atribuição de Endereços IP

Inicialmente, a necessidade de automatizar a requisição e distribuição do endereço IP deu-se em função da existência de estações sem disco (*diskless*). Esta demanda provocou o uso do protocolo de camada de enlace RARP.

Com o aumento do número de máquinas nas redes e também a crescente necessidade de maiores informações de configuração para comunicação em uma rede, o RARP mostrou-se ineficiente, o que levou a criação do protocolo BOOTP.

O advento da computação móvel trouxe uma grande limitação ao BOOTP. Foi criado, então, o DHCP (*Dynamic Host Configuration Protocol*), uma versão estendida do BOOTP, que permite a atribuição dinâmica de endereços IP e simplifica a administração da rede TCP/IP.

O DHCP é especificado pela IETF por meio dos RFCs 1533, 1534, 1541 e 1542.

- **RARP**

Em condições normais (uma estação completa), o endereço IP fica armazenado na memória da máquina, carregado após o *boot* (inicialização). Quando a máquina não possui um disco para inicialização do sistema (estação *diskless*) para carregar o seu endereço IP, a imagem de memória daquela estação fica armazenada no servidor.

A estação *diskless* utiliza um protocolo que permite a obtenção do endereço IP fazendo uso do endereço físico (MAC) de sua NIC (Network Interface Card). Este protocolo é o **RARP** (*Reverse Address Resolution Protocol*).

O RARP é uma adaptação do protocolo ARP [RFC826].

Algumas desvantagens de uso deste protocolo são:

- Como o RARP opera num nível mais baixo, ele utiliza um acesso direto ao hardware de rede, com isso torna-se muito complicado para um programador de aplicativos construir um servidor;
- Pelo fato do RARP utilizar um endereço de hardware para identificar o equipamento, ele não pode ser aplicado em redes que atribuem esses endereços dinamicamente.

- **O BOOTP**

As deficiências encontradas no RARP foram solucionadas com a criação do BOOTP (*BOOTstrap Protocol*).

Por utilizar o UDP (*User Datagram Protocol*) para trafegar suas mensagens, ele pode ser usado por uma aplicação de forma mais simples que o RARP. Ele também é mais eficiente que este protocolo por embutir em sua mensagem outras informações importantes para a inicialização.

Diferente da comunicação RARP, a comunicação BOOTP se processa na camada de rede. A estação cliente lança a sua solicitação na rede utilizando um endereço IP de difusão. Os servidores BOOTP serão os únicos a reconhecer e responder também por difusão. Esta forma de resposta é utilizada pelo fato do cliente não possuir ainda, o seu endereço IP para confirmar o recebimento.

O BOOTP delega ao cliente toda a responsabilidade por uma comunicação segura pois, os protocolos utilizados são passíveis de corrupção ou perda de dados. O BOOTP solicita ao UDP que faça um *checksum* e ainda especifica que solicitações e respostas tenham seu campo ***dont fragment*** ativo para comportar clientes de memória pequena.

O BOOTP fornece alocação fixa de um único endereço IP para cada cliente, reservando permanentemente esse endereço no banco de dados do servidor BOOTP. Ou seja, os clientes BOOTP não renovam suas configurações, a não ser que o sistema seja reinicializado.

- **O DHCP**

O DHCP (*Dynamic Host Control Protocol*) surgiu como evolução do BOOTP. Ele pode atribuir endereço para um equipamento de rede de três formas: configuração manual, automática e dinâmica.

- Configuração Manual

Neste caso, é possível atrelar um endereço IP a uma determinada máquina na rede. Para isso, é necessária a associação de um endereço existente no banco do servidor DHCP ao endereço MAC do adaptador de rede da máquina. Configurado desta forma, o DHCP irá trabalhar de maneira semelhante ao BOOTP. Esse endereço "amarrado" à NIC não poderá ser utilizado por outra.

- Configuração Automática

Nesta forma, o servidor DHCP é configurado para atribuir um endereço IP a um equipamento por tempo indeterminado. Quando este se conecta pela primeira vez na rede, lhe é atribuído um endereço permanente. A diferença existente entre esta e a primeira configuração é que nesta não é necessária uma especificação do equipamento que utilizará determinado endereço. Ele é atribuído de forma automática.

- Configuração Dinâmica

Neste tipo de configuração, é que reside a característica principal do DHCP, que o diferencia do BOOTP. Desta forma o endereço IP é locado temporariamente a um equipamento e periodicamente,

é necessária a atualização dessa locação. Com essa configuração, é possível ser utilizado por diferentes equipamentos, em momentos diferentes, o mesmo endereço IP. Basta, para isso, que o primeiro a locar o endereço, deixe de utilizá-lo. Quando o outro equipamento solicitar ao servidor DHCP um endereço IP poderá ser fornecido ao mesmo o endereço deixado pelo primeiro.

- O SERVIDOR DHCP

O **servidor DHCP** deve ser configurado pelo administrador da rede para disponibilizar aos seus clientes, endereços IP em uma das três formas de fornecimento descritas (manual, automática ou dinâmica). Para tanto, ele alimenta um banco com os endereços da sua sub-rede que serão fornecidos de forma automática. É importante deixar claro que, em uma rede, o administrador deverá deixar fixo em algumas máquinas os seus endereços IP.

Nas configurações, será estabelecido o prazo de locação de um endereço. Esse prazo pode variar de horas a dias ou simplesmente ser ilimitado. Essa decisão irá depender da rede em que o DHCP está servindo e das necessidades de um determinado equipamento.

- O CLIENTE DHCP

Um **cliente DHCP** é um equipamento que está configurado para solicitar a um servidor DHCP um endereço IP. Como já foi dito anteriormente, alguns equipamentos na rede devem possuir endereços IP fixos, já configurados na própria máquina, em função dos serviços que eles disponibilizam na rede. Essas máquinas não são consideradas como clientes DHCP.

Nome de Domínio

Domínio é um nome que serve para localizar e identificar conjuntos de computadores na rede. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Sem ele, teríamos que memorizar números IPs.

O **DNS** (*Domain Name System* - Sistema de Nomes de Domínios) é um sistema de gerenciamento de nomes hierárquico e distribuído visando resolver nomes de domínios em endereços IP.

O sistema de distribuição de nomes de domínio foi introduzido em 1984. Ele baseia-se em nomes hierárquicos e permite a inscrição de vários dados digitados além do nome do host e seu IP. Em virtude do banco de dados de DNS ser distribuído, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Este tipo de servidor usa como porta padrão a 53.

O servidor DNS traduz nomes para os endereços IP e endereços IP para nomes respectivos. Dessa forma permite a localização de hosts em um domínio determinado.

Um servidor DNS secundário é uma espécie de cópia de segurança do servidor DNS primário.

Existem 13 servidores DNS raiz no mundo todo e sem eles a Internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa.

Para Aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003.

Localização dos Servidores DNS raiz.

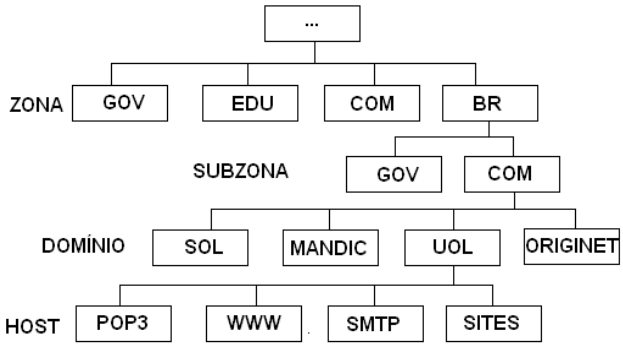
Normalmente o DNS atua resolvendo o nome do domínio de um host qualquer para seu endereço IP correspondente. O **DNS Reverso** resolve o endereço IP, buscando o nome de domínio associado ao host. Ou seja, quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio (nome dado à máquina ou outro equipamento que acesse uma rede), tentamos resolver o endereço IP através do DNS reverso que procura qual nome de domínio está associado aquele endereço.

Os servidores que utilizam o DNS Reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS. Isto evita que alguém utilize um domínio que não lhe pertence para enviar *spam*, por exemplo.

O espaço de nomes de domínio e endereços IP são recursos críticos para a internet, no sentido que requerem coordenação global. Cada endereço IP deve identificar um único equipamento, de forma que não é possível atribuir endereços IP de maneira descentralizada. Da mesma forma, um nome de domínio deve identificar o conjunto de computadores que o mantém. A organização responsável por atribuir nomes de domínio e endereços IP em nível global é a ICANN (http://www.icann.org/).

O **TLD** (*top-level domain* – domínio de topo) é um dos componentes dos endereços de Internet. Cada nome de domínio na Internet consiste de alguns nomes separados por pontos, e o último desses nomes é o domínio de topo, ou TLD. Por exemplo, no nome de domínio exemplo.com, o TLD é **com**.

O **gTLD** (*generic top-level domain*) é uma das categorias dos domínios de topo (TLD) para uso no DNS (Sistema de Nomes de Domínios da Internet).



Exemplo de hierarquia de Nomes de Domínios

A **ICANN** atualmente distingue os seguintes grupos de domínios de topo:

- domínio de topo de código de país (country-code top-level domains ou ccTLD)
- domínios de topo genéricos (generic top-level domains ou gTLD)
- domínios de topo patrocinados (sponsored top-level domains ou sTLD)
- domínios de topo não patrocinados (unsponsored top-level domains)
- domínios de topo de infraestruturas (infrastructure top-level domain)
- domínios de topo internacionalizados (internationalized top-level domains ou IDNs)
- domínios de topo de código de país internacionalizado (internationalized country code top-level domains)
- domínios de topo em teste(testing top-level domains)

Em 20 de junho de 2011, o comité do ICANN aprovou o fim das restrições a sufixos para domínios de topo genéricos (gTLD) além dos 22 até então disponíveis (como por exemplo .com, .gov, .edu, etc). Com isso, as empresas e as organizações poderão escolher sufixos arbitrários para os seus gTLD.

Também o uso de caracteres não-latinos, como os dos alfabetos cirílico, árabe, chinês, tailandês, georgiano, hebraico ou outros, passou a ser permitido.

A Conexão em Rede por Cabos TP

O cabeamento por par trançado (**TP** – *Twisted Pair*) é feito por um tipo de cabo que possui pares de fios entrelaçados um ao redor do outro para cancelar as interferências eletromagnéticas de fontes externas e interferências mútuas (*crosstalk* – linha cruzada) entre cabos vizinhos. A taxa de tranças (normalmente definida em termos de tranças por metro) é parte da especificação de certo tipo de cabo. Quanto maior o número de tranças, maior é o cancelamento do ruído.

Essa tecnologia foi originalmente produzida para transmissão telefônica analógica que utilizou o sistema de transmissão por par de fios.

A matéria-prima fundamental utilizada para a fabricação dos cabos TP é o cobre.

Existem três tipos de cabos Par trançado:

UTP (***Unshielded Twisted Pair*** – Par Trançado sem Blindagem): é o mais usado atualmente tanto em redes domésticas quanto em grandes redes industriais devido ao fácil manuseio, instalação, permitindo taxas de transmissão de até 100 Mbps com a utilização do cabo CAT 5e; é o mais barato para distâncias de até 100 metros; Para distâncias maiores emprega-se cabos de fibra óptica. Sua estrutura é de quatro pares de fios entrelaçados e revestidos por uma capa de PVC. Pela falta de blindagem este tipo de cabo não é recomendado ser instalado próximo a equipamentos que possam gerar campos magnéticos (fios de rede elétrica, motores, inversores de frequência) e também não podem ficar em ambientes com humidade.

STP (***Shielded Twisted Pair*** – Par Trançado com Blindagem): possui uma blindagem feita com a malha metálica em cada par. É recomendado para ambientes com interferência eletromagnética acentuada. Por causa de sua blindagem especial em cada par acaba possuindo um custo mais elevado. Caso o ambiente possua umidade, grande interferência eletromagnética, distâncias acima de 100 metros ou exposto diretamente ao sol, ainda é aconselhável o uso de cabos de fibra óptica.

ScTP (***Screened Twisted Pair*** - também referenciado como **FTP**, ***Foil Twisted Pair***): para este tipo de cabo uma película de metal é enrolada sobre o conjunto de pares trançados, melhorando a resposta a interferências, embora exija maiores cuidados quanto ao aterramento.

Os cabos TP foram padronizados pelas normas da EIA/TIA-568-B (*Electric Industries Association / Telecommunication Industries Associations*) e são divididos em categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores.

A seguir temos um resumo simplificado dos cabos UTP.

Categoria do cabo 1 (CAT1)
Consiste em um cabo blindado com dois pares trançados compostos por fios 26 AWG. São utilizados por equipamentos de telecomunicação e rádio. Foi usado nas primeiras redes Token-ring mas não é aconselhável para uma rede par trançado. O CAT1 não é mais recomendado pela TIA/EIA.

Categoria do cabo 2 (CAT2)
É formado por pares de fios blindados (para voz) e pares de fios não blindados (para dados). Também foi projetado para antigas redes token ring e ARCnet chegando a velocidade próxima de 4Mbps. O CAT2 não é mais recomendado pela TIA/EIA.

Categoria do cabo 3 (CAT3)
Foi o primeiro padrão de cabos de par trançado desenvolvido especialmente para uso em redes. O padrão é certificado para até 16 MHz, o que permitiu seu uso no padrão 10BASE-T, que é o padrão de redes Ethernet de 10 megabits para cabos de par trançado. Existiu ainda um padrão de 100 megabits para cabos de categoria 3, o 100BASE-T, mas ele é pouco usado e não é suportado por todas as placas de rede.

Pode ser usado para VOIP, rede de telefonia e redes de comunicação 10BASE-T e 100BASE-T. O CAT3 é recomendado pela norma TIA/EIA-568-B.

Categoria do cabo 4 (CAT4)
É um cabo par trançado não blindado (UTP – Unshield Twisted Pair) que pode ser utilizado para transmitir dados a uma frequência de até 20 MHz e dados a 20 Mbps. Foi usado em redes que podem atuar com taxa de transmissão de até 20Mbps como token ring, 10BASET e 100BASET4. Não é mais utilizado, pois foi substituído pelos cabos CAT5 e CAT5e. O CAT4 não é mais recomendado pela TIA/EIA.

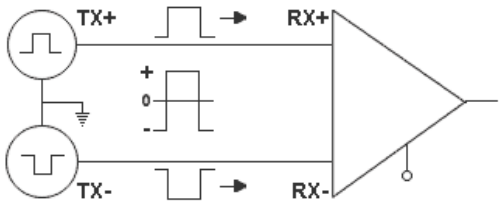
Categoria do cabo 5 (CAT5)
Usado em redes *fast ethernet* em frequências de até 100 MHz com uma taxa de 100 Mbps. O CAT5 não é mais recomendado pela TIA/EIA.

Categoria do cabo 5e (CAT5e)
É uma melhoria da categoria 5. Pode ser usado para frequências até 125 MHz em redes 1000BASE-T gigabit ethernet. Ela foi criada com a nova revisão da norma EIA/TIA-568-B. Porém, o CAT5e não é mais recomendado pela norma EIA/TIA-568-B).

Categoria do cabo 6 (CAT6)
Definido pela norma ANSI EIA/TIA-568-B-2.1 possui bitola 24 AWG e banda passante de até 250 MHz e pode ser usado em redes gigabit ethernet a velocidade de 1Gbps.

Categoria do cabo 6a (CAT 6a)
É uma melhoria dos cabos CAT6. O a de CAT6a significa *augmented* (ampliado). Os cabos dessa categoria suportam até 500 MHz e podem ter até 55 metros no caso da rede ser de 10Gbps, caso contrario podem ter até 100 metros. Para que os cabos CAT 6a sofressem menos interferências os pares de fios são separados uns dos outros, o que aumentou o seu tamanho e os tornou menos flexíveis. Essa categoria de cabos tem os seus conectores específicos que ajudam à evitar interferências.

Para potencializar o efeito da blindagem eletromagnética, as placas de rede utilizam o sistema ***balanced pair*** de transmissão, onde, dentro de cada par, os dois fios enviam o mesmo sinal, porém com a polaridade invertida. Para um bit "1", o primeiro fio envia um sinal elétrico positivo, enquanto o outro envia um sinal elétrico negativo:

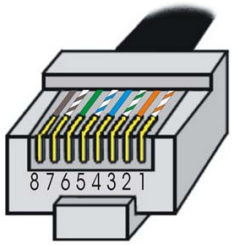


Devido a esta técnica de transmissão, os cabos de par trançado são também chamados de "***balanced twisted pair***", ou "cabo de par trançado balanceado".

O quadro a seguir compara as perdas em Cat.3, Cat.4 e Cat.5 em 100m em função da frequência.

Frequência (MHz)	Cat. 3 Atenuação (dB)	Cat. 4 Atenuação (dB)	Cat. 5 Atenuação (dB)
1,0	2,6	2,2	2,0
4,0	5,6	4,3	4,1
8,0	8,5	6,2	5,8
10,0	9,7	6,9	6,5
16,0	13,1	8,9	8,2
20,0	-	10,0	9,3
25,0	-	-	10,4
31,25	-	-	11,7
62,5	-	-	17,0
100,0	-	-	22,0
Atenuação por 100 metros (328 pés) a 20 ° C			

O conector padrão para cabos TP é o **RJ45**.



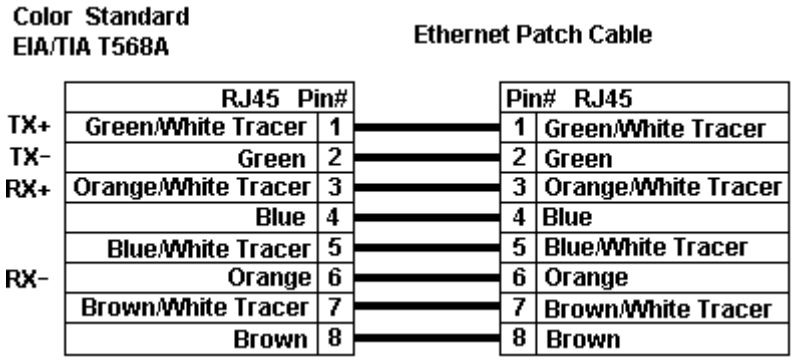
Há dois padrões de utilização dos conectores: o T568A e o T568B.

Padrão T568B:	**Padrão T568A:**
pino / cor 1. branco laranja (Recepção) 2. laranja (Recepção) 3. branco verde (Transmissão) 4. azul 5. branco azul 6. verde (Transmissão) 7. branco marrom 8. marrom	pino / cor 1. branco verde (transmissão) 2. verde (transmissão) 3. branco laranja (Recepção) 4. azul 5. branco azul 6. laranja (Recepção) 7. branco marrom 8. marrom

De acordo com a aplicação desejada, podemos construir cabos de três formas:

O **cabo reto** ou ***Straight Through***: consiste em ligar os pinos na proporção 1 para 1 entre as pontas. Isto é feito utilizando o mesmo padrão (T568A ou T568B) nas duas pontas.

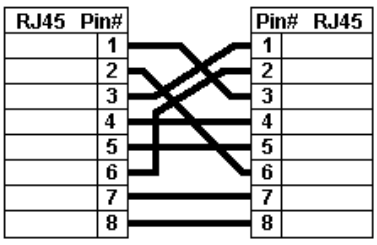
A figura seguinte ilustra a construção de um cabo straigh com o T568A.



O mesmo efeito é alcançado utilizando o padrão T568B nas duas pontas do cabo.

O cabo reto é usado na interligação de hosts através de um elemento concentrador como um hub ou switch.

O **cabo cruzado** ou ***Crossover*** (ou simplesmente **Cross**) é construído com a utilização de uma ponta do cabo no padrão T568A e a outra ponta no padrão T568B. Nesta configuração, os pinos 1 e 2 de uma das pontas são conectados a 3 e 6 da outra (ligando TX de um lado ao RX do outro e vice versa). A figura seguinte ilustra as interligações em um cabo crossover ethernet (10Mbps) e FastEthernet (100Mbps).



Cabo crossover

A conexão gigabit exige que os 8 fios sejam cruzados.

Color Standard
EIA/TIA T568A

RJ45	Pin#	Pin#	RJ45
Green/White	1	1	Orange/White
Green	2	2	Orange
Orange/White	3	3	Green/White
Blue	4	4	Brown/White
Blue/White	5	5	Brown
Orange	6	6	Green
Brown/White	7	7	Blue
Brown	8	8	Blue/White

"A" is earlier

Color Standard
EIA/TIA T568B

RJ45	Pin#	Pin#	RJ45
Orange/White	1	1	Green/White
Orange	2	2	Green
Green/White	3	3	Orange/White
Blue	4	4	Brown/White
Blue/White	5	5	Brown
Green	6	6	Orange
Brown/White	7	7	Blue
Brown	8	8	Blue/White

"B" is most recent

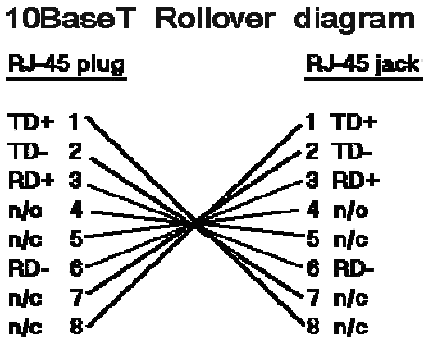
O cabo crossover é usado nas seguintes situações:

- Para ligar um computador a um router
- Conexão de um computador para um computador
- Ligar um router a um router
- Ligar um hub a um hub

Além destes, há também o cabo ***Rollover***. Este é construído com a interligação dos pinos 1~8 de uma ponta respectivamente em 8~1 da outra. A figura ao lado ilustra essas ligações.

.

Cabos *Rollover*, também chamado de cabos ***Yost***, costumam ligar porta *AUX* do roteador ao qual se tem acesso (via ssh/telnet/afins), e a outra ponta no dispositivo que se deseja acessar na porta *CONSOLE*.



Um cabo de rede Ethernet operando a 100Mbps (FastEthernet) trabalha com uma frequência de clock de 125MHz com uma taxa de transmissão de 8 bits a cada 10 símbolos.

Aprimoramentos nos protocolos possibilitam atingir 10 bits em 10 símbolos. Isto significa operar a até 125Mbps.

Nos cabos gigabit (1000baseT), todos os fios são usados e são bidirecionais. Como cada um opera a até 125Mbps, será possível atingir 8 x 125Mbps = 1000Mbps.

Cabeamento estruturado é a disposição organizada e padronizada de conectores e meios de transmissão para redes de informática e telefonia, de modo a tornar a infraestrutura de cabos autônoma quanto ao tipo de aplicação e de layout. O Sistema de Cabeamento Estruturado utiliza o conector RJ45 e o cabo UTP como mídias-padrão para a transmissão de dados, análogo ao padrão da tomada elétrica que permite a alimentação elétrica de um equipamento independentemente do tipo de aplicação.

O conceito de Sistema de Cabeamento Estruturado se baseia na disposição de uma rede de cabos com integração de serviços de dados e voz que facilmente pode ser redirecionada por caminhos diferentes, no mesmo complexo de Cabeamento, para prover um caminho de transmissão entre pontos da rede distintos.

Um Sistema de Cabeamento Estruturado EIA/TIA-568-B (ver a norma brasileira equivalente: **NBR 14.565**) é formado por sete subsistemas.

1. Entrada do Edifício
2. Sala de Equipamentos
3. Cabeamento de Backbone
4. Armário de Telecomunicações
5. Cabeamento Horizontal
6. Área de Trabalho
7. Norma 606 "Administração do Sistema"

Os padrões EIA/TIA-568-B foram publicados em 2001. Eles substituem o padrão EIA/TIA-568-A um conjunto de padrões que atualmente está obsoleto. A norma é muito conhecida pela característica do cabeamento *EIA/TIA-568-B.1-2001* que são 8 condutores de fios 100-ohm balanceados e trançados. Estes condutores são nomeados T568A e T568B, e frequentemente se refere (erroneamente) como EIA/TIA-568A e EIA/TIA-568B.

O foco do cabeamento estruturado consiste em preparar todo o prédio de forma a colocar pontos de rede em todos os pontos onde eles possam ser necessários. Todos os cabos vão para um ponto central, onde ficam os equipamentos de rede. Os pontos não precisam ficar necessariamente ativados, mas a instalação fica pronta para quando precisar ser usada.

O conceito defende que, em longo prazo, é mais barato instalar todo o cabeamento de uma vez, de preferência antes do local ser ocupado, do que ficar fazendo modificações cada vez que for preciso adicionar um novo ponto de rede.

O início de tudo é na sala de equipamentos (*equipment room*). A sala de equipamentos deve ser uma área de acesso restrito, onde os equipamentos fiquem fisicamente protegidos.

Em um prédio, a sala de equipamentos ficaria normalmente no andar térreo. É inviável puxar um cabo separado para cada um dos pontos de rede do prédio, da sala de equipamento até cada ponto de rede individual; por isso é criado um segundo nível hierárquico, representado pelos armários de telecomunicações (*telecommunications closed*).

O armário de telecomunicações é um ponto de distribuição, de onde saem os cabos que vão até os pontos individuais. Normalmente é usado um *rack*, contendo todos os equipamentos, o qual é também instalado em uma sala ou em um armário com acesso restrito.

Além dos switches, um equipamento muito usado no armário de telecomunicações é o ***patch panel*** (painel de conexão). Ele é um intermediário entre as tomadas de parede e outros pontos de conexão de cada andar e sala do prédio e os switches da rede. Os cabos vindos dos pontos individuais são numerados e instalados em portas correspondentes do *patch panel* e as portas utilizadas são então ligadas aos switches.

Uma vantagem é que com os cabos concentrados no patch panel, tarefas como desativar um ponto ou ligá-lo a outro segmento da rede (ligando-o a outro switch ou roteador) ficam muito mais simples.

Os patch panels são apenas suportes, sem componentes eletrônicos e por isso são relativamente baratos. Eles são normalmente instalados em racks, junto com os switches e outros equipamentos. Os switches são ligados às portas do patch panel usando cabos de rede curtos, chamados de "***patch cords***" (cabos de conexão). Os *patch cords* são muitas vezes feitos com cabos ***stranded*** (cabos de par trançado onde cada condutor é composto por várias fibras) de forma a serem mais flexíveis.

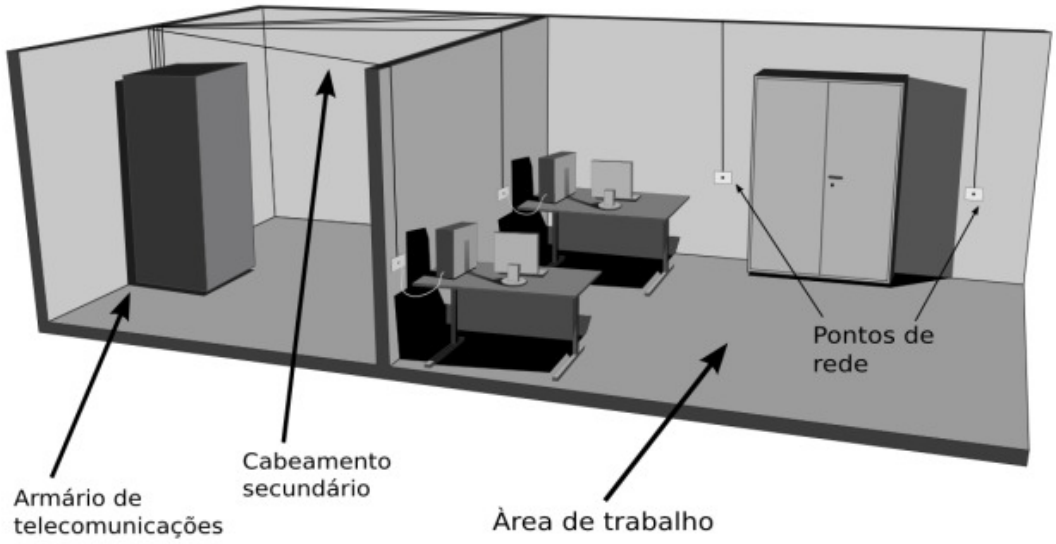
Cada andar tem um ou mais armários de telecomunicações (de acordo com as peculiaridades da construção e a distância a cobrir) e todos são ligados a um switch ou um roteador na sala de equipamentos através de cabos verticais chamados de **rede primária** (eles são também chamados de **cabeamento vertical** ou de ***backbones***). Se a distância permitir, podem ser usados cabos de par trançado, mas é muito comum usar cabos de fibra óptica para esta função.

Temos em seguida a **rede secundária** (*horizontal cabling* – cabeamento horizontal), composta pelos cabos que ligam o armário de telecomunicações às tomadas onde são conectados os PCs da rede. Estes são os cabos permanentes, que são instalados como parte do cabeamento inicial e continuam sendo usados por muito tempo.

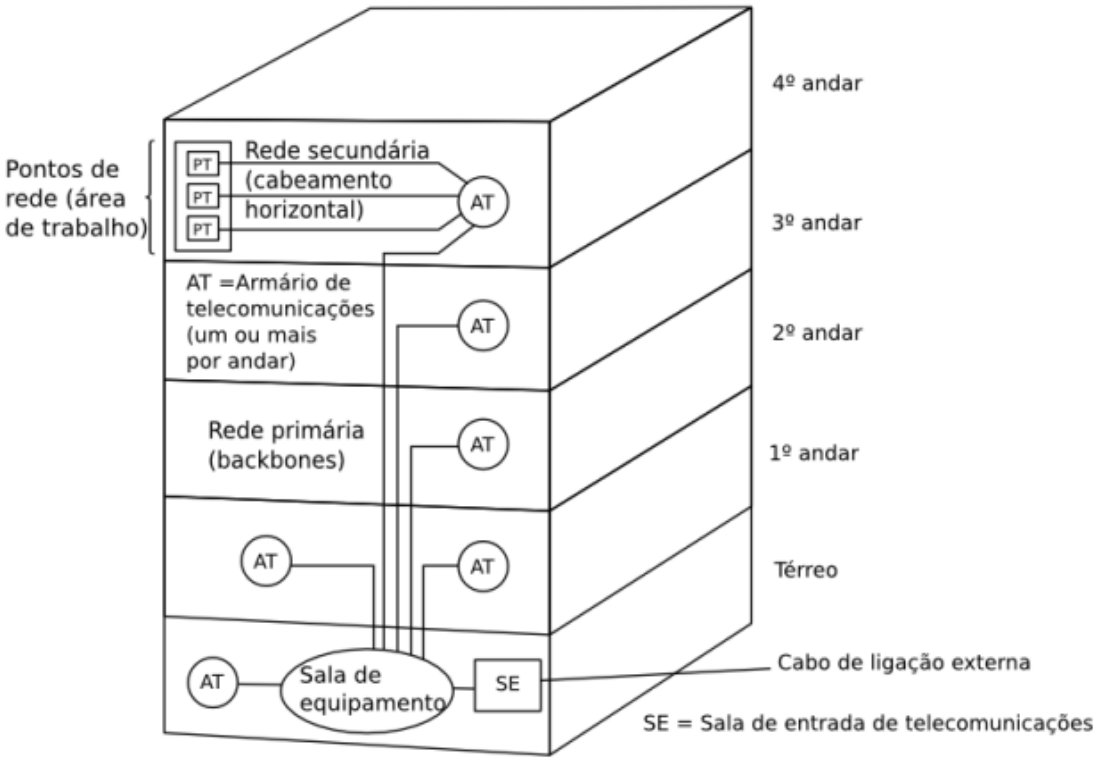
Assim, este sistema prevê o uso de três segmentos de cabo:

a) O ***patch cord*** ligando o switch ao *patch panel*.
b) O cabo da **rede secundária**, ligando o patch panel à tomada na área de trabalho.
c) O cabo entre a tomada e o PC.

Dentro do padrão, o cabo da rede secundária não deve ter mais do que 90 metros, o *patch cord* entre o patch panel e o switch não deve ter mais do que 6 metros e o cabo entre a tomada e o PC não deve ter mais do que 3 metros. Estes valores foram definidos tomando por base o limite de 100 metros para cabos de par trançado (90+6+3=99), de forma que, ao usar um cabo de rede secundária com menos de 90 metros, pode-se usar um patch cord, ou um cabo maior para o PC, desde que o comprimento total não exceda os 100 metros permitidos.



Cabeamento horizontal (rede secundária) e *work área*



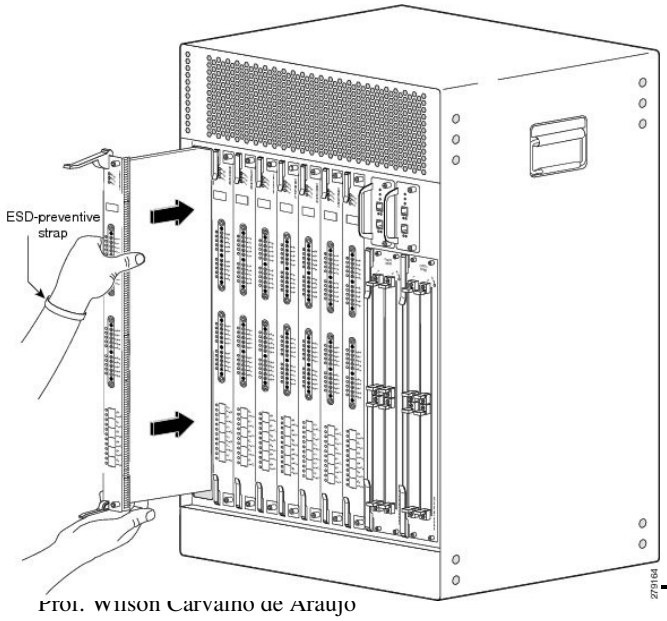
Exemplo de cabeamento

As salas e os outros ambientes contendo as tomadas, onde ficam os micros, são chamadas de área de trabalho (*work area*), já que em um escritório corresponderiam às áreas úteis, onde os funcionários trabalham. Na norma da ABNT, as tomadas são chamadas de "*pontos de telecomunicações*" e não de "pontos de rede". Isso acontece porque o cabeamento estruturado prevê também o uso de cabos de telefone e de outros tipos de cabos de telecomunicação, não se limitando aos cabos de rede.

Equipamentos de Redes de Dados

- **Modem**

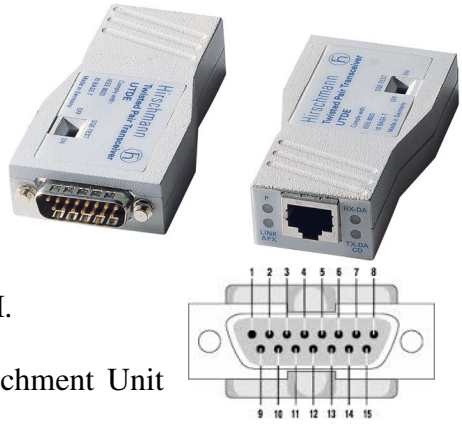
O termo modem vem da combinação de **mo**dulador**/dem**odulador. De início dedicado a converter dados para comunicação por linhas telefônicas, hoje permite altas velocidades em redes de acesso.



Cisco uBR 10012

Por exemplo: através do uso de *Channel bonding* empresas brasileiras já conseguem comercializar a velocidade de 100Mbps, utilizando *CMTS* Cisco uBR 10012 e **Cable modem** Cisco DPC300 que suporta 4 canais agregados (downstream e upstream), o que fornece uma taxa de transferência máxima praticável de 152 Mbps.

- **Transceiver**



Um Transceiver (de *Transmitter* + *Receiver*), também designado **MAU** (*Media Attachment Unit*), é um dispositivo que funciona como receptor e emissor de um sinais elétricos. Existem transceivers para amplificar sinais ou para adaptar duas interfaces elétricas diferentes. Por serem dispositivos que trabalham com nível elétrico e/ou conexões mecânicas, os transceivers trabalham na camada física (camada 1) do modelo OSI.

Podemos utilizar transceivers para adaptar a interface AUI (Attachment Unit Interface) à interface RJ-45.

conector AUI

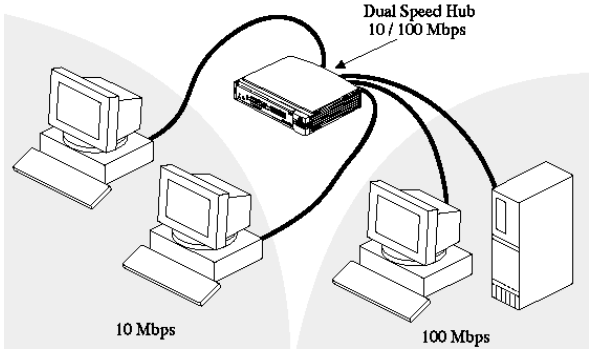
- **Hub**

Por vezes também designado concentrador, repetidor ou até comutador de nível 1, o **hub** é um dispositivo que permite interligar uma série de dispositivos Ethernet para que funcionem como um único segmento de rede (**domínio de colisão**).

Uma rede constituída por uma série de dispositivos Ethernet interligados através de um hub tem uma topologia em estrela a nível físico, mas a nível lógico tem uma topologia em barramento (segmento partilhado).

Tal como os transceivers, os hubs funcionam na camada física (camada 1) do modelo OSI.

Embora na versão mais pura um hub apenas seja capaz de interligar interfaces a funcionar à mesma velocidade, existem dual-speed hubs capazes de interligar segmentos de rede de 10Mbps com segmentos de 100Mbps. No entanto, estes dispositivos são híbridos entre hubs e bridges ou comutadores (discutidos mais adiante), pois não existe um único segmento de rede, mas dois — um a 10Mbps e outro a 100Mbps. O conjunto destes dois segmentos funciona como um único domínio de difusão, mas cada um dos segmentos é um domínio de colisão separado.

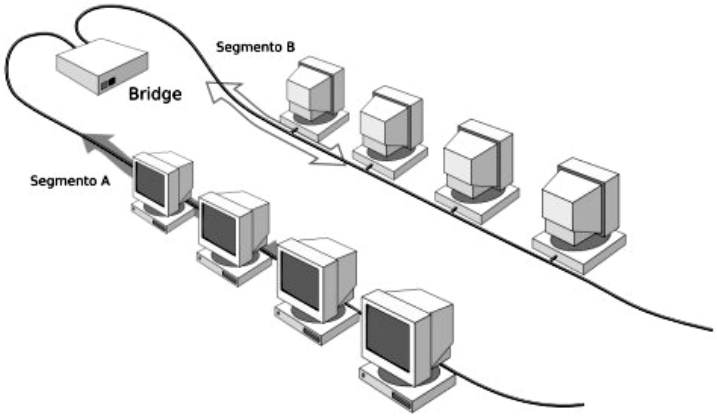


Existem duas classes de hubs Fast-Ethernet: classe I e classe II. A diferença reside no fato de os primeiros recuperarem o sinal para uma forma digital para o retransmitir, enquanto os segundos apenas amplificam e reenviam o sinal recebido de forma analógica. Uma vez que os hubs classe I introduzem um atraso superior (máx. 140 bits) aos classe II (máx. 92 bits), pode existir um único hub classe I entre qualquer par de máquinas numa rede, mas podem existir dois hubs classe II.

- **Bridge**

A **bridge** (ponte) é um dispositivo que permite interligar dois segmentos de rede, unindo dois domínios de colisão num único domínio de difusão.

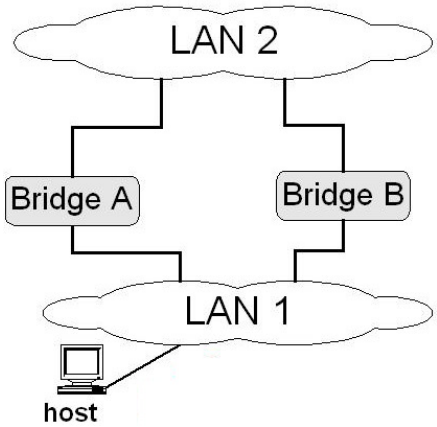
Uma bridge "aprende" quais endereços MAC se encontram de um lado e do outro. Um frame recebido de um segmento é retransmitido ao outro se destinar-se a um endereço MAC que a bridge sabe estar do outro lado, ou destinar-se a um endereço MAC de difusão (*broadcast* ou *multicast*) ou ainda destinar-se a um endereço MAC desconhecido.



Divisão de uma rede em dois domínios de colisão com uma Bridge

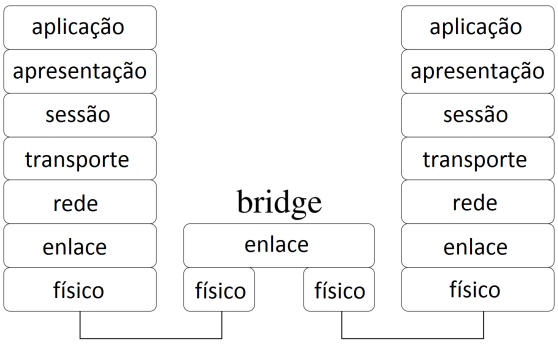
Para evitar ciclos de retransmissão em redes com várias bridges, estas rodam um algoritmo denominado *spanning tree* (árvores de abrangência), utilizado para o reenvio de frames incluídos nos casos de difusão ou de localização desconhecida.

O **Spanning Tree Protocol** (STP) possibilita a inclusão de ligações redundantes entre os comutadores, provendo caminhos alternativos no caso de falha de uma dessas ligações. Nesse contexto, ele serve para evitar a formação de *loops* entre os comutadores e permitir a ativação e desativação automática dos caminhos alternativos e auxiliando na melhor *performace* da rede



Os quadros (frames) são recuperados em uma memória antes de (eventualmente) serem retransmitidos pela bridge, o que possibilita a interligação de segmentos que operem em velocidades diferentes.

Uma vez que trabalha no nível de frames e faz filtragem através de endereços MAC, a bridge opera na camada de ligação lógica (enlace - camada 2) do modelo OSI.



Com o uso de uma bridge, os segmentos de rede são unidos para formar uma única rede (um único domínio de broadcast), porém o tráfego de dados nos dois segmentos passa a ser isolado, com gerenciamento da bridge, restringindo o domínio de colisão a cada segmento.

- **Access Point**

Um ponto de acesso (AP - Access Point) é uma bridge em que (pelo menos) um dos segmentos é sem fios (wireless). Os pontos de acesso são usados como interface entre um segmento cabeado e um segmento wireless.

A aparência de um AP é muito similar à de roteadores sem fio populares, porém o AP não interliga redes diferentes.

- **Switch**

Embora o termo **switch** (comutador) possa referir-se a diferentes tipos de dispositivos que trabalham em diferentes camadas do modelo OSI — um comutador **ATM** (*Asynchronous Transfer Mode*) trabalha na camada de rede (camada 3) e historicamente utilizou-se o termo *packet switch* para designar *routers* — no uso mais frequente, hoje em dia, refere-se ao dispositivo que comuta frames, efetuando filtragem com base nos endereços MAC.

Na realidade, um comutador Ethernet (*switch*) não é mais que uma bridge com múltiplas portas. É, portanto, um dispositivo que opera na camada de ligação lógica (camada 2) do modelo OSI.
Em termos de aspecto físico, um comutador Ethernet (*switch*) é muito semelhante a um hub; por vezes, a única maneira de os distinguir visualmente é pelo fato de ter escrito hub ou switch em seu painel.

Exemplo da aparência de um switch

No switch, assim como nas bridges, apesar de transmitir mensagens de broadcast, o domínio de colisão fica restrito a cada porta.

Há switches usados em redes de alta capacidade e redes corporativas que são gerenciáveis e possibilitam a criação de ***VLANs***.

Uma **rede local virtual**, normalmente denominada de **VLAN**, é uma rede logicamente independente. Várias VLAN's podem co-existir em um mesmo comutador (switch), de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando domínios de broadcast separados. Uma VLAN também torna possível colocar em um mesmo domínio de broadcast, hosts com localizações físicas distintas e ligados a switches diferentes. Outro propósito de uma rede virtual é restringir acesso a recursos de rede sem considerar a topologia da rede, porém este método é questionável.

Redes virtuais operam na camada 2 do modelo OSI. No entanto, uma VLAN geralmente é configurada para mapear diretamente uma rede ou sub-rede IP, o que dá a impressão que a camada 3 está envolvida.

Os enlaces **switch-a-switch** e **switch-a-roteador** são chamados de **troncos**. O processo de interligar mais de uma VLAN através de um link único é chamado de **trunking**. Um roteador ou switch de camada 3 serve como o backbone entre o tráfego que passa através de VLANs diferentes.

- **Router**

O roteador (router) é um dispositivo que permite interligar redes diferentes. A função primordial de um router é o reenvio (*forwarding*) de pacotes entre as suas diferentes interfaces. No entanto, para desempenhar esta função, os routers necessitam manter tabelas de encaminhamento atualizadas. Para o fazerem de forma autônoma e distribuída, os routers rodam um ou mais protocolos de encaminhamento (routing) que lhe permitem preencher e atualizar as suas tabelas de roteamento.

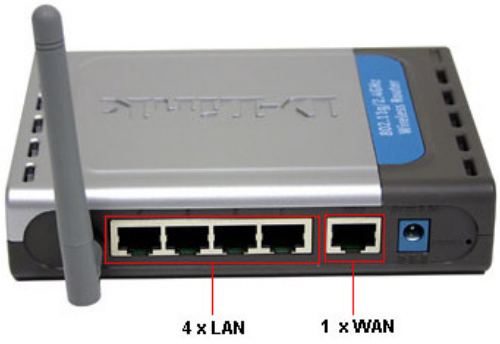
Roteadores

Enquanto o reenvio de pacotes é uma função do plano de dados, o encaminhamento (escolha da rota) é uma função do plano de controle. Além destas duas funções, a maioria dos routers suporta muitas outras funções (NAT, DHCP, etc.); contudo, são o reenvio e roteamento que lhe dão nome.

Os routers transportam os pacotes (datagramas) desde o terminal de origem até ao terminal de destino. Trabalham, portanto, na camada de rede (camada 3) do modelo OSI.

São exemplos de protocolo de roteamento, o protocolo RIP (*Routing Information Protocol*) e o OSPF (*Open Shortest Path First*).

Com a popularização de redes locais, a figura do roteador de baixo custo se tornou muito comum. Seu aspecto é parecido com o do AP, mas ele interconecta redes. Normalmente tem uma porta designada WAN, para conexão externa (Internet, no uso mais corriqueiro) e quatro portas para rede local comutada (switch). Opcionalmente pode ter também uma interface sem fio (wireless) para rede local.



Apesar de oferecerem 254 endereços de hosts em suas conexões, muitos roteadores populares (de baixo custo) têm grandes limitações de conexão de LAN. Alguns, como os roteadores *android* (de celulares) permitem apenas quatro conexões de hosts.

- **Switches da camada 3**

Enquanto a maioria dos switches opera na camada de enlace de dados (camada 2) do Modelo de referência OSI, alguns incorporam funções de um roteador e também operam na camada de rede (camada 3). Na verdade, um switch de camada 3 é muito parecido com um roteador.

Quando um roteador recebe um pacote, ele observa os endereços da fonte e do destino da camada 3 para determinar o caminho que o pacote deve tomar. Um switch padrão utiliza os endereços MAC para determinar a fonte e o destino do pacote. Este procedimento é feito na camada 2 (enlace de dados) da rede.

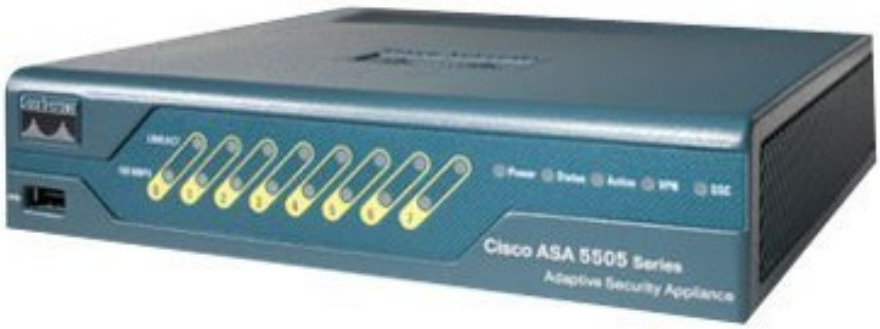
A principal diferença entre um roteador e um switch de camada 3 é que os switches têm hardware otimizado para transmitir dados tão rapidamente quanto os switches de camada 2. Entretanto, eles ainda decidem como transmitir o tráfego na camada 3, exatamente como um roteador faria. Dentro de um ambiente LAN, um switch de camada 3 é geralmente mais rápido do que um roteador porque é construído para ser um hardware de comutação. Muitos switches de camada 3 da Cisco são, na verdade, roteadores que operam mais rapidamente porque são construídos com pastilhas personalizadas de comutação.

O reconhecimento de padrões (*pattern matching*) e a memória cache em switches de camada 3 funcionam de maneira semelhante a um roteador. Ambos utilizam um protocolo e uma tabela de roteamento para determinar o melhor caminho. Entretanto, um switch de camada 3 tem a capacidade de reprogramar dinamicamente um hardware com as informações atuais de roteamento da camada 3. Por isso o processamento dos pacotes é mais rápido.

Nos switches de camada 3 atuais, as informações recebidas pelos protocolos de roteamento são utilizadas para atualizar a memória cache das tabelas do hardware.

- **Firewall**

Um **firewall** é um dispositivo que inspeciona o tráfego que o atravessa e, mediante um conjunto de regras, permite ou nega a passagem a determinados pacotes. O firewall intercala-se entre a rede interna e a rede externa, isolando a primeira da segunda por motivos de segurança - pode permitir-se o acesso à rede externa por parte de máquinas da rede interna, mas normalmente nega-se o acesso de máquinas da rede externa à rede interna. Além destas duas zonas, normalmente os firewalls suportam uma terceira, designada zona desmilitarizada (*Demilitarized Zone* - **DMZ**), na qual se colocam máquinas às quais se permite o acesso (embora restrito) a partir do exterior.



Exemplo de Firewall: Cisco ASA5505

Os firewalls de primeira geração efetuavam apenas uma filtragem *stateless*; os de segunda geração podem manter informação de estado para as conexões que as atravessam e efetuar a filtragem com base não apenas em pacotes individuais, mas também na relação de cada pacote com os anteriores da

mesma conexão (*stateful*); os firewals de terceira geração podem, adicionalmente, entender (pelo menos parcialmente) alguns protocolos de aplicação (http, ftp, DNS, protocolos P2P) e, assim, detectar se pacotes de algum protocolo indesejado estão circulando numa porta não-*standard* (fora de padrão) ou se algum serviço está sendo atacado usando o protocolo de uma forma que se sabe ser nociva.

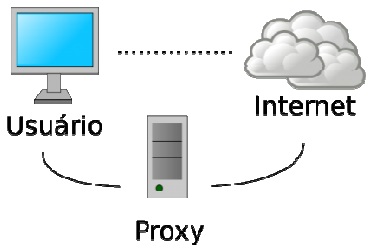
Os firewalls trabalham pelo menos nas camadas de rede e de transporte (camadas 3 e 4) do modelo OSI, embora alguns possam usar também critérios da(s) camada(s) superiores.

- **Proxy**

A tradução da palavra inglesa proxy, segundo o dicionário Michaelis, significa procurador, substituto ou representante.

O proxy surgiu da necessidade de conectar uma rede local à internet através de um computador da rede que compartilha sua conexão com as demais máquinas. Em outras palavras, podemos dizer que o proxy é que permite as máquinas da rede interna terem acesso à rede externa.

Geralmente, máquinas da rede interna não possuem endereços válidos na internet e, portanto, não têm uma conexão direta com a internet. Assim, toda solicitação de conexão de uma máquina da rede local para um host da internet é direcionada ao proxy, este, por sua vez, realiza o contato com o host desejado, repassando a resposta à solicitação para a máquina da rede local. Por este motivo, é utilizado o termo proxy para este tipo de serviço, que é traduzido para *procurador* ou *intermediário*. É comum termos o proxy com conexão direta com a internet.



Um servidor proxy pode, opcionalmente, alterar a requisição do cliente ou a resposta do servidor e, algumas vezes, pode disponibilizar este recurso mesmo sem se conectar ao servidor especificado. Pode também atuar como um servidor que armazena dados em forma de cache em redes de computadores. São instalados em máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.

Uma aplicação proxy popular é o proxy de armazenamento local (ou cache) web, em inglês ***caching web proxy***, um proxy web usado para armazenar e atualizar (conforme pré-programado). Este provê um armazenamento local de páginas da Internet e arquivos disponíveis em servidores remotos da Internet assim como sua constante atualização, permitindo aos clientes de uma rede local (LAN) acessá-los mais rapidamente e de forma viável sem a necessidade de acesso externo.

Quando recebe uma requisição para acesso a um recurso da Internet (a ser especificado por uma URL), um proxy que usa cache procura resultados da URL em primeira instância no armazenamento local. Se o recurso for encontrado, este é consentido imediatamente. Caso contrário, carrega o recurso do servidor remoto, retornando-o ao solicitante e armazena uma cópia deste na sua unidade de armazenamento local.

É importante notar que, utilizando um proxy, o endereço que fica registrado nos servidores externos acessados é o do proxy e não o do cliente.

O proxy usa um algoritmo de expiração para a remoção de documentos e arquivos de acordo com a sua idade, tamanho e histórico de acesso (previamente programado).

Dois algoritmos simples são o ***Least Recently Used*** (**LRU**) e o **Least Frequently Used** (**LFU**).

O **LRU** remove os documentos que passaram mais tempo sem serem usados, enquanto o **LFU** remove documentos menos frequentemente usados.

Uma vez que o proxy atua como intermediário no acesso à rede externa, nele podemos definir a política de regras (*policy*) da rede, bloqueando ou liberando serviços (*ports*), tipos de dados, páginas web, etc.

Uma vez que as funções de firewall e proxy são implementadas em software, é comum termos hosts que atuam como firewall e proxy simultaneamente.

Na Internet é possível encontrar vários **proxies abertos**. Nestes, qualquer usuário da Internet pode fazer uso do *forwarding* (repasse), o que auxilia a manter o anonimato enquanto navega pela web ou usa outro recurso.

Através dos proxies é possível enviar mensagens eletrônicas anônimas e visitar páginas na Internet de forma anônima. Também há mensageiros simples e anônimos, o IRC e o intercâmbio de arquivos.

> - ***Internet Relay Chat (IRC)*** *é um protocolo de comunicação utilizado na Internet. Ele é utilizado basicamente como bate-papo (chat) e troca de arquivos, permitindo a conversa em grupo ou privada. Foi documentado formalmente pela primeira vez em 1993, com a RFC 1459.*

Alguns donos de proxies incluem o registro de *logs* (relatórios) em seus servidores, para diminuir problemas legais. Guardam as requisições e o endereço IP original do usuário. Além disso, alguns enviam cabeçalhos HTTP, como X-Powered-by, contendo o endereço IP original do usuário.

- **Proxy reverso**

Um **proxy reverso** é um servidor de rede geralmente instalado para ficar na frente de um servidor Web. Ele repassa o tráfego de rede recebido para um conjunto de servidores, tornando-o a única interface para as requisições externas.

Por exemplo, um proxy reverso pode ser usado para balancear a carga de um *cluster* de servidores Web, o que é exatamente o oposto de um proxy convencional que age como um despachante para o tráfego de saída de uma rede, representando as requisições dos clientes internos para os servidores externos a rede a qual o servidor proxy atende.

O proxy reverso pode proporcionar segurança, criptografia, balanceamento de carga, cache e compressão de dados.

- **Appliance**

Máquinas que têm função dedicada (*hardware + software*) são também chamadas ***appliance***. A tradução mais simples para este tema é simplesmente "ferramenta". No mundo da informática, as *Appliances* são equipamentos pré-configurados para executar uma tarefa específica, como servir para compartilhar a conexão com a *Web* ou como um *firewall* para a rede, como um sistema de caixa registradora e leitor de código de barras, um centro de multimídia, um centro de controle de um sistema de automatização doméstica e assim por diante. As possibilidades são quase infinitas.

- **NAT Box**

Embora possa existir num equipamento independente (NAT box), a função NAT (*Network Address Translation*) está quase sempre integrada num router ou num *firewall*. A versão mais simples do NAT (tradução apenas de endereços IP) funciona na camada de rede (camada 3) do modelo OSI; versões mais elaboradas (NAPT, masquerading) funcionam nas camadas de rede e de transporte (camadas 3 e 4).

The Bulletin 9300 NAT Device

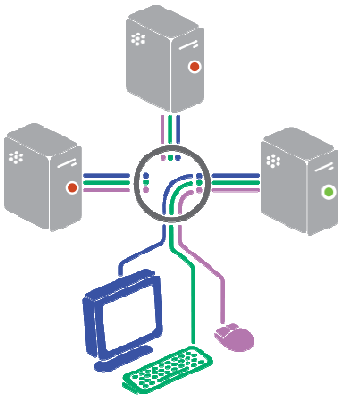
- **Server**

Um servidor (*Server*) é um dispositivo que disponibiliza um ou mais serviços de rede, segundo o modelo *cliente/servidor*. Muito embora o termo servidor se associe, normalmente, a máquinas de grande capacidade e confiabilidade, nem todos os servidores encaixam neste estereótipo (sobretudo em termos de capacidade), é possível construir servidores com base em hardware comum. De fato, uma vez que não necessitam de uma interface gráfica, os servidores dispensam aquele que, hoje em dia, é o subsistema mais complexo e consumidor de recursos num computador pessoal ou *workstation* (estação de trabalho): o subsistema gráfico. Um computador que opera unicamente como servidor é denominado *Servidor Dedicado*. Os computadores clientes dos servidores são as *estações de trabalho* ou *Workstation.*

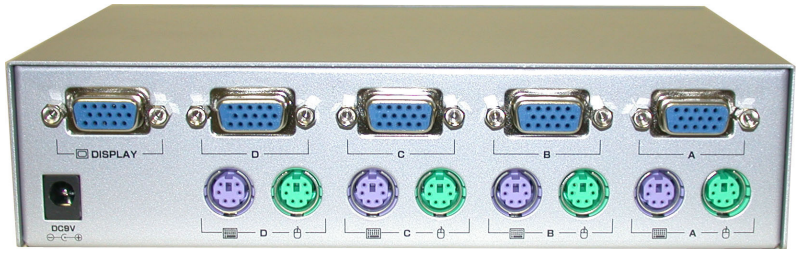
Os servidores trabalham nas camadas superiores (5 a 7) do modelo OSI (camada 4, ou de aplicação, no modelo TCP/IP).

Muitas vezes necessitamos de vários servidores devido às várias aplicações de rede. Neste caso, é comum agrupá-los em um mesmo ambiente, formando um *grupo de servidores*.

Para simplificar a instalação do monitor, teclado e mouse de cada um dos servidores, podemos usar um **KVM Switch** (comutador de ***K****eyboard*, ***V****ideo* e ***M****ouse*).



Com ele, um único monitor, teclado e mouse podem ser compartilhados entre vários computadores. Existem modelos eletrônicos (melhores e mais caros) e mecânicos.



Exemplo de KVM para quatro hosts

Tecnologias de Redes

- **Arcnet**

A Arcnet é uma tecnologia de rede antiga, que existe desde a década de 70. Tornou-se obsoleta com o surgimento e evolução de novas tecnologias como a Ethernet. As redes Arcnet são capazes de transmitir a apenas 2.5 Mbps e quase não existem *drivers* (controladores) para Windows para as placas de rede. Os poucos que se aventuram a usá-las atualmente normalmente as utilizam em modo de compatibilidade, usando *drivers* MS-DOS antigos.

- **Ethernet**

Ethernet é uma tecnologia de interconexão para redes locais baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a camada física, e formato de pacotes e protocolos para a subcamada de controle de acesso ao meio (Media Access Control - MAC) do modelo OSI. A Ethernet foi padronizada pelo IEEE como 802.3. A partir dos anos 90, ela vem sendo a tecnologia de LAN mais amplamente utilizada e tem tomado grande parte do espaço de outros padrões de rede como Token Ring, FDDI e ARCNET.

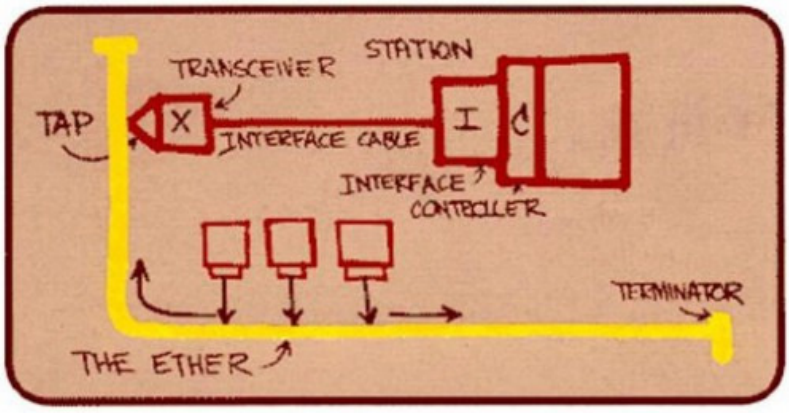
Em 1973 dentro do PARC (o laboratório de desenvolvimento da Xerox, em Palo Alto, EUA), foi feito o primeiro teste de transmissão de dados usando o padrão *Ethernet*. Por sinal, foi no PARC onde várias outras tecnologias importantes, incluindo a interface gráfica e o mouse, foram originalmente desenvolvidas. O teste deu origem ao primeiro padrão Ethernet, que transmitia dados a 2.94 megabits através de cabos coaxiais e permitia a conexão de até 256 estações de trabalho.

O termo "***ether***" era usado para descrever o meio de transmissão dos sinais em um sistema.

No Ethernet original, o "*ether*" era um cabo coaxial, mas em outros padrões pode ser usado um cabo de fibra óptica, ou mesmo o ar, no caso das redes *wireless*. O termo foi escolhido para enfatizar que o padrão Ethernet não era dependente do meio e podia ser adaptado para trabalhar em conjunto com outras mídias.

É importante frisar que isso aconteceu muito antes do lançamento do primeiro micro PC, o que só aconteceu em 1981. Os desenvolvedores do PARC criaram diversos protótipos de estações de trabalho durante a década de 70, incluindo versões com interfaces gráficas elaboradas (para a época) que acabaram não entrando em produção devido ao custo. O padrão Ethernet surgiu, então, da necessidade natural de ligar estas estações de trabalho em rede.

O desenho a seguir foi feito por Bob Metcalf, o principal desenvolvedor do padrão, para ilustrar o conceito:



- **Token Ring**

Foi desenvolvida pela IBM em meados de 1980, essa arquitetura opera a uma velocidade de transmissão de 4 a 16 Mbps. É um protocolo de redes que opera na camada física (ligação de dados) e de enlace do modelo OSI dependendo da sua aplicação. Usa um símbolo (em inglês, *token*), que consiste em uma trama de três bytes, que circula numa topologia em anel em que as estações devem aguardar a sua recepção para transmitir. A transmissão se dá durante uma pequena janela de tempo, e apenas por quem detém o token.

Este protocolo foi descontinuado em detrimento de Ethernet e é utilizado atualmente apenas em infra-estruturas antigas.

- **FDDI**

O padrão **FDDI** (*Fiber Distributed Data Interface*) foi estabelecido pelo ANSI (*American National Standards Institute*) em 1987. Este abrange o nível físico e de ligação de dados (as primeiras duas camadas do modelo OSI).

As redes FDDI adotam uma tecnologia de transmissão idêntica às das redes Token Ring, mas utilizando, normalmente, cabos de fibra óptica, o que lhes concede capacidades de transmissão muito elevadas (em escala até de Gigabits por segundo) e a oportunidade de atingirem distâncias de até 200 Km, conectando até 1000 estações de trabalho. Estas particularidades tornam esse padrão bastante indicado para a interligação de redes através de um backbone – nesse caso, o backbone deste tipo de redes é justamente o cabo de fibra óptica duplo, com configuração em anel FDDI, ao qual se ligam as sub-redes. FDDI utiliza uma arquitetura em anel duplo

- **ISDN**

ISDN é a sigla para *Integrated Services Digital Network*. Essa tecnologia também recebe o nome de **RDSI** - *Rede Digital de Serviços Integrados*. Trata-se de um serviço disponível em centrais telefônicas digitais, que permite acesso à internet e baseia-se na troca digital de dados, onde são transmitidos pacotes por multiplexação sobre condutores de "par-trançado".

A tecnologia ISDN já existe há algum tempo, tendo sido consolidada entre os anos de 1984 e 1986. Através do uso de um equipamento adequado, uma linha telefônica convencional é transformada em dois canais de 64 Kb/s, onde é possível usar voz e dados ao mesmo tempo, sendo que cada um ocupa um canal. Também é possível usar os dois canais para voz ou para dados. De grosso modo, é como se a linha telefônica fosse transformada em duas.

Um computador com ISDN também pode ser conectado a outro que utilize a mesma tecnologia, um recurso interessante para empresas que desejem conectar diretamente filiais com a matriz, por exemplo.

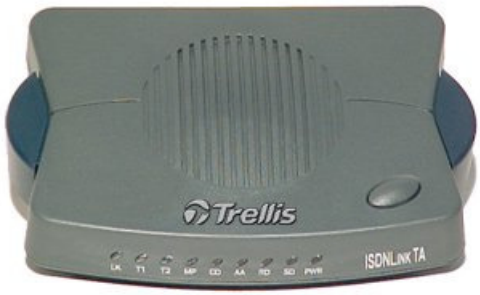
A tecnologia ISDN possui um padrão de transmissão que possibilita aos sinais que trafegam internamente às centrais telefônicas serem gerados e recebidos em formato digital no computador do usuário, sem a necessidade de um modem de linha discada, comum na época. No entanto, para que um serviço ISDN seja ativado em uma linha telefônica é necessária a instalação de equipamentos ISDN no local de acesso do usuário e a central telefônica deve estar preparada para prover o serviço de ISDN.

A largura de banda de uma linha telefônica analógica convencional é de 4 KHz. Numa linha digital ISDN esse valor é de 128 Kb/s, o que faz com que o sinal de 4 KHz não exista mais, pois a interface

da central de comutação na outra "ponta da linha" não trabalha mais com sinais analógicos. Os circuitos eletrônicos da central telefônica efetuam a equalização e detecção do sinal digital a 128 Kb/s transmitido a partir do equipamento do usuário.

Essa técnica de transmissão na linha digital é a conhecida como "*Híbrida com Cancelamento de Eco*". O equipamento do usuário recebe o fio do telefone proveniente da rede telefônica e disponibiliza duas ou mais saídas: uma para o aparelho telefônico e a outra para a conexão com o computador, geralmente via cabo serial.

Quando o equipamento do usuário é informado pela central telefônica que chegará até ele uma chamada telefônica, ou quando o usuário aciona o aparelho telefônico para realizar uma chamada, automaticamente um dos dois canais utilizados na transmissão de 128 Kb/s passa a transmitir os dados a 64 Kb/s enquanto o usuário utiliza o telefone para voz, no canal disponibilizado. Após o término do uso de voz, o canal volta a ser usado para a transmissão de dados a 128 Kb/s. No entanto, é importante frisar que o equipamento de ISDN do usuário tem que ter suporte a este mecanismo (conhecido como *call bumping*), caso contrário esse recurso pode não funcionar e o usuário não receber a chamada telefônica.



Equipamento RDSI da Trellis

- **SNA**

SNA significa *System Network Architecture* e é propriedade da **IBM**. Foi definida antes do modelo OSI e é também baseada numa estrutura de camadas. As duas arquiteturas possuem muitas semelhanças, embora também haja muitas diferenças nos serviços que são prestados e na maneira como estes serviços estão distribuídos entre as camadas. É ainda utilizada geralmente em sistemas de grande porte (mainframes).

- **X.25**

X.25 é um conjunto de protocolos padronizado pela ITU para redes de longa distância e que usam o sistema telefônico ou ISDN como meio de transmissão.

O protocolo X.25 foi lançado em 1970 pelo *Tymnet*, sendo baseado em uma estrutura de rede analógica, predominante na época de sua criação. É considerado o precursor do protocolo *Frame Relay*. Como protocolo de rede sua função é gerenciar pacotes organizando as informações, atuando na camada de enlace do RM-OSI (camada de enlace). O X.25 executa esta tarefa ficando responsável pela interpretação de uma onda modulada recebida, efetuando a demodulação do sinal e lendo o cabeçalho de cada pacote. Quando uma informação entra na interface de rede esse é o primeiro protocolo a ser acionado. Muito utilizado hoje para troca de dados dos Pin Pad (máquinas de cartão de crédito).

No X.25 a transmissão de dados ocorre entre o terminal cliente denominado de *Data Terminal Equipment* (**DTE**) e um equipamento de rede denominado *Data Circuit-terminating Equipment* ou *Data Communications Equipment* (**DCE**). A transmissão dos pacotes de dados é realizada através de um serviço orientado a conexão (a origem manda uma mensagem ao destino pedindo a conexão antes de enviar os pacotes), garantindo assim a entrega dos dados na ordem correta, sem perdas ou duplicações.

- **Frame Relay**

O **Frame Relay** é uma tecnologia de comunicação de dados de alta velocidade que é usada em muitas redes ao redor do mundo para interligar aplicações do tipo LAN, SNA, Internet e Voz.

Basicamente pode-se dizer que a tecnologia Frame Relay fornece um meio para enviar informações através de uma rede de dados, dividindo essas informações em *frames* (quadros) ou *packets* (pacotes). Cada frame carrega um endereço que é usado pelos equipamentos da rede para determinar o seu destino.

A tecnologia Frame Relay utiliza uma forma simplificada de chaveamento de pacotes, que é adequada para computadores, estações de trabalho e servidores de alta performance que operam com protocolos inteligentes, tais como SNA e TCP/IP. Isto permite que uma grande variedade de aplicações utilize essa tecnologia, aproveitando-se de sua confiabilidade e eficiência no uso de banda.

O Protocolo Frame Relay, sendo descendente direto do X-25, utiliza-se das funcionalidades de multiplexação estatística e compartilhamento de portas, porém com a alta velocidade e baixo atraso (*delay*) dos circuitos TDM (*Time Division Multiplex*). Isto é possível pois o mesmo não utiliza o processamento da camada de rede (camada 3) do X.25. Isto exige redes confiáveis para a sua implementação eficiente, pois em caso de erro no meio de transmissão, ocorre um aumento significativo no número de retransmissões, pois a checagem de erros ocorre somente nas pontas.

O protocolo Frame Relay proporciona orientação à conexão em sua camada de trabalho (camada 2 do modelo OSI - Enlace).

- **ATM**

O ATM (*Asynchronous Transfer Mode*) surgiu em 1990. Foi desenhado como um protocolo de comunicação de alta velocidade que não depende de nenhuma topologia de rede específica. É uma tecnologia de comunicação de dados de alta velocidade usada para interligar redes locais, metropolitanas e de longa distância para aplicações de dados, voz, áudio e vídeo.

Basicamente a tecnologia ATM fornece um meio para enviar informações em modo assíncrono através de uma rede de dados, dividindo essas informações em pacotes de tamanho fixo de 53 bytes (48 bytes de dados e 5 de cabeçalho) denominados **células** (*cells*). Cada célula carrega um endereço que é usado pelos equipamentos da rede para determinar o seu destino.

Uma célula é análoga a um pacote de dados, à exceção que as células ATM nem sempre contém a informação de endereçamento de camada superior nem informação de controle de pacote.

A velocidade do ATM começa em 25 Mbps, 51 Mbps, 155 Mbps e superiores. Estas velocidades podem ser atingidas com cabeamento de cobre ou fibra óptica (com a utilização exclusiva de cabeamento em fibra óptica pode-se atingir até 622.08 Mbps). Estas velocidades são possíveis porque o ATM foi desenhado para ser implementado por hardware em vez de software, sendo assim são conseguidas velocidades de processamento mais altas.

- **DSL**

A linha digital de assinante (*DSL – Digital Line Subscriber,* ou ainda **xDSL**) é uma família de tecnologias que fornecem um meio de transmissão digital de dados, aproveitando a própria rede de telefonia que chega na maioria das residências. As velocidades típicas de download de uma linha DSL variam de 128 Kbits/s até 52 Mbits/s dependendo da tecnologia implementada e oferecida aos clientes. Quando as velocidades de upload são menores do que as de download é denominado **ADSL** e quando as velocidades são iguais é **SDSL**.

O DSL é a base para várias tecnologias: DSL: ADSL, ADSL Lite, ADSL2, ADSL2+, SDSL, IDSL, HDSL, RADSL, VDSL, VDSL2, G.SHDSL, VoDSL, PDSL e UDSL.

No **ADSL** (*Asymmetric Digital Subscriber Line*) convencional, geralmente as menores taxas de Download começam em 64 Kbit/s e podem atingir 8 Mbit/s dentro de 300 metros de distância da central telefônica onde está instalado o sistema. As taxas podem chegar a 52 Mbit/s dentro de 100 metros (o denominado **VDSL** - Very-high-bit-rate Digital Subscriber Line).

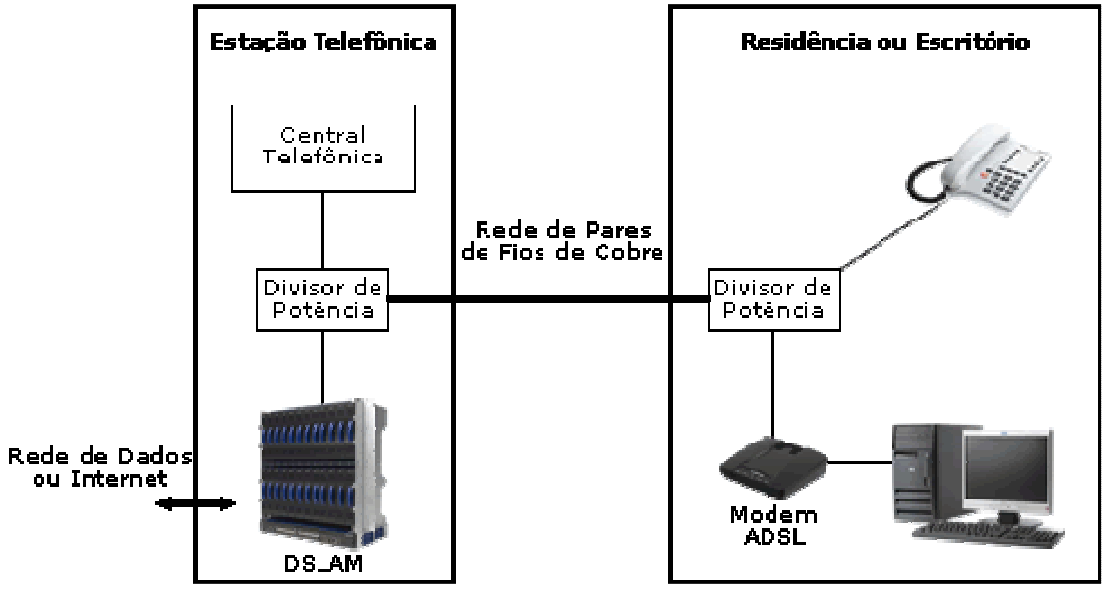
As taxas de envio geralmente começam em 64 Kbit/s e vão até 256 Kbit/s, mas podem ir até 768 Kbit/s. O nome **UDSL** é às vezes usado para versões mais lentas (*Universal Asymmetric Digital Subscriber Line* ou UADSL, UDSL ou ADSL Lite).

São componentes de uma rede ADSL:

Modem ADSL: Na residência ou escritório do usuário é instalado um modem ADSL para conexão com um PC. O modem é geralmente conectado a uma placa de rede no micro. Este micro pode servir de servidor para uma pequena rede local.

Divisores de potência: Divisores de potência e filtros colocados na residência do usuário e na Estação telefônica permitem a separação do sinal de voz da chamada telefônica do tráfego de dados via ADSL.

DSLAM: Na estação telefônica cada par telefônico é conectado a um mutiplexador de acesso DSL (DSLAM). A função do DSLAM é concentrar o tráfego de dados das várias linhas com modem DSL e conectá-lo com a rede de dados.



Componentes de uma rede de acesso ADSL.

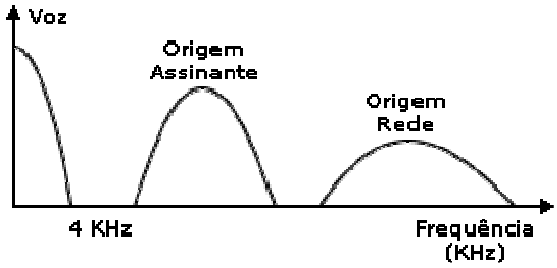
A conexão através de circuitos ATM é a mais utilizada em redes ADSL. Existem equipamentos DSLAM que assumiram o papel de nó de acesso incorporando sistemas de comutação ATM.

Rede de dados: A rede de dados a que se conecta o DSLAM poderá ser a rede do provedor de conexão a Internet ou qualquer outro tipo de rede de dados.

No ADSL a faixa de freqüências de transmissão no pares de cobre é dividida em três canais:

- Serviço telefônico convencional de Voz (0-4 kHz);
- Dados originados no cliente e transmitidos para a rede (tráfego *upstream*);
- Dados originado na rede e transmitidos para o cliente (tráfego *downstream*).

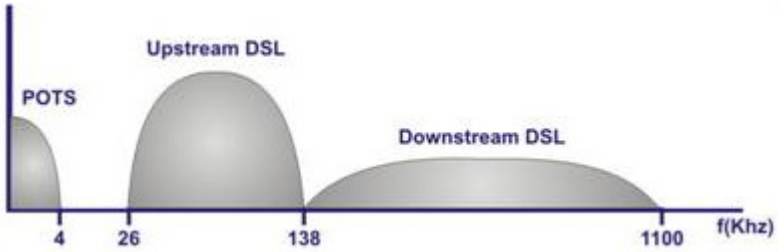
A figura seguinte ilustra estes canais no espectro de freqüências.



É possível desta forma a operação simultânea dos serviços de voz e ADSL e o aumento da taxa de dados pela utilização de freqüências mais altas.

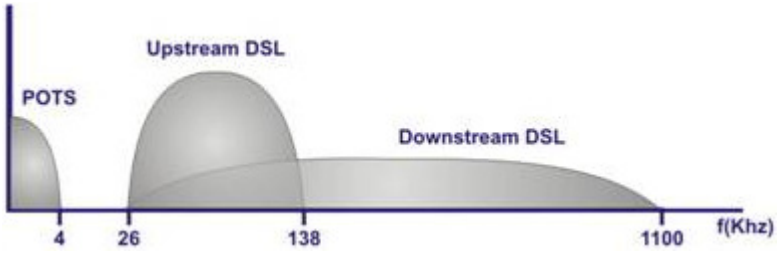
Ao criar canais múltiplos, os modems ADSL dividem a largura de banda disponível de uma linha telefônica utilizando uma das seguintes técnicas: **Multiplexação por Divisão de Frequência** (FDM) ou **Cancelamento de Eco**.

O **FDM** determina uma faixa inferior de dados e outra faixa superior. A inferior é dividida então através de multiplexação por divisão de tempo em um ou mais canais de alta velocidade ou em um ou mais canais de baixa velocidade, conforme mostra figura a seguir. A faixa superior está também multiplexada em canais correspondentes de baixa velocidade.



Espectro de Freqüência do ADSL usando FDM

O **cancelamento de eco** sobrepõe a faixa superior na inferior, e separa os dois por meio de cancelamento de eco local conforme mostra a figura a seguir. Esta técnica é empregada nos padrões V.32 e V.34.



Espectro de Freqüência do ADSL usando Cancelamento de Eco

Em ambas as técnicas, o ADSL divide uma faixa de 4 kHz da linha comum, que é destinada ao tráfego de voz.

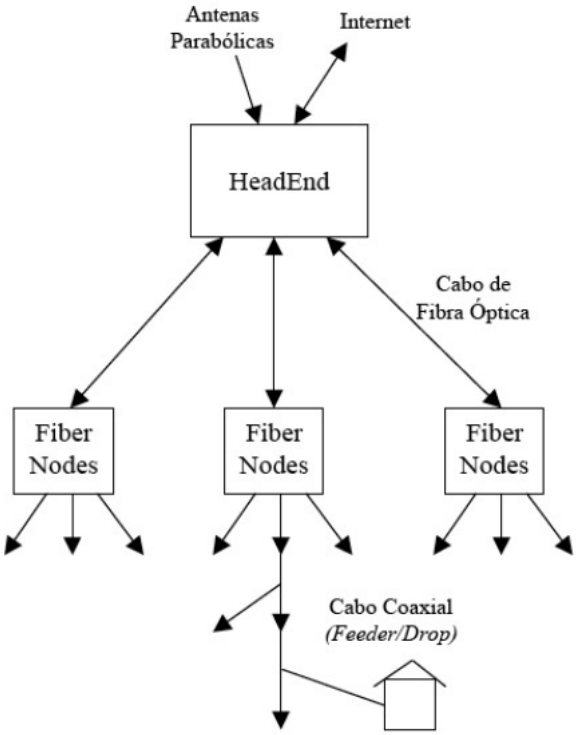
O ADSL é apenas um meio físico de conexão, que trabalha com os sinais elétricos que serão enviados e recebidos. Funcionando dessa forma, é necessário um protocolo para encapsular os dados de seu computador até a central telefônica. O protocolo mais utilizado para essa finalidade é o **PPPoE** (*Point-to-Point Protocol over Ethernet* - RFC 2516).

O **PPPoE** trabalha com a tecnologia **Ethernet**, que é usada para ligar sua placa de rede ao modem, permitindo a autenticação para a conexão e aquisição de um endereço IP à máquina do usuário. É por isso que cada vez mais as empresas que oferecem ADSL usam programas ou o navegador de internet do usuário para que este se autentique. Através da autenticação é mais fácil identificar o usuário conectado e controlar suas ações.

Outra opção é autenticar o usuário através do endereço MAC da placa de rede, onde esta identificação é registrada na operadora. Durante a conexão, essa informação é trocada entre os modens ADSL, e neste momento, a autenticação é realizada.

- **Rede HFC**

Com o passar dos anos, o sistema de televisão cresceu, e os cabos entre as várias cidades foram substituídos por fibra óptica de alta largura de banda, de forma semelhante ao que aconteceu no sistema telefônico. Um sistema com fibra nas linhas principais e cabo coaxial nas ligações para residências é chamado HFC (*Hybrid Fiber Coaxial*) Sistema híbrido de cabo coaxial e fibra.



Outra possibilidade de acesso residencial que se observa é a linha híbrida de cabo de fibra óptica e cabo coaxial. A rigor, essa tecnologia utiliza a infraestrutura de TV a cabo para transmissão de dados até 30 Mbit/s.

A tecnologia modem a cabo, diferentemente das outras tecnologias de acesso residencial, é um meio de transmissão compartilhado. Cada pacote enviado pelo provedor trafega por todos os enlaces até todas as casas. Isso faz com que os pacotes enviados simultaneamente por duas casas diferentes colidam e se destruam. Portanto, a taxa efetiva de transmissão, depende do número de usuários ativos.

Uma possível vantagem da tecnologia ADSL sobre a de modem a cabo reside justamente no fato de ADSL ser uma linha dedicada e não compartilhada. Entretanto, uma rede HFC bem dimensionada provê taxa de transmissão maior que a do ADSL. Opcionalmente, HFC permite utilizar um *Interactive Set-Top-Box*, cuja principal função é a de disponibilizar um maior número de canais de TV, sobre a mesma banda passante. O *Set-Top-Box* cria um canal de retorno que permite ao usuário navegar pela Internet e receber os resultados na tela da TV. Serviços como voz sobre IP, quando bem dimensionados, podem ser implantados com alta qualidade.

A partir de meados dos anos 90, o desenvolvimento de tecnologia digital com baixo custo e o crescente interesse por serviços digitais interativos veio trazer algumas experiências que deram origem a alguns protocolos proprietários.

O **DOCSIS** (*Data Over Cable Service Interface Specifications*) é um padrão técnico internacional desenvolvido por *CableLabs* em conjunto com empresas fornecedoras do setor e define os requisitos de interface dos *cable modems* para a transferência de dados a alto desempenho sobre redes de TV a cabo.

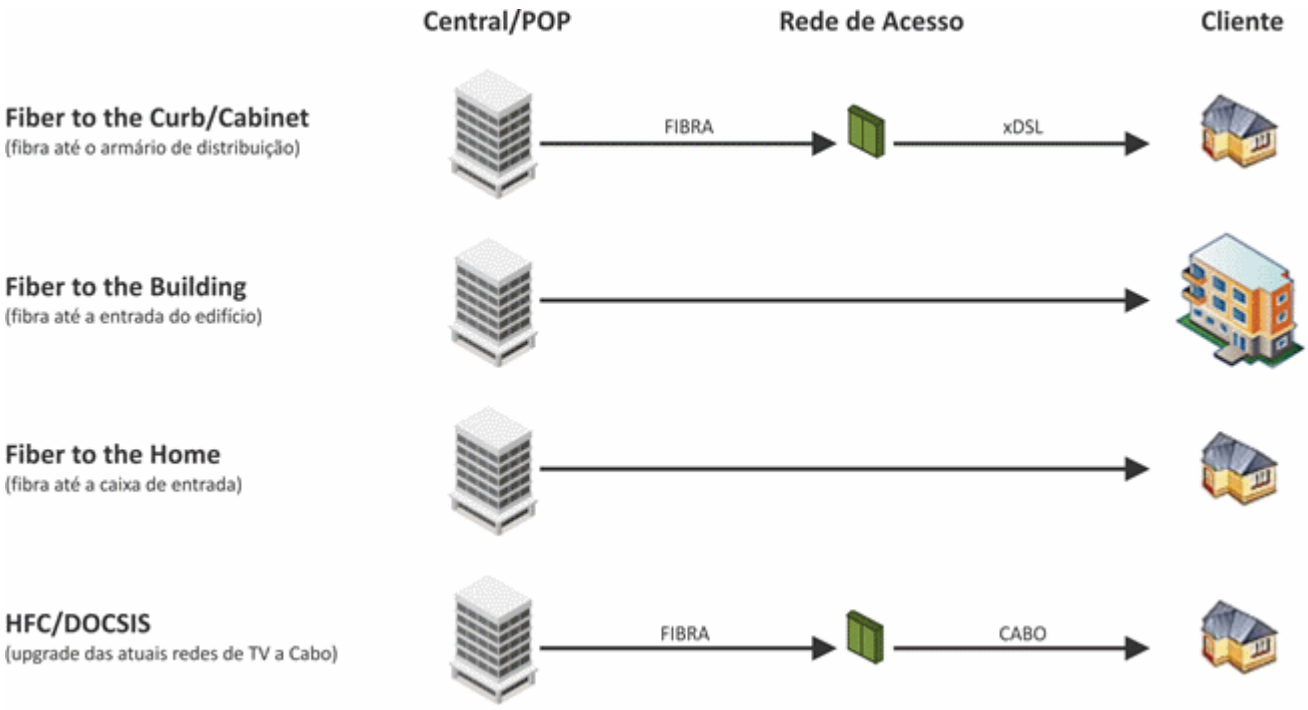
A versão 3.0 do DOCSIS permite a utilização de 4 ou mais canais agregados para a transferência de dados. Embora a especificação não determine um número máximo de canais que podem ser agregados, existe um limite prático, além do fluxo de *downstream*, o meio físico também necessita transportar os canais analógicos e os digitais.

Recentemente, a Cisco realizou um teste onde alcançou quase 1.6 Gbps, utilizando seu novo CMTS (*Cable Modem Termination System*), que suporta agregar até 72 canais no fluxo de *downstream* e 60 canais no de *upstream*.

Além da falta de espectro disponível na rede HFC, outro fator que limita o número de canais que podem ser agregados pelas operadoras é a falta de cable modems que suportem mais de 8 canais agregado. No teste da Cisco, foram utilizados protótipos de cable modems que suportam 16 canais agregados no fluxo de downstream e 4 canais no de upstream. Mesmo assim, foram utilizados três destes protótipos para realizar o teste com 48 canais agregados. É tecnologicamente possível produzir cable modems que agreguem 72 canais ou mais, mas o custo é alto.

- **FTTX**

Uma rede FTTX é uma rede de acesso baseada em fibra que conecta uma grande quantidade de usuários finais (residências, prédios, ERBs, etc.) a um ponto central, conhecido como nó de acesso ou ponto de presença (POP) da operadora.



Uma rede FTTX pode apresentar várias arquiteturas:

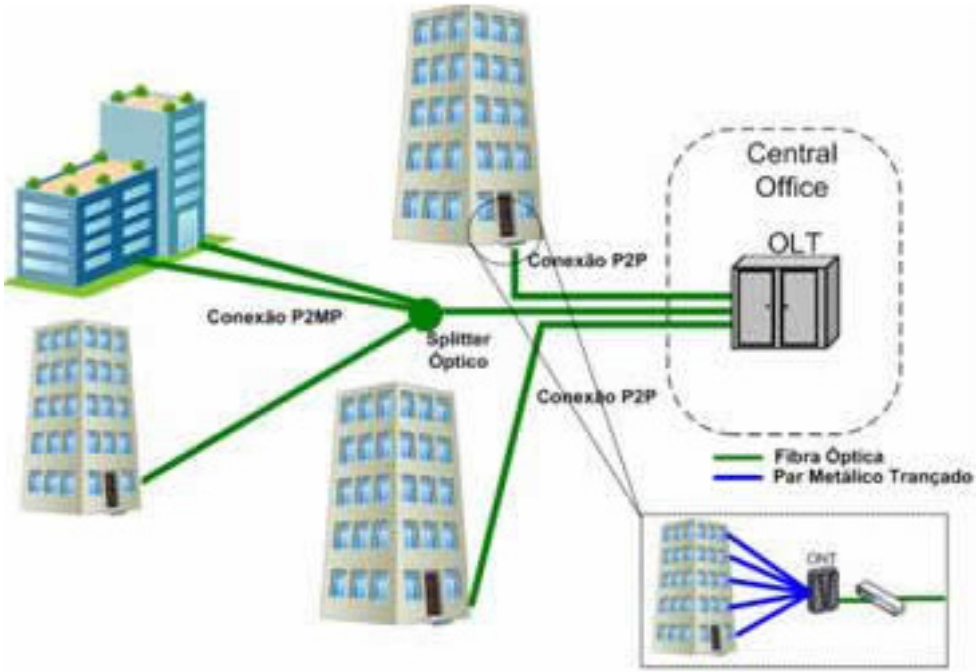
- Fibre to the home (**FTTH**), ou fibra até a residência do usuário final.
- Fibre to the building (**FTTB**), onde a fibra vai até o prédio e a distribuição para os assinantes são feitas através de uma rede Ethernet tendo como meio o cabo coaxial ou o par de cobre.
- Fibre to the curb (**FTTC**) – onde a fibra vai até um armário na rua e a distribuição para os assinantes na quela vizinhança é através deVDSL2 ou Ethernet tendo como meio o cabo coaxial ou o par de cobre.
- Redes Híbridas de Fibra e Cabo (**HFC**), arquitetura utilizada pelas operadoras de TV a Cabo.

- **FTTB – Fibra até o Prédio**

Esta solução permite a implantação de uma fibra óptica ponto-a-ponto e ponto-multiponto. Na sala apropriada do estabelecimento a ser atendido por FTTB é instalada uma ONT (*Optical Network Terminal*) que é conectada a um switch para a distribuição dos serviços aos diversos andares de forma que as conexões entre o switch e equipamento do cliente podem ter terminações óptico – óptico ou óptico – elétrico. Normalmente o atendimento interno a partir do switch é através de uma rede metálica de cabeamento estruturado, onde se tem a aplicação mais comum de tecnologias ADSL2+, VDSL2, 10/100Base-T.

A fibra é terminada num terminal remoto (RT), um equipamento ativo que requer energização e segurança comumente instalado no subsolo do prédio dentro de um armário de utilidades ou numa sala de comunicações. Se o edifício tiver uma solução de cabeamento estruturado do tipo Cat.5 para cada unidade, uma rede Ethernet local é instalada para prover uma banda compartilhada de 10 ou 100 Mbps.

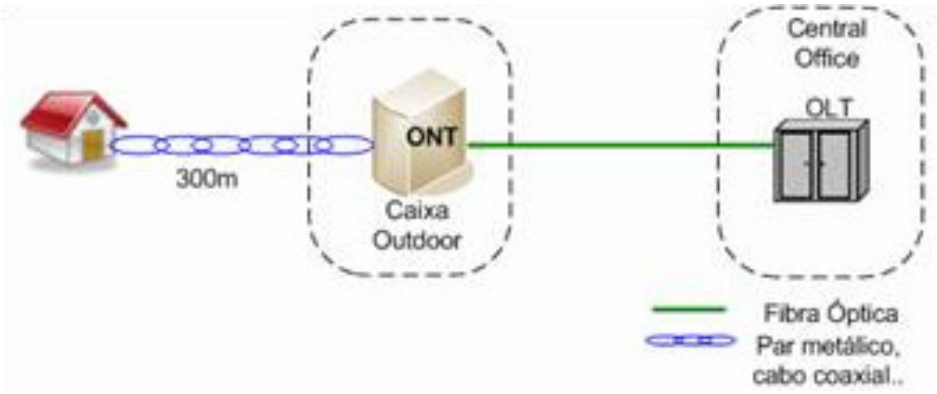
Casos apenas pares de fios telefônicos são disponíveis, o RT é um DSLAM (*Digital Subscriber Line Access Multiplexer*) que provê os serviços de banda necessários no edifício. Atualmente aplicações típicas de FTTB provêm cerca de 10 Mbps.



Solução FTTB em conexão P2P e P2MP

- **FTTC – Fibra até o Armário**

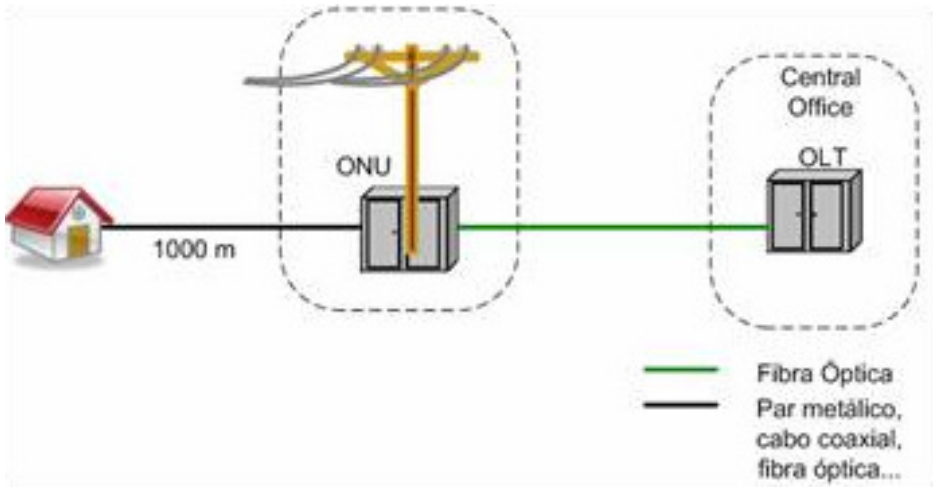
É realizado o atendimento até um distribuidor intermediário (exemplo: uma caixa outdoor instalada no auto de um poste de energia na rua) e a partir do mesmo é realizado o atendimento a um edifício ou residência se utilizando de cabos coaxiais, cabos metálicos, fibra óptica ou algum outro meio para a transmissão das informações. Muito similar ao FTTN (*Fiber to the Node*), mas a distância da ONU (*Optical Network Unite*) ao usuário final não deve ultrapassar 300 metros de distância. Este equipamento deve possuir elementos robustos que suportem grandes variações de temperatura e demais intempéries climáticas no meio em que for instalado, visto que pode haver uma dificuldade com a refrigeração do mesmo, devido as suas instalações.



Solução FTTC

- **FTTN – Fibra até o Nó**

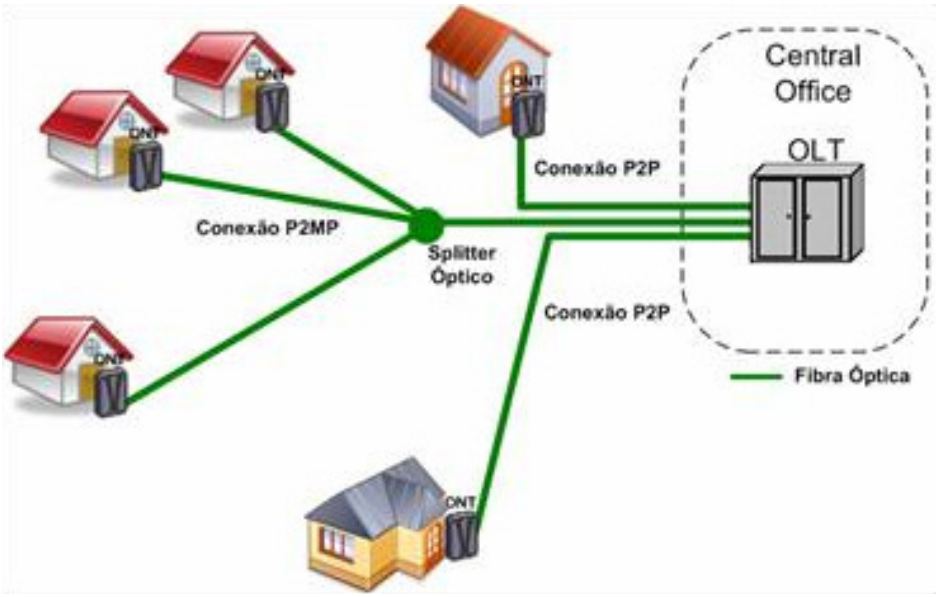
Refere-se a uma arquitetura de atendimento PON (*Passive Optical Network*) em que as ONTs (*Optical Network Terminal*) se distanciam a aproximadamente 1 km (quilometro) do usuário final. Normalmente instaladas em um distribuidor intermediário (Armário) disponibilizam o serviço ao usuário por meio de cabos coaxiais, cabos metálicos, fibra óptica ou algum outro meio para a transmissão das informações.



Solução FTTN

- **FTTH – Fibra até a Casa**

Uma fibra óptica é instalada diretamente da Central (OLT – *Optical Line Terminal*) até a Residência do Cliente (ONU – *Optical Network Unit*). Este atendimento é o que gera maior custo para os prestadores de serviços, pois um novo cabeamento é realizado por ser atendimento óptico e não elétrico - nenhuma estrutura da rede metálica existente é utilizada.



Solução FTTH

As redes FTTH oferecem velocidades de até 100 Mbps. Com o uso crescente da banda larga e a demanda por velocidades maiores aumentaram os investimentos em redes FTTH em todo o mundo.

- **PLC**

O *Power Line Communication* (**PLC**) é uma tecnologia de rede de acesso, ainda não comercial, que transforma a rede de distribuição de energia em uma rede de comunicação pela superposição de um sinal de informação de baixa energia ao sinal de corrente alternada de alta potência.

Com o propósito de assegurar a coexistência correta e a separação entre os 2 sistemas, a faixa de freqüência utilizada para comunicação é bastante distante daquela utilizada para a corrente alternada (50 ou 60 Hz), sendo 1,7 MHz a 50 MHz para aplicações banda larga. Os dois sinais podem conviver harmoniosamente, no mesmo meio. Com isso, mesmo se a energia elétrica não estiver passando no fio naquele momento, o sinal da Internet não será interrompido.

Os fornecedores da tecnologia PLC estão atingindo capacidades de largura de banda de 200 Mbit/s (capacidade partilhada nos fluxos de dados brutos downstream e upstream), velocidade que compete com outras tecnologias de acesso.

A tecnologia PLC pode utilizar à rede de Baixa Tensão (BT) e/ou a rede de Média Tensão (MT) como suporte. A utilização da alta tensão (AT) é objeto de estudos adicionais com possíveis resultados futuros em escala comercial.

A tecnologia PLC é adequada tanto às redes de baixa tensão aérea quanto às redes de distribuição subterrânea.

Entre os principais pontos fortes da tecnologia PLC, os seguintes merecem destaque:

- Utiliza-se da infra-estrutura existente com um potencial de cobertura superior ao das tecnologias competidoras, permitindo estar presente em todas as partes sem precedentes (indoor e outdoor);

- Permite uma implantação rápida, modular e seletiva;

- A instalação interna (em residências e escritórios) é rápida e simples;

- Investimentos e custos operacionais na rede PLC estão ficando a cada ano mais competitivo com relação à ADSL (*Asymmetric Digital Subscriber Line*) e menor do que o serviço de distribuição via cabo;

- O desenvolvimento da tecnologia tira proveito, se apóia e é convergente com os desenvolvimentos mais recentes do quadro de serviços NGN (*Next Generation Network*) e protocolos IP, por exemplo, parâmetros de QoS (*Quality of Service*), IPv6 (Internet Protocol versão 6), etc..

A PLC trabalha na camada 2 do modelo ISO/OSI, ou seja, na camada de enlace. Sendo assim, pode ser agregada a uma rede TCP/IP (camada 3) já existente, além de poder trabalhar em conjunto com outras tecnologias de camada 2.

As principais dúvidas em relação à PLC referem-se à interferência que os aparelhos elétricos exercem sobre ela. Uma das grandes desvantagens é que qualquer "ponto de energia" pode se tornar um ponto de interferência, ou seja, todos os outros equipamentos que utilizam radiofreqüência, como receptores de rádio, telefones sem fio, alguns tipos de interfone e, dependendo da situação, lâmpadas fluorescentes, furadeiras, batedeiras e até mesmo os televisores e outros equipamentos que consome muita energia estão entre os vilões. Mas, de acordo com Orlando César Oliveira, coordenador do empreendimento PLC da COPEL (Companhia Paranaense de Energia), a instalação de filtros nos disjuntores e tomadas da residência reduz o problema. Pelas regras da Agência Nacional de Telecomunicações (Anatel), antes de iniciar uma operação comercial, as empresas devem fazer uma varredura da área para verificar se há conflito com sistemas de comunicações.

Em 13/04/2009, a Anatel publicou a Resolução 527, que aprova o Regulamento sobre Condições de Uso de Radiofreqüências por Sistemas de Banda Larga por meio de Redes de Energia Elétrica (PLC). O documento estabelece os critérios e parâmetros técnicos que permitem a utilização dessa tecnologia de forma harmônica com as aplicações de radiocomunicação que usam radiofreqüência na faixa entre 1,705 kHz e 50 MHz.

Em 18/08/2009, a ANEEL publicou portaria que regulamenta o uso da tecnologia PLC. A Resolução Normativa nº 375/2009 estabelece as condições de compartilhamento da infra-estruturar das distribuidoras.

- **Wi-Fi**

Uma **WLAN** (*Wireless* LAN) é uma rede local sem fio padronizada pelo IEEE 802.11. É conhecida também pelo nome de **WiFi** (*wireless fidelity* – fidelidade sem fios) e a marca registrada pertencente à WECA (*Wireless Ethernet Compatibility Alliance*).

O funcionamento desse tipo de rede é bem parecido com as redes cabeadas: utilizam o TCP/IP.

A configuração da rede *wireless* é feita em duas etapas. Primeiro é preciso configurar o **ESSID** (*Extended Service Set ID*) e o canal, e depois configurar a chave de acesso **WEP** (*Wired Equivalent Privacy*) ou **WPA** (WiFi *Protected Access*).

Quando uma rede WiFi é configurada, é necessário criar o **ESSID**. Trata-se de um nome atribuído à rede. Deste modo, ao se conectar a rede desejada, não ocorre uma troca de dados com a rede incorreta.

Como o sinal de acesso é aberto, quem estiver no raio de alcance conseguirá acessar sem problemas a sua rede. Por esse motivo, quando se configura uma rede com essa característica, deve-se utilizar o serviço de criptografia de dados, deste modo, mesmo que outros usuários consigam captar o sinal, não conseguirão conectar-se à rede sem a chave de decriptografia. Há três tipos de criptografia, o WEP de 64 bits, o WEP de 128 bits e o WPA.

O **WEP** *(Wired Equivalent Privacy* – Privacidade equivalente aos fios*)* foi o primeiro protocolo de criptografia lançado para redes sem fio. O WEP é um sistema de criptografia adotado pelo padrão IEEE 802.11. Ele utiliza uma senha compartilhada para criptografar os dados e funciona de forma estática. Ele fornece apenas um controle de acesso e de privacidade de dados na rede sem fio.

As chaves de acesso utilizam 64 ou 128 bits e o algoritmo **RC4** para criptografar os pacotes, que são transmitidos pelas ondas de rádio. Além disso, faz uso de uma função detectora de erros para verificar a autenticidade e dados.

Poucos anos após ter sido lançado, várias vulnerabilidades foram encontradas no uso do protocolo, até que o WPA foi lançado.

O **WPA** (*Wi-Fi Protected Access*) é um protocolo WEP melhorado. Também chamado de **WEP2**, ou **TKIP** (*Temporal Key Integrity Protocol*), essa primeira versão do WPA surgiu de um esforço conjunto de membros da *Wi-Fi Aliance* e de membros do *IEEE* empenhados em aumentar o nível de segurança das redes sem fio, em 2003, combatendo algumas das vulnerabilidades do WEP.

Apesar de não ser o padrão IEEE 802.11, é baseado nele e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente:

- Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado.
- Migrar para WPA requer somente atualização de software.
- WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

O **WPA2** (**802.11i**) é considerada a versão final o WPA. A principal diferença entre o WPA e o WPA2 é a forma com a qual ele criptografa os dados. Enquanto o WPA utiliza o **TKIP** como algoritmo de criptografia, o WPA2 utiliza o algoritmo **AES** (*Advanced Encryption Standard).* O algoritmo AES é consideravelmente mais pesado que o TKIP. Por conta disso, as placas mais antigas não suportam o WPA2, nem com um *firmware* atualizado.

O AES é o padrão de criptografia utilizado pelo Governo Norte Americano.

Padrões IEEE

O IEEE (*Institute of Electrical and Electronics Engineers*) instaurou um comitê para padronizar a conectividade sem fio em 1990, além de ser considerada a maior organização profissional do mundo de engenheiros eletrotécnicos e eletrônicos. Em 1997 surgiu o padrão para as conexões e regulamentar o uso de freqüências para transmissão de dados.

Nos itens a seguir, são apresentados alguns dos principais padrões de WiFi utilizados atualmente.

Padrão 802.11b
Esse padrão foi o primeiro padrão para comunicação *wireless* utilizado em grande escala, e com ele foi possível a comunicação e interação com dispositivos de diversos fabricantes.

Nas redes de padrão 802.11b, utiliza-se uma freqüência de banda de 2,4 GHz, permitindo a transmissão de 11 Mbit/s a um alcance de 100 metros. Contudo essa velocidade pode ser alterada dependendo do número de obstáculos presentes na transmissão.

O distanciamento do ponto de acesso faz com que o sinal diminua até que se perca definitivamente e através de alguns softwares específicos, é possível medir a qualidade do sinal.

Padrão 802.11b+
Esse padrão é uma evolução do padrão 802.11b. Com ele é possível se conectar a uma rede a 22 Mbit/s, o dobro do tradicional 802.11b, porém para que isso seja efetivamente possível, as duas placas *wireless* devem ser 802.11b+ e estarem bem próximas do ponto de acesso. Caso ocorra a mistura de dispositivos, como por exemplo, 802.11b e 802.11b+, a velocidade de acesso será 11 Mbit/s respeitando assim o dispositivo mais lento.

Padrão 802.11a
Conforme indica o nome, esse padrão começou a ser desenvolvido antes do padrão 802.11b, porém ficou pronto depois. Com ele é possível trabalhar a uma velocidade teórica de 54 Mbit/s e com uma freqüência de 5 GHz. Também é capaz de compartilhar dados com os padrões 802.11b e 802.11b+ lembrando que a velocidade será sempre considerada à do dispositivo mais lento.

Padrão 802.11g
Esse padrão é a evolução dos padrões anteriores, agrupando o melhor do 802.11b (alcance do sinal) e do 802.11a (taxa de transmissão). Com ele é possível chegar aos 54 Mbit/s. Porém como os outros padrões caso alguém se conecte a rede WiFi com uma placa que não seja 802.11g a rede inteira começará a trabalhar a uma velocidade de 11 Mbit/s. Um ponto importante é que o 802.11g não trabalha com placas tipo 802.11a.

Há também as placas *dual-band*, que transmitem simultaneamente dois canais diferentes, isso faz com que a taxa de transferência seja dobrada. Lembrando que mais uma vez, apesar da velocidade muito superior às outras, o nível máximo de transferência só será atingido caso todas as placas sejam também dual-band.

A transmissão WiFi, no Brasil, ocorre na faixa não licenciada de 2,4GHz.

Nas redes 802.11b e 802.11g estão disponíveis 14 canais de transmissão. No Brasil são permitidos 11 destes, que englobam as freqüências de 2.412 GHz (canal 1) a 2.462 GHz (canal 11), com intervalos de 5 MHz entre eles.

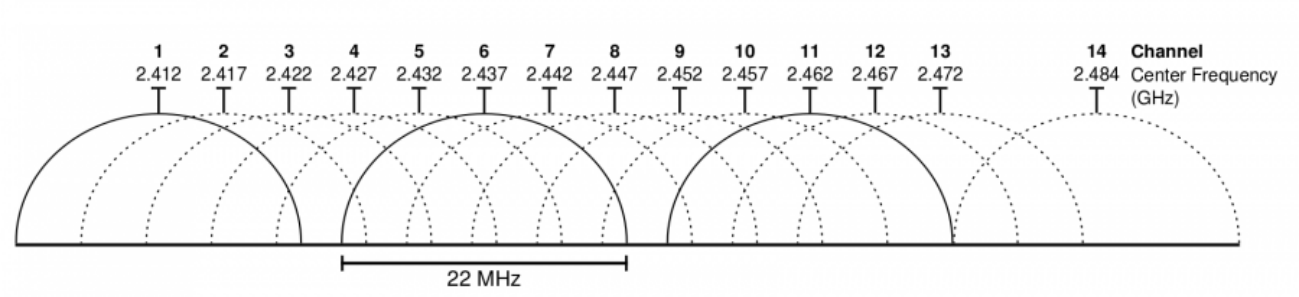
Como os canais utilizam uma banda total de 22 MHz (em muitas citações, o valor é arredondado para 20 MHz), as freqüências acabam sendo compartilhadas, fazendo com que redes operando em canais próximos interfiram entre si.

O canal 6, por exemplo, cuja freqüência nominal é 2.437 GHz, opera na verdade entre 2.426 e 2.448 GHz, invadindo as freqüências dos canais 2 até o 10.

A tabela a seguir mostra a listra de canais Wi-Fi disponíveis no Brasil e cada faixa ocupada.

Canal	Frequência nominal	Faixa de Frequências
1	2.412 GHz	2.401 a 2.423 GHz
2	2.417 GHz	2.405 a 2.428 GHz
3	2.422 GHz	2.411 a 2.433 GHz
4	2.427 GHz	2.416 a 2.438 GHz
5	2.432 GHz	2.421 a 2.443 GHz
6	2.437 GHz	2.426 a 2.448 GHz
7	2.442 GHz	2.431 a 2.453 GHz
8	2.447 GHz	2.436 a 2.458 GHz
9	2.452 GHz	2.441 a 2.463 GHz
10	2.457 GHz	2.446 a 2.468 GHz
11	2.462 GHz	2.451 a 2.473 GHz

Tabela de frequência nominal e faixa ocupada por canal WiFi.



Representação de ocupação dos canais WiFi no espectro de frequências.

Os canais 1, 6 e 11 são os únicos que podem ser utilizados simultaneamente sem que exista nenhuma interferência considerável entre as redes (em inglês, os três são chamados de "*non-overlapping channels*" ou seja, canais que não se sobrepõem).

Isto faz com que muitos usuários do sistema utilizem estes 3 canais como regra, o que é um engano, pois só é valido para um sistema ideal, com apenas 3 redes wifi irradiando. Deve-se levar em consideração todos os canais irradiando nas proximidades para escolher as opções com menor interferência.

A Potência de transmissão

O **ganho da antena** é medido em relação a um **radiador isotrópico** (modelo teórico de antena, onde o sinal seria transmitido igualmente em todas as direções).

Todas as antenas concentram o sinal em determinadas direções, sendo que quanto mais concentrado é o sinal, maior é o ganho. Uma antena de 3 dBi, por exemplo, irradia o sinal com o dobro de potência que um radiador isotrópico, porém irradia em um ângulo duas vezes menor. Uma antena de 6 dBi oferece um sinal quatro vezes mais concentrado, porém para um ângulo 4 vezes mais estreito, e assim por diante.

De uma forma geral, quanto maior é o ganho desejado, maior precisa ser a antena; justamente por isso as antenas ominidirecionais e yagi de alto ganho são muito maiores que as antenas padrão de 2.2 dBi dos pontos de acesso.

A maioria dos modelos domésticos de pontos de acesso trabalham com 17.5 dBm (56 mW) ou 18 dBm (63 mW) de potência, mas existem modelos com apenas 15 dBm (31.6 mW) e, no outro extremo, alguns modelos com até 400 mW (26 dBm) como, por exemplo, o Senao ECB-3220 e o OVISLINK WL-5460:

Senao ECB-3220

OVISLINK WL-5460

É importante notar que, em muitos casos, a potência anunciada pelo fabricante inclui o ganho da antena, de forma que um ponto de acesso com sinal de 20 dBm pode ser, na verdade, um ponto de acesso com transmissor de 18 dBm e uma antena de 2 dBi. Nesse caso, você obteria 24 dBm ao substituir a antena padrão por uma antena de 6 dBi e não 26 dBm (20dBm+6dB) como seria de se esperar. Uma diferença de 2 dBm pode parecer pequena, mas na verdade equivale a um aumento de 66% na potência do sinal, daí a importância de checar as especificações.

Nenhuma antena irradia o sinal igualmente em todas as direções. Mesmo as antenas ominidirecionais irradiam mais sinal na horizontal que na vertical. Isso significa que o sinal é concentrado dentro da área de transmissão da antena, tornando-se mais forte. Como vimos, quanto maior o ganho da antena, mais concentrado e forte é o sinal, fazendo com que ele seja capaz de percorrer distâncias maiores e superar mais obstáculos. Se a potência de transmissão nominal é de 400 mW, o uso de uma antena de 2.2 dBi faria com que, na prática, tivéssemos uma potência de transmissão de 660 mW (28.2 dBm).

Extendendo o alcance para enlaces de longa distância

Substituindo a antena padrão por uma antena *yagi* com ganho de 18 dBi, a potência de transmissão subiria para 44 dBm e, se a antena tivesse 24 dBi, subiria para impressionantes 50 dBm. Na prática, os valores seriam um pouco mais baixos, devido à perda introduzida pelo cabo e pelos conectores, mas ainda assim os números são impressionantes.

Mesmo um ponto de acesso mais simples, com um transmissor de 56 milliwatts (17.5 dBm), pode atingir uma boa potência de transmissão se combinado com uma antena de bom ganho. Usando uma antena setorial de 12 dBi, a potência total de transmissão já seria de 29.5 dBm, o que equivale a 891mW. A principal diferença é que nesse caso o sinal seria concentrado em uma área muito menor, tornando-o utilizável para um link de longa distância, mas não para uma rede doméstica, onde o sinal precisa ficar disponível em todo o ambiente.

Em se tratando de links de longa distância, é preciso ter em mente que a potência de transmissão do ponto de acesso não está necessariamente relacionada à sua sensibilidade de recepção e a falha em

captar o sinal do cliente também leva à perda da conexão. Ou seja, para obter um ganho tangível, é necessário usar produtos com uma maior potência de transmissão dos dois lados do link.

Uma antena de alto ganho (corretamente focalizada), por outro lado, aumenta tanto a potência de transmissão quanto a sensibilidade de recepção, já que é capaz de concentrar o sinal em ambas as direções. É por isso que instalar uma antena *yagi* na placa de um *notebook*, por exemplo, permite que ele consiga se conectar a redes distantes, mesmo sem modificações nos respectivos pontos de acesso.

O sinal transmitido pelo ponto de acesso é espalhado por uma grande área, de forma que apenas uma pequena quantidade da energia irradiada é efetivamente captada pela antena receptora. O mesmo acontece no caminho inverso.

Em um ambiente livre de obstáculos, para 2,4GHz, temos aproximadamente a seguinte perda:

- 500 metros: -94.4 dB
- 1000 metros: -100.4 dB
- 2000 metros: -106.4 dB
- 4000 metros: -112.4 dB

Em um ambiente real, devemos considerar uma perda um pouco maior que a apresentada, com um acréscimo de 6 a 9 dB cada vez que a distância dobra.

A margem é necessária, pois, em uma situação real, raramente se consegue obter um alinhamento perfeito das antenas e também a fatores ambientais, como o vento e a chuva. Sem uma boa margem de tolerância, sua rede poderá ficar instável nos dias nublados, com ventos ou durante as chuvas.

Ao receber o sinal, o receptor precisa amplificá-lo, de forma que ele possa ser processado. Neste ponto deve-se atentar à sensibilidade de recepção (*receive sensitivity*), que corresponde ao nível mínimo de sinal que o receptor precisa para receber os dados, com um volume aceitável de erros de recepção.

Ao criar um link de longa distância, é importante usar pontos de acesso e placas com a maior sensibilidade possível. Com o exposto acima, vimos que uma diferença de apenas 6 dB na recepção permite obter o dobro do alcance, utilizando as mesmas antenas. Este acaba sendo o principal diferencial entre interfaces de rede de diferentes fabricantes, mesmo quando elas são baseadas no mesmo *chipset*.

Uma dica prática é que os pontos de acesso e placas 802.11g atuais oferecem em geral uma recepção melhor do que produtos antigos, baseados no padrão 802.11b (mesmo se utilizadas as mesmas antenas), devido a melhorias nos *chipsets*.

Os aparelhos baseados no 802.11n oferecem uma taxa de transferência muito maior em curtas distâncias, devido ao uso do **MIMO** (*Multiple-input and multiple-output* é o conjunto de técnicas de transmissão para sistemas de comunicação sem fio com múltiplas antenas na transmissão e na recepção), mas esta característica é praticamente inútil em links de longa distância, onde normalmente utilizamos uma única antena. O 802.11n oferece algumas melhorias adicionais no sistema de correção de erros e na transmissão do sinal, que reduzem o *overhead* da transmissão em relação ao 802.11g, resultando em um certo ganho na taxa de transmissão (mesmo com uma única antena), mas não muito.

É possível encontrar a relação entre o nível mínimo de sinal para cada taxa de transferência nas especificações da placa ou do ponto de acesso. A maioria dos dispositivos trabalha com um valor mínimo de -92 dBm e alguns chegam a -95 dBm (note que a sensibilidade de recepção não está necessariamente relacionada à potência de transmissão).

Entretanto, esse valor corresponde à taxa de transmissão mínima, a 1 megabit por segundo. Para que a rede possa trabalhar a velocidades mais altas, é necessário um sinal mais forte.

Para exemplificar, podemos construir uma relação entre taxa de transmissão e potência de recepção baseada nos valores teóricos esperados em uma comunicação sem fio. Os valores podem variar em até 6 dBm, de acordo com a marca e o modelo da placa:

- 1 Mbps: -92 dBm
- 2 Mbps: -91 dBm
- 5.5 Mbps: -90 dBm
- 9 Mbps: -88 dBm
- 12 Mbps: -87 dBm
- 18 Mbps: -86 dBm
- 24 Mbps: -83 dBm
- 36 Mbps: -80 dBm
- 48 Mbps: -74 dBm
- 54 Mbps: -72 dBm

Pela lista podemos ver que um sinal de -98 dBm é muito baixo, mesmo para criar um link de apenas 1 megabit. Para cada redução de 3 dB no sinal, temos uma redução de 50% na potência, de forma que -98 dBi corresponde a apenas um quarto de -92 dBi, que seria o mínimo para estabelecer a conexão, dentro das especificações da lista apresentada.

Diante de tal nível de recepção, uma antena setorial ou yagi com 8 dBi de ganho, devidamente apontada para a antena do ponto de acesso remoto, seria suficiente para elevar o sinal ao nível mínimo (a 1 Mbps), mas seria necessário usar uma antena com pelo menos 26 dBi para ter uma chance de efetuar a conexão na velocidade máxima, a 54 Mbps.

O valor de potência irradiado pela antena é dado em **EIRP** (*equivalent isotropically radiated power*) e corresponde à potência efetiva da transmissão, obtida somando a potência do transmissor e o ganho da antena (descontando perdas causadas pelos cabos, conectores e outros fatores).

Em muitos países da Europa, vigora uma norma muito mais restritiva, que limita as transmissões a apenas 100 milliwatts (20 dBm), o que equivale à potência nominal da maioria dos pontos de acesso, sem modificações na antena ou uso de amplificadores.

No Brasil, vigora uma norma de 2004 da **Anatel** (*resolução 365, artigo 39*) que limita a potência EIRP do sinal a um máximo de 400 milliwatts (26 dBm) em cidades com mais de 500 habitantes. Acima disso, é necessário obter uma licença de operação.

Alguns roteadores sem fio têm o recurso de configurá-los em WDS.

WDS (*Wireless Distribution System*) é um sistema que permite a interconexão de *access points* sem a utilização de cabos ou fios, descrito nas normas do IEEE 802.11 e IEEE 802.16.

Com o WDS, um *access point* pode ser uma base central, de repetição ou remoto. Uma base central é tipicamente conectada à rede por fios. Uma base de repetição retransmite dados entre bases remotas e centrais, clientes wireless ou outras bases de repetição. Uma base remota aceita conexões de clientes wireless e as repassa para estações centrais ou de repetição.

Todas as estações base em uma rede WDS precisam ser configuradas para utilizarem o mesmo canal e compartilharem chaves WEP se for utilizado.

Firmware: A maioria de fornecedores de equipamentos promove melhoras em seus produtos e os disponibiliza na forma de novas versões dos modelos. Essas melhoras também podem ocorrer no software de administração do produto (***firmware***) que pode corrigir falhas que causam instabilidade de funcionamento ou mesmo novas funcionalidades.

Esse *firmware* é o sistema operacional dos roteadores wi-fi. Os fabricantes normalmente o desenvolvem de forma dedicada e proprietária procurando extrair um bom custo/benefício do produto.

Muitos fabricantes consideram como ponto de partida sistemas operacionais de código aberto, como o Linux ou o BSD. Com isso, muitos roteadores wi-fi disponíveis no mercado, possibilitam a substituição de seu *firmware* por outro, construído de forma independente. Essa é a proposta do DD-WRT (http://www.dd-wrt.com).

O DD-WRT é uma alternativa de *firmware Opensource* baseada em Linux suportado por uma grande variedade de equipamentos wi-fi e que pode prover acesso a ajustes não liberados pelo fabricante do equipamento.

Porém, deve-se tomar muito cuidado com a atualização do *firmware*, pois, um erro ou falha no procedimento, como queda de energia, desconexão ou escolha de firmware errado pode inutilizar o aparelho.

- **Bluetooth**

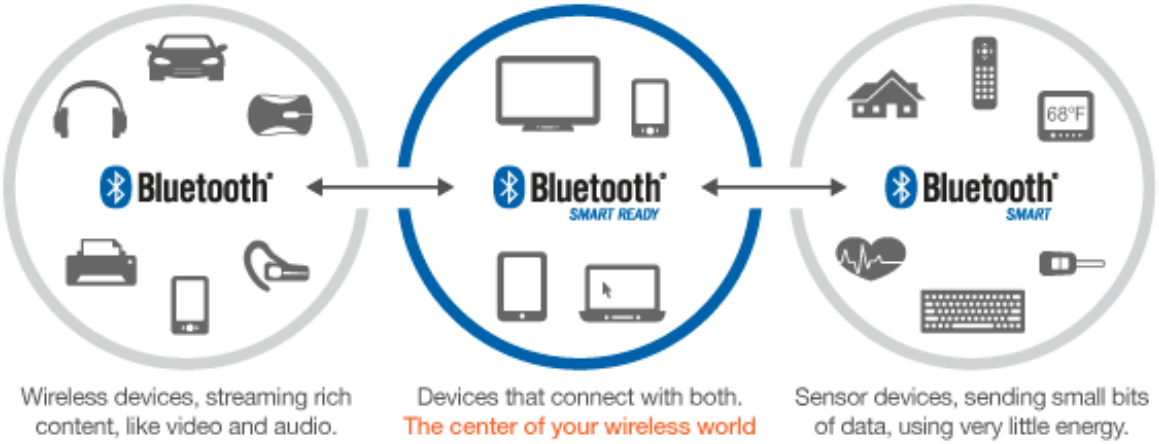
Bluetooth é o nome dado ao protocolo de rádio baseado em saltos de frequências (*frequency-hopping*) de curto alcance (10 a 100 metros) que visa complementar ou substituir ás redes convencionais cabeadas, cujo meio físico de transmissão é o cabo de par trançado, cabo coaxial e fibra óptica.

Este protocolo surgiu em 1994 após a empresa de dispositivos móveis Ericsson (hoje Sony-Ericsson) identificar a deficiência que os dispositivo tinham em estabelecer uma interconexão entre si como, por exemplo: fone de ouvido, aparelhos celulares, impressoras, auto rádio e etc.

Quatro anos após a investigação as empresas IBM, NOKIA, INTEL e TOSHIBA se uniram á Ericsson e desenvolveram o protocolo Bluetooth. A este grupo formado foi dado o nome de *Bluetooth Special Interest Group* (SIG). Um ano depois, se incorporaram ao SIG a 3com, Lucent Technologies, Microsoft e Motorola com a proposta de maior penetração no mercado.

O protocolo recebeu esse nome, em homenagem ao primeiro rei Cristão da Dinamarca, o rei Harald Blatand (Bluetooth, em inglês), por conseguir comandar os reinos da Dinamarca e da Noruega à distância. A sua primeira versão foi lançado em 1999 e suas atualizações trazem a otimização do consumo, além da mesma ser compatível com as versões anteriores.

A figura seguinte ilustra os objetivos de aplicações do Bluetooth.



A proposta do Bluetooth é substituir as várias soluções proprietárias existentes para conexão de dispositivos com uma solução padronizada que possa ser adotada a nível mundial. Os requisitos principais que nortearam o desenvolvimento do Bluetooth foram:

- Baixo consumo de potência;
- Baixo custo, US$ 5 a 10 para adicionar o Bluetooth a um dispositivo.
- Cobertura pequena, tipicamente 10 metros;
- Transmissão de voz, dados e sinalização.

O Bluetooth opera na faixa de frequências de 2,4 GHz a 2,483 GHz que não precisa de autorização para ser utilizada (faixa não licenciada) e adotou o espalhamento espectral por salto de frequência (Frequency-Hopping) de modo a garantir uma comunicação robusta em uma faixa de frequências compartilhada com outras aplicações como o WI-FI e ISM (Industrial, Científica e Médica).

Apesar de ser padronizada pelo IEEE 802.15 como uma WPAN (Wireless Personal Area Network), uma rede Bluetooth assemelha-se mais a um barramento para extensão de portas de um dispositivo como por exemplo o USB (Universal Serial Bus) encontrado nos PCs.

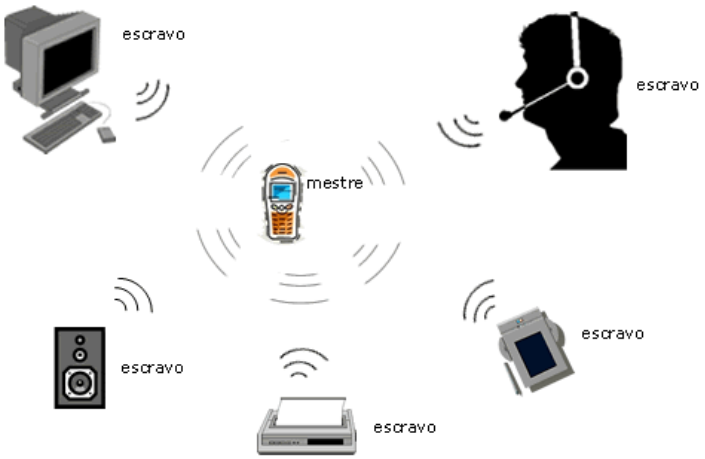
O Bluetooth pode, a grosso modo, ser comparado a um USB wireless onde um dispositivo mestre (PC no caso do USB) se comunica com seus periféricos. A diferença é que no Bluettoth qualquer dispositivo pode assumir o papel de mestre e montar a sua rede de periféricos denominada de *piconet* .

Uma ***piconet*** é uma rede Blootooth formada por até 8 dispositivos, sendo 1 mestre e os demais escravos. Todos os dispositivos estão sincronizados ao relógio e sequência de salto de frequência (*hopping*) do mestre.

Em uma *piconet* toda comunicação ocorre entre mestre e escravos. Não existe comunicação direta entre escravos em uma *piconet*.

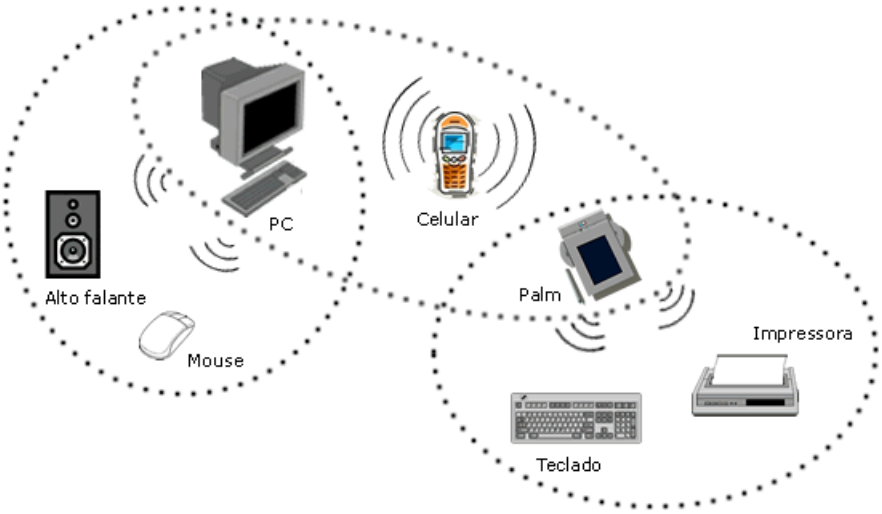
Em um determinado local podem existir várias *piconets* independentes. Cada *piconet* tem um canal físico diferente, ou seja, um dispositivo mestre diferente e um relógio e sequência de salto de frequência independentes.

Um dispositivo Bluetooth pode participar concorrentemente em duas ou mais *piconets*. No entanto não pode ser mestre de mais de uma *piconet*. Como o canal físico que caracteriza a *piconet* é definido pelo relógio e endereço do dispositivo mestre é impossível ser o mestre de duas ou mais *piconets*. Um dispositivo pode ser escravo em várias *piconets* independentes.



Exemplo de Piconet

Um dispositivo Bluetooth que é um membro de duas ou mais *piconets* é dito estar envolvido em uma ***scatternet***. O envolvimento em uma ***scaternet*** não implica necessariamente em qualquer função ou capacidade de roteamento no dispositivo Bluetooth. Os protocolos do Bluetooth não oferecem esta funcionalidade, que é responsabilidade de protocolos de mais alto nível.



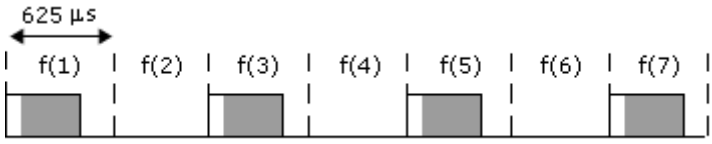
Exemplo de Scatternet

O Bluetooth oferece suporte para dois tipos de tráfego:

- Assíncrono a uma taxa máxima de 723,2 kbit/s (unidirecional).
- Bidirecional síncrono com taxa de 64 kbit/s que suporta tráfego de voz entre os dois dispositivos.

A faixa de frequência ocupada pelo Bluetooth (2,4 GHz a 2,483 GHz) foi divida em 79 frequências com Bandas de 1 MHz entre 2402 MHz e 2480 MHz.

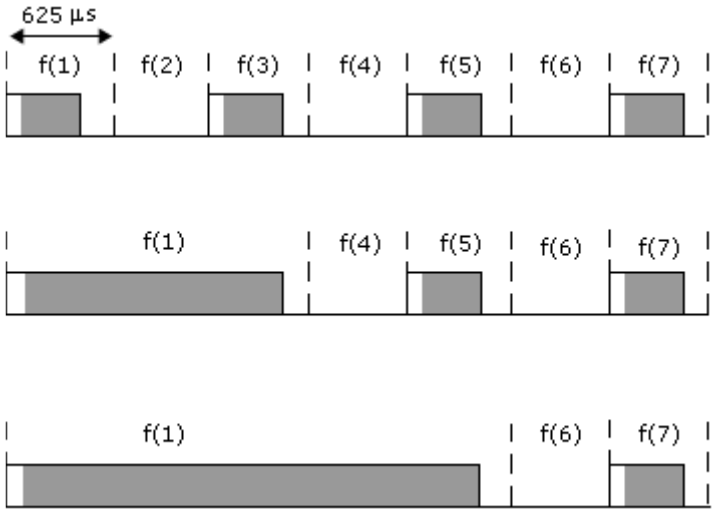
Em um canal físico básico de *piconet* do Bluetooth a sua frequência muda de forma pseudo-aleatória 1600 vezes por segundo (a cada 0,625 µs). O intervalo de tempo de 0,625 µs que dura a transmissão em uma frequência é chamado de *slot*. A sequência de salto de frequência é definida pelo relógio e endereço Bluetooth do dispositivo mestre.



Os dispositivos em uma *piconet* compartilham este canal físico de comunicação. O compartilhamento ocorre usando o método TDMA (*Time Division Multiple Access*), que define *slots* específicos para cada um dos dispositivos conectados através do canal físico (mestre, escravo 1, escravo 2, etc.) alocados em tempos distintos, sobre esse canal. Todos os dispositivos participantes de uma *piconet* utilizam a mesma frequência, porém, ao longo do tempo e de forma organizada, apenas um deles usa o canal para transmitir ou receber informações, de acordo com o *slot* que lhe foi atribuído.

Quando ocorre um salto de frequência os seus transmissores e receptores são sintonizados ao mesmo tempo na nova frequência. A transmissão e a recepção usam o esquema TDD (*Time Division Duplex*), onde a mesma frequência é utilizada tanto para transmitir como para receber informações. A vantagem desse método é a possibilidade de alocar dinamicamente largura de banda entre o enlace direto e o enlace reverso, o que permite ter enlaces de dados assimétricos.

Um pacote de dados é transmitido em cada slot de tempo. É possível também estender o pacote para ocupar 3 ou 5 slots de modo a aumentar a taxa de dados transmitida como apresentado na figura:



O ***release* 1.2** da especificação do Bluetooth definiu também um canal de piconet adaptado que apresenta as seguintes diferenças em relação ao canal básico:

- As frequências nas quais um escravo transmite são as mesmas que o mestre acabou de transmitir. Ou seja, não há um salto de frequência entre um pacote do mestre e o pacote do escravo que vem logo a seguir.

- É possível excluir algumas frequências entre as 79 disponíveis para a sequência de salto de frequências, que são marcadas como fora de uso. Evita-se desta forma a utilização de frequências com alto grau de interferência.

Além destes canais existem ainda dois outros canais físicos utilizados em funções de gerenciamento: inquiry scan e page canal.

O ***release* 2** da especificação do Bluetooth definiu um novo modo de operação, o *Enhanced Data Rate – EDR*, que possibilitou aumentar a taxa da dados na interface rádio para 2 ou 3 Mbit/s (até 2,1 Mbit/s para a camada de aplicação), mantendo a mesma taxa de símbolos de 1 MS/s.

O ***release* 3** da especificação do Bluetooth introduziu um novo modo de operação, o *Alternate MAC/PHY – AMP*, que permitiu o uso de protocolos alternativos nas camadas física (*PHY*) e de controle de acesso ao meio (*MAC*) na interface rádio, para aumentar a taxa de dados para até 54 Mbit/s (até 24 Mbit/s para a camada de aplicação). Adicionalmente, o novo release inclui o uso da faixa de 5 GHz para a comunicação entre os dispositivos.

Os aperfeiçoamentos do ***release* 3** têm como objetivo principalmente propiciar o uso das conexões Bluetooth em aplicações que necessitam grandes transferências de dados, ou em aplicações de vídeo *streaming* sincronizado.

O ***release* 4** atualizou a especificação do Bluetooth para dar suporte aos dispositivos de baixo consumo de energia (*Low Energy*) até a Camada L2CAP, ao *Attribute Protocol (ATT)* e ao *Generic Attribute Profile* (GATT), e para habilitar os *High Speed Controller Subsystems*.

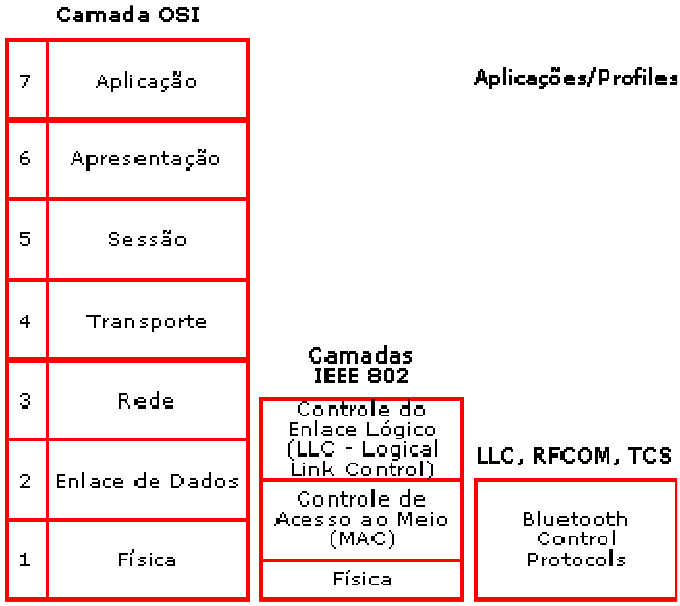
A seguir temos as características dos canais físicos de dispositivos Bluetooth.

PARÂMETRO	INFORMAÇÃO / VALOR
Antena	Omndirecional
Faixa de Frequências	2,4 GHz a 2,483 GHz
Modulação	**GFSK** (*Gaussian Frequency Shift Keying*) – *Basic Rate* **PI/4 DQPSK** (*PI/4 Rotated Differential Quaternary Phase Shift Keying*) – EDR em 2 Mbit/s **8DPSK** (*8 phase Differential Phase Shift Keying*) – EDR em 3 Mbit/s
Taxa de símbolos	1 Mega Símbolo/seg (1 MS/s).
Nº de Canais	79
Banda do Canal	1 MHz
Banda de Guarda	Inferior 2 MHz, superior 3,5 MHz
Potência de transmissão	Classe 1: 1 (0 dBm) a 100 mW (20 dBm) Classe 2: 0,25 (-6 dBm) a 2,5 mW (4 dBm) – nominal = 1 mW Classe 3: <= 1 mW (0 dBm)
Espalhamento Espectral	Salto de frequência (Frequency-Hopping) a cada 625 micro segundo (µseg)

Bluetooth – *Enhanced Rate*

A taxa de dados bruta máxima em um canal físico do Bluetooth varia de 1 a 3 Mbit/s, dependendo do modo de operação (*Basic Rate* e *Enhanced Data Rate*).

A figura a seguir apresenta a relação entre as camadas de protocolo definidas pela especificação core do Bluetooth e as camadas do modelo OSI e do IEEE802. As camadas definidas pela especificação principal (*core*) do Bluetooth correspondem às camadas de MAC e física do IEEE 802.

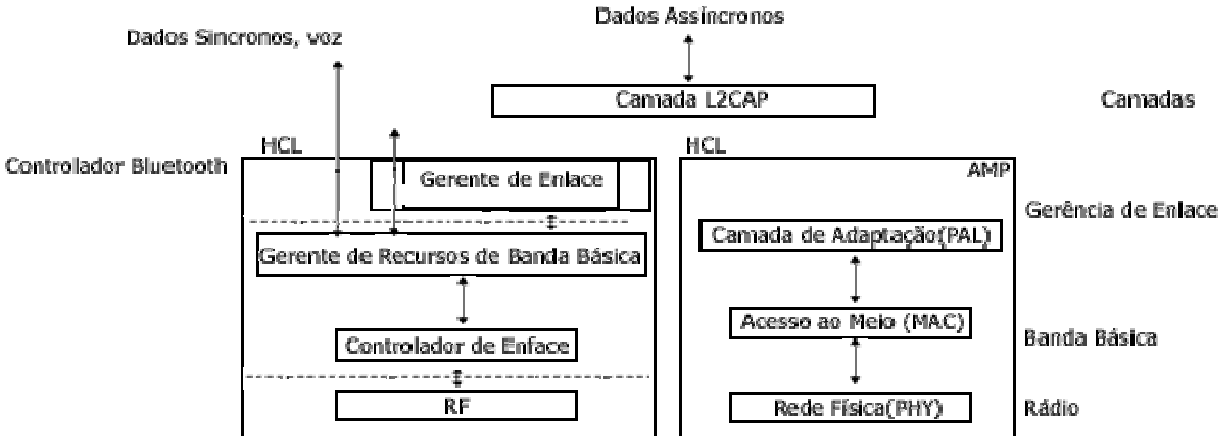


Comparação entre OSI x IEEE 802 x Bluetooth

O Bluetooth core pode ser divido nas seguintes camadas:

- *Logical Link Control Adaptation Protocol* **(L2CAP)**: Fornece serviços de conexão de dados com e sem conexão para as camadas superiores de protocolo. Executa funções de multiplexação, segmentação, controle de fluxo e de erro e gerenciamento de grupo. O L2CAP é utilizado para multiplexar canais lógicos em um único enlace físico.
- **Gerência de Enlace**: É a camada responsável pela codificação e decodificação dos pacotes Bluetooth do pacote de dados e parâmetros relacionados com o canal físico, transporte lógico e enlace lógico. É responsável pelo estabelecimento de enlaces entre os vários dispositivos Bluetooth, controlando a negociação dos tamanhos de pacotes, chaves de segurança, modos de potência e estado de uma unidade na *piconet*.
- **Banda Básica**: Fornece o suporte para o link de RF em funções como sincronização e salto de freqüências e controle de acesso ao meio.
- **Rádio**: É a parte de Rádio Freqüência (RF) propriamente dita;
- **Camada de Adaptação – PAL (AMP)**: fornece os serviços de conversão de protocolo entre a camada MAC e o L2CAP;
- **Acesso ao Meio – MAC (AMP)**: fornece os serviços de controle de acesso ao meio (MAC);
- **Rede Física – PHY (AMP)**: é a rede física propriamente dita, no caso compatível com as redes IEEE802.11.

As 3 camadas inferiores são normalmente implementadas em um Controlador Bluetooth. A interface entre este controlador e um servidor onde residem as camadas superiores do protocolo foi padronizada de modo a garantir a interoperabilidade entre dispositivos de vários fornecedores. Esta interface é chamada de *Host Controller Interface* (HCI).



Existem disponíveis no mercado, na forma de Circuitos Integrados (CI's), que implementam o Controlador Bluetooth através de um ou dois CI's, permitindo inclusive a incorporação de software de camadas superiores como o L2CAP. Para exemplos de fornecedores consulte o site www.bluetooth.com.

O Bluetooth oferece serviços de transporte lógico a serem utilizados por enlaces lógicos de suporte a canais do L2CAP ou protocolos de ordem superior. Estes serviços podem ser classificados em síncronos e assíncronos.

Nos serviços síncronos é feita a reserva de slots no canal físico podendo ser considerado uma forma de conexão comutada a circuito. A taxa de dados é de 64 kbit/s e tipicamente a informação transmitida é voz sendo a interface de áudio feita diretamente na camada de banda básica. Os serviços definidos são o SCO (*Synchronous connection-oriented*) e o eSCO (*Extended SCO*)

Os serviços de dados assíncronos disponíveis no Bluetooth para o transporte de dados como suporte à camada L2CAP e superiores são:

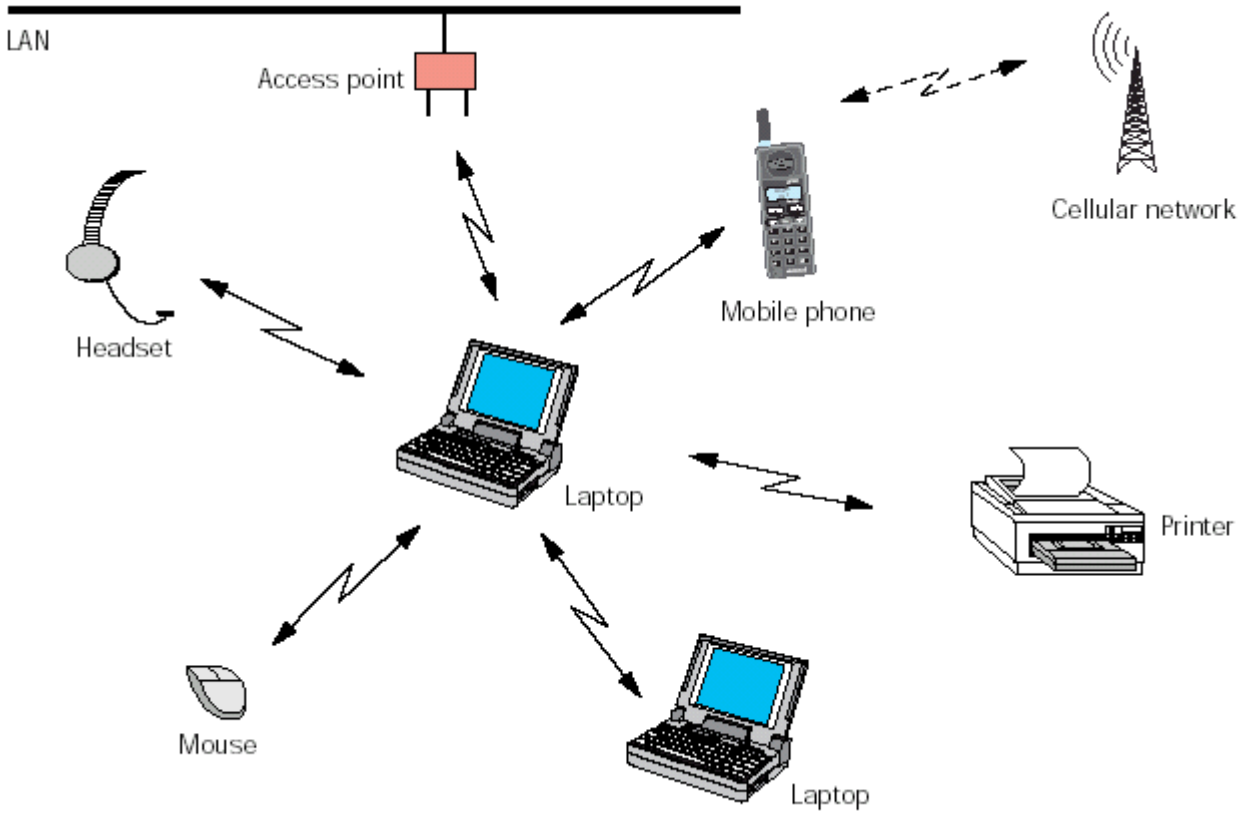
- **ACL (***Asynchronous connection-oriented***)**, assíncrono orientado a conexão que fornece um serviço confiável de transporte como detecção e correção de erros.
- **ASB (***Active Slave Broadcast***)**, sem conexão utilizado para o broadcast de dados para os dispositivos escravos.

Após quase 20 anos de desenvolvimento o Bluetooth apresenta uma especificação consolidada e fornecedores de CI que possibilitaram uma massificação desta solução.

As principais aplicações disponíveis hoje para o Bluetooth são destinadas a celulares, *smartphone*, *tablets* e computadores, permitindo a comunicação entre eles e seus periféricos, como *mouses*, teclados, e impressoras, entre outros. Existem inclusive pequenos dispositivos como adaptadores USB/Bluetooth facilitam a conexão Bluetooth com computadores.

Outras áreas da indústria estão adotando também o Bluetooth: Eletro-Eletrônicos (*Consumer Electronics*), Saúde e Bem-estar (*Health and Wellness*), Esporte e *Fitness* (*Sports and Fitness*), e Casas Inteligentes (*Smart Homes*).

Ainda podemos dizer que um exemplo comum de aplicação do Bluetooth são os fones de ouvido (*Headset*), que podem ser utilizados para ouvir vários dispositivos, tais como o celular, a TV ou o rádio.



Interação do Bluetooth com outras redes

A Convergência das Redes de Comunicação

Desde a criação do telégrafo nos anos 1830, a cada nova mídia de comunicação adotada foi criada uma rede distinta para torná-la disponível a seus usuários. Sucessivamente tivemos o telefone, o telex, a comunicação de dados e a TV a cabo, cada acompanhado por sua própria rede de serviços.

Hoje é comum o usuário final possuir conexões separadas às redes de telefonia, de dados e de TV a cabo.

Quando se fala da convergência na área de telecomunicações, se refere à redução para uma única conexão de rede, fornecendo todos os serviços, com consequente economia de escala.

A convergência é um tema discutido desde os anos 80, quando foi reconhecida pela primeira vez a importância crescente da comunicação entre computadores. Com a digitalização da rede de telefonia, a voz passou a ser transmitida como dados entre as centrais telefônicas mantendo-se, porém, a rede de terminais analógicos para os usuários finais.

Nessa época já foi defendida a extensão do canal de voz digital até o usuário final, substituindo seu antigo telefone analógico por um aparelho digital. Foi proposta a criação da Rede Digital de Serviço Integrado (RDSI, em inglês ISDN), que levaria ao usuário uma única conexão (digital), podendo ser usada indistintamente para voz (telefonia) e comunicação de dados em até 128 kbps. Quando foi proposto, esse serviço seria revolucionário, pois os modems usados na época eram tipicamente de 2400 bits/s.

Porém, ele demorou muito para chegar. No Brasil, somente passou a ser oferecido ao público no final dos anos 90, quando já existiam modems de 56 kbps, e alternativas ainda mais rápidas.

A segunda tentativa de promover a convergência veio ainda nos anos 80, associada à introdução de fibras óticas e serviços de faixa larga.

A fibra ótica possui uma capacidade de transmissão digital tão grande que abriu a possibilidade de enviar por cabo novos serviços antes impraticáveis, tais como televisão.

Na perspectiva de realizar um novo nível de integração entre as redes de comunicação, foi lançada a proposta de RDSI de Faixa Larga (RDSI-FL), baseada em Asynchronous Transmission Mode (ATM). Nesta proposta, seria criada uma rede mundial ATM, à qual todos os computadores estariam ligados, e através de uma única conexão seria realizado acesso a serviços de telefonia, televisão e dados. Para dar suporte à transmissão de voz e vídeo, o ATM previu suporte diferenciado para diferentes tipos de serviço, de qualidades e prioridades distintas.

Embora o ATM hoje seja muito usado nos backbones das grandes redes de dados, não se espera para ele uma sobrevida longa. O que teria lhe sido fatal foi a concorrência com outras tecnologias de rede, especialmente a Ethernet, que permite interligar computadores em rede local por um preço muito menor que o ATM.

Sem interligar diretamente as centenas de milhões de computadores das grandes redes, o ATM passou a ser apenas mais uma tecnologia de rede, entre várias, e requerendo ainda uma tecnologia de inter-redes, tal como o TCP/IP da Internet para comunicação fim-a-fim.

Hoje se acredita que a convergência entre as redes de serviços deva ser realizada através do TCP/IP, estendido para tratar prioritariamente aplicações como voz e vídeo.

A extensão mais promissora se chama *Serviços Diferenciados*, que permite uma classificação simples de aplicações, de acordo com seu grau de urgência ou importância, ou com o preço cobrado para sua transmissão. Nesta visão, a Internet deverá deixar de ser uma rede onde todos os usuários são tratados de forma igual.

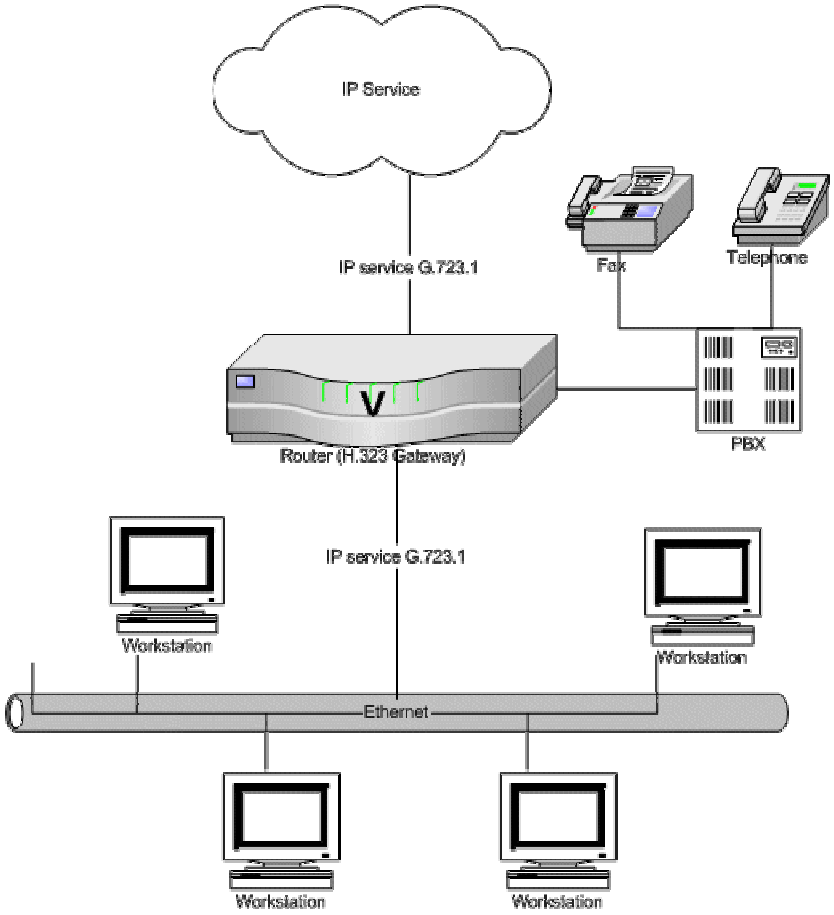
Será este o preço a pagar para se tornar a rede única para todos os serviços diferentes.

Devem aparecer novos serviços, talvez principalmente de entretenimento, pelos quais deva se pagar um preço maior do que pelo serviço tradicional de hoje.

Essa visão do futuro já está se evidenciando em nível mundial através das fusões entre empresas operadoras de serviços de telecomunicações (telefonia e TV a cabo), e entre fabricantes de equipamentos.

Entre fabricantes de telefonia, há uma corrida generalizada para a tecnologia TCP/IP de comunicação de dados, geralmente através da aquisição de empresas especializadas. A primeira conseqüência foi o lançamento acelerado de equipamentos de telefonia IP, termo que caracteriza a comunicação por voz, com qualidade e recursos da telefonia, usando redes de dados para sua transmissão.

Enfim, parece que a tecnologia vai permitir realizar a sonhada convergência para uma rede única.
Porém isto só deve trazer benefícios para o usuário final, se ele tiver a liberdade de escolher quem será seu provedor destes serviços integrados.



Exemplo de rede convergente: VoIP

O exemplo mais simples da convergência de serviços em redes de comunicação é o VoIP (voz sobre IP) que, com a utilização de infraestrutura única há menor custo de implantação e manutenção com facilidade de ampliação dos serviços oferecidos.

Redes NGN

Next Generation Networking (**NGN**) é um termo amplo para descrever algumas importantes evoluções arquiteturais em redes de telecomunicações que serão implantadas nos próximos 5-10 anos. A idéia geral de NGN é que uma mesma rede transporte todas as informações e serviços (voz, dados e todos os tipos de mídias como o vídeo), encapsulando-os em pacotes tal como é feito o tráfego de dados na Internet. NGNs são geralmente construídas com base no protocolo IP.

O NGN é um conceito e não uma tecnologia. É a construção inteligente de uma plataforma multi serviços em cima de uma rede IP. Com esta alteração a convergência de mídia se torna muito mais forte, sendo que uma mesma rede transporta voz, vídeo e dados. O conceito de NGN permite que as operadoras de telefonia administrem melhor sua rede, pois as ativações e desativações de serviços passam a ser lógicos e não mais físicos.

Com a modificação dos meios físicos, permitindo cada vez um número maior de informações pelo mesmo meio, a possibilidade de serviços convergentes em uma rede se torna cada vez mais real. Poderemos ver chegar no mesmo ponto conexão para internet, sinal para TV Digital, Voz, Videoconferência, entre outros.

Com os sistemas integrados e a rede inteligente, as grandes operadoras poderão oferecer serviços mais baratos e com qualidade, sem perder dinheiro. Assim surgirá uma gama de serviços novos e inimagináveis. Poderemos ver e controlar televisões, geladeiras, iluminação, etc., de maneira online sem custos astronômicos para isto.

Assim, as Redes NGN são redes que integram todos os serviços das redes modernas podendo transmitir Voz sobre IP através de diversos protocolos como o SIP, MGCP ou MEGACO além de outros serviços.

Como exemplos de equipamentos uma rede NGN, partindo da visão de operadora de telefonia, temos o *Softswitch* e o *Media Gateway*.

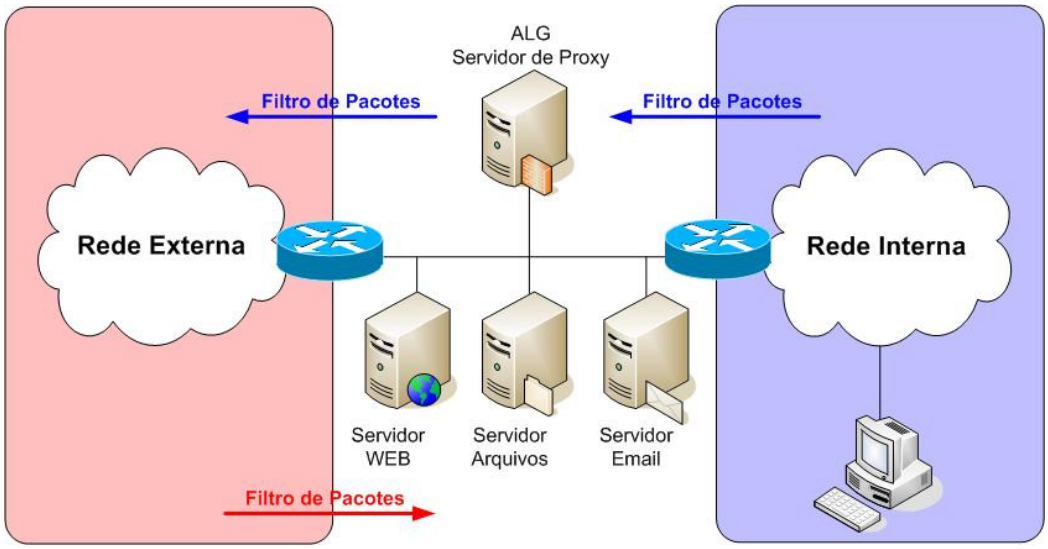
O *Softswitch* nada mais é que um *Switch* (comutador - a central que faz comutação telefônica), mas em forma de software. Como vantagem de usar um *softswitch* em relação a uma central telefônica convencional temos os serviços oferecidos como o VoIP, além do custo (muito menor que uma central), menor tamanho (ocupam alguns racks ao invés de alguns andares), maior capacidade, desenvolvimento mais rápido e mais flexível.

Media Gateway, tem a função de traduzir os protocolos de uma linguagem a outra, de uma rede a outra. Conversa o mundo IP (por exemplo, os protocolos de voz sobre IP como SIP) e as redes tradicionais (por exemplo, PCM-E1). Neste caso um media gateway converte a voz que vem dos canais PCM-E1 para pacotes IP.

Exemplo de hardware Media Gateway – G700 da Waycom:
interconecta redes TDM (GSM/EDGE) e redes IP

A Zona Desmilitarizada DMZ

Uma DMZ fica localizada entre uma rede interna e uma rede externa:



Com a finalidade de prover uma camada adicional de segurança os engenheiros de redes desenvolveram um conceito denominado "*screened subnet based on creating a buffer network*", uma pequena rede com filtros e *cache* localizada entre duas zonas de segurança conhecida como *DMZ* (Zona Desmilitarizada).

Normalmente administradores de redes não permitem que qualquer tráfego passe diretamente através de uma DMZ.

Uma DMZ pode ser implementada com fitros de rede configurados nas suas bordas, estes filtros são responsáveis por realizar o controle de acesso do que entra e do que sai da DMZ e podem ser do tipo *packet filtering*, *stateful packet filtering* e de *cache* como servidores de *proxy* conhecidos como *ALGs* (*Application Layer Gateway*).

O ***Packet filtering*** limita o tráfego dentro da rede baseado no destino e na origem de endereços IPs, portas e outras flags que podem ser utilizadas na implementação das regras de filtro.

O ***Stateful packet filtering*** filtra o tráfego baseado no destino e na origem dos endereços IPs, portas, flags além de realizar "*stateful inspection*" uma inspeção de pacotes que permite o armazenamento de dados de cada conexão em uma tabela de sessão. Esta tabela armazena o estado do fluxo de pacotes e serve como ponto de referência para determinar se os pacotes pertencem a uma conexão existente ou se são pacotes de uma fonte não autorizada.

As ***ALGs*** funcionam no nível da aplicação e interceptam e estabelecem conexões dos hosts da rede interna com a rede externa, autorizando ou não a conexão.

As DMZs podem possuir a capacidade de conter um ataque e limitar os danos na rede. Uma das arquiteturas mais utilizadas são as DMZs que utilizam uma solução de defesa em camadas.
As multiplas camadas de segurança que uma DMZ ofereçe são distribuidas entre pontos de serviços e de filtragem:

- Os pontos de filtragem inicialmente servem para proteger os serviços. Se os serviços da rede são comprometidos, a capacidade de um ataque prosseguir fica limitado. Tanto o tráfego que entra e sai da DMZ é filtrado, seja por roteadores ou por meio de firewalls;

- Os servidores públicos que ficam localizados na DMZ exigem medidas de segurança adequadas. Os serviços são duramente protegidos, aumentando a dificuldade de um invasor comprometer os serviços disponíveis dentro do perímetro da DMZ;

- As ALGs (servidores de proxy) localizados em uma DMZ, servem como intermediários entre os hosts da rede interna e as redes externas como à Internet. É possível impor restrições de acesso com base no horário, login, endereço IP entre outros. Uma ALG serve também como cache de rede, armazenando as informações de páginas e arquivos já acessados.

- Quando um ataque consegue entrar na DMZ, o ataque não é capaz de passar para a rede interna devido aos pontos de filtragem que oferecem uma defesa adicional. A implementação de funcionalidades tais como VLANs podem ajudar a combater estes ataques.

Para implementar uma DMZ podemos utilizar diversos tipos de dispositivos, sendo que o nível de segurança pode ser variado dependendo das funcionalidades disponíveis em cada dispositivo.

Em roteadores SOHO (*Small Office / Home Office*) é possível criar uma DMZ rapidamente, porém este tipo de DMZ somente libera o acesso de um dispositivo da rede interna para a rede externa sem adicionar funciolalidades avançadas de segurança.

Para uma DMZ que utilize multiplas camadas de segurança, precisamos reunir diversas funcionalidades como *packet filtering*, *stateful packet filtering* e um servidor de *proxy*.

Quanto aos equipamentos para implementação de uma DMZ, podemos utilizar roteadores com sistema operacional que permita funções avançadas de segurança, *appliances* de segurança específicos ou servidores *linux*.

Características de uma DMZ:

- A DMZ acomoda servidores que precisam ser acessados externamente;
- As DMZs são estabelecidas entre duas zonas de segurança;
- Em uma DMZ pode-se posicionar dispositivos para realizarem um *cache* de rede;
- As DMZs realizam o controle do tráfego do que entra e do que sai da rede;
- A DMZ pode conter um ataque sem que o mesmo passe para a rede interna.

Esgotamento do IPv4

Para melhor compreensão do esgotamento do endereçamento IPv4, precisamos rever alguns conceitos e sua evolução.

As especificações do IPv4 reservam 32 bits para endereçamento que possibilitam gerar mais de 4 bilhões de endereços distintos. Inicialmente, estes endereços foram divididos em três classes de tamanhos fixos, como mostra a tabela:

Classe	Formato	Redes	Hosts
A	7 bits Rede, 24 bits Host	126	16.777.214
B	14 bits Rede, 16 bits Host	16.384	66.534
C	21 bits Rede, 8 bits Host	2.097.152	254

Diante do provável esgotamento dos endereços IP, a IETF (*Internet Engineering Task Force*) passou a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento. Em novembro de 1991 foi formado o grupo de trabalho ROAD (*Routing and Addressing*), que apresentou como solução a estes problemas, a utilização do CIDR (*Classless Inter-domain Routing*). Definido na RFC 4632 (tornou obsoleta a RFC 1519), o CIDR tem como idéia básica o fim do uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado a real necessidade de cada rede; e a agregação de rotas, reduzindo o tamanho da tabela de roteamento.

Outra solução, apresentada na RFC 2131 (tornou obsoleta a RFC 1541), foi o protocolo DHCP (*Dynamic Host Configuration Protocol*).

A NAT (*Network Address Translation*) foi outra técnica desenvolvida para resolver o problema do esgotamento dos endereços IPv4. Definida na RFC 3022 (tornou obsoleta a RFC 1631) tem como

objetivo básico permitir que, com um único endereço IP, ou um pequeno número deles, vários hosts possam trafegar na Internet. Dentro de uma rede, cada computador recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno. No entanto, quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.

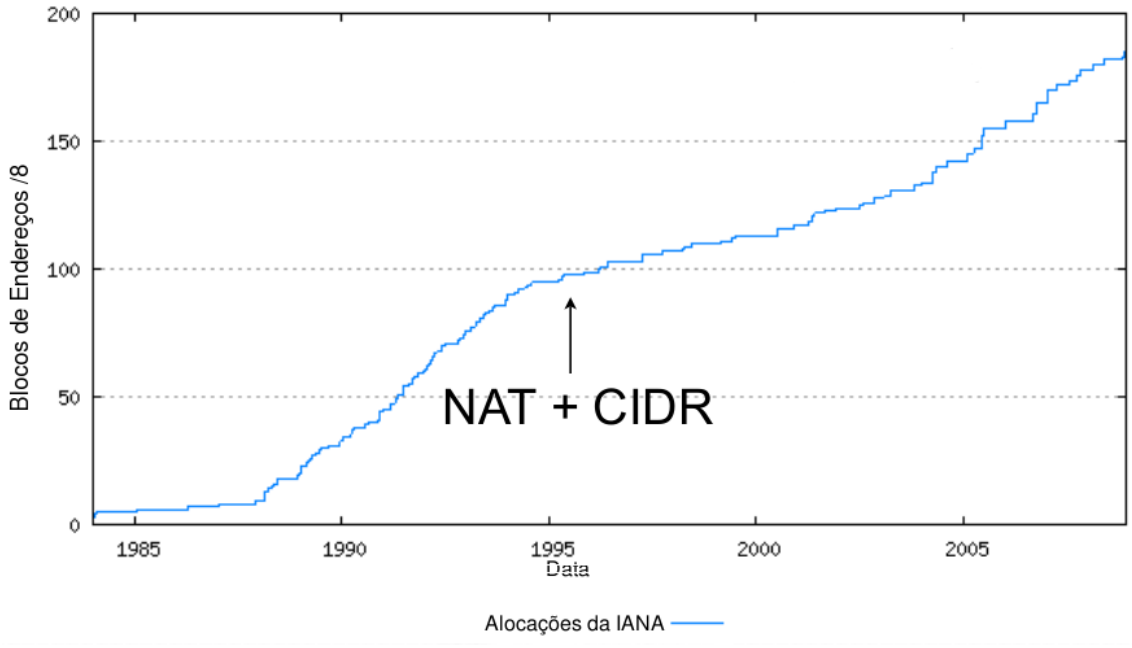
Para tornar possível este esquema, utiliza-se os três intervalos de endereços IP declarados como privados na RFC 1918, sendo que a única regra de utilização, é que nenhum pacote contendo estes endereços pode trafegar na Internet pública. As três faixas reservadas são:

- 10.0.0.0 a 10.255.255.255 /8 (16.777.216 hosts)
- 172.16.0.0 a 172.31.255.255 /12 (1.048.576 hosts)
- 192.168.0.0 a 192.168.255.255 /16 (65.536 hosts)

A utilização da NAT mostrou-se eficiente no que diz respeito a economia de endereços IP, além de apresentar alguns outros aspectos positivos, como facilitar a numeração interna das redes, ocultar a topologia das redes e só permitir a entrada de pacotes gerados em resposta a um pedido da rede. No entanto, o uso da NAT apresenta inconvenientes que não compensam as vantagens oferecidas.

A NAT quebra o modelo fim-a-fim da Internet, não permitindo conexões diretas entre dois hosts, o que dificulta o funcionamento de uma série de aplicações, como P2P, VoIP e VPNs. Outro problema é a baixa escalabilidade, pois o número de conexões simultâneas é limitado, além de exigir um grande poder de processamento do dispositivo tradutor. O uso da NAT também impossibilita rastrear o caminho do pacote (através de ferramentas como traceroute, por exemplo) e dificulta a utilização de algumas técnicas de segurança como IPSec. Além disso, seu uso passa uma falsa sensação de segurança, pois, apesar de não permitir a entrada de pacotes não autorizados, a NAT não realiza nenhum tipo de filtragem ou verificação nos pacotes que passa por ela.

A figura seguinte mostra o quanto essas medidas ajudaram a diminuir o aumento da alocação de endereço:



Embora estas soluções tenham diminuído a demanda por IPs, elas não foram suficientes para resolver os problemas decorrentes do crescimento da Internet. A adoção dessas técnicas reduziu em apenas 14% a quantidade de blocos de endereços solicitados à IANA e a curva de crescimento da Internet continuava apresentando um aumento exponencial. Essas medidas, na verdade, serviram para que houvesse mais tempo para se desenvolver uma nova versão do IP, que fosse baseada nos princípios que fizeram o sucesso do IPv4, porém, que fosse capaz de suprir as falhas apresentadas por ele.

Em dezembro de 1993 a IETF formalizou, através da RFC 1550, as pesquisas a respeito da nova versão do protocolo IP, solicitando o envio de projetos e propostas para o novo protocolo. Esta foi umas das primeiras ações do grupo de trabalho da IETF denominado *Internet Protocol next generation* (IPng). As principais questões que deveriam ser abordadas na elaboração da próxima versão do protocolo IP foram:

- Escalabilidade;
- Segurança;
- Configuração e administração de rede;
- Suporte a QoS;
- Mobilidade;
- Políticas de roteamento;
- Transição.

Diversos projetos começaram a estudar os efeitos do crescimento da Internet, sendo os principais o CNAT, o IP Encaps, o Nimrod e o Simple CLNP. Destas propostas surgiram o TCP and UDP with Bigger Addresses (TUBA), que foi uma evolução do Simple CLNP, e o IP Address Encapsulation (IPAE), uma evolução do IP Encaps. Alguns meses depois foram apresentados os projetos Paul's Internet Protocol (PIP), o Simple Internet Protocol (SIP) e o TP/IX. Uma nova versão do SIP, que englobava algumas funcionalidades do IPAE, foi apresentada pouco antes de agregar-se ao PIP, resultando no Simple Internet Protocol Plus (SIPP). No mesmo período, o TP/IX mudou seu nome para Common Architecture for the Internet (CATNIP).

Em janeiro de 1995, na RFC 1752 o IPng apresentou um resumo das avaliações das três principais propostas:

- CATNIP – foi concebido como um protocolo de convergência, para permitir a qualquer protocolo da camada de transporte ser executado sobre qualquer protocolo de camada de rede, criando um ambiente comum entre os protocolos da Internet, OSI e Novell;
- TUBA – sua proposta era de aumentar o espaço para endereçamento do IPv4 e torná-lo mais hierárquico, buscando evitar a necessidade de se alterar os protocolos da camada de transporte e aplicação. Pretendia uma migração simples e em longo prazo, baseada na atualização dos host e servidores DNS, entretanto, sem a necessidade de encapsulamento ou tradução de pacotes, ou mapeamento de endereços;
- SIPP – concebido para ser uma etapa evolutiva do IPv4, sem mudanças radicais e mantendo a interoperabilidade com a versão 4 do protocolo IP, fornecia uma plataforma para novas funcionalidades da Internet, aumentava o espaço para endereçamento de 32 bits para 64 bits, apresentava um nível maior de hierarquia e era composto por um mecanismo que permitia "alargar o endereço" chamado *cluster addresses*. Já possuía cabeçalhos de extensão e um campo *flow* para identificar o tipo de fluxo de cada pacote.

Entretanto, conforme relatado também na RFC 1752, todas as três propostas apresentavam problemas significativos. Deste modo, a recomendação final para o novo Protocolo Internet baseou-se em uma versão revisada do SIPP, que passou a incorporar endereços de 128 bits, juntamente com os elementos de transição e auto configuração do TUBA, o endereçamento baseado no CIDR e os cabeçalhos de extensão. O CATNIP, por ser considerado muito incompleto, foi descartado.

Após esta definição, a nova versão do Protocolo Internet passou a ser chamado oficialmente de IPv6.

IPv6

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter:

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 \text{ endereços}$$

Este valor representa aproximadamente 79 octilhões ($7{,}9\times10^{28}$) de vezes a quantidade de endereços IPv4 e representa, também, mais de 56 octilhões ($5{,}6\times10^{28}$) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes.

A representação dos endereços IPv6, divide o endereço em oito grupos de 16 bits, separando-os por ":", escritos com dígitos hexadecimais (0-F). Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos. Além disso, regras de abreviação podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos. É permitido omitir os zeros a esquerda de cada bloco de 16 bits, além de substituir uma sequência longa de zeros por "::".

Por exemplo, o endereço: 2001:0DB8:0000:0000:130F:0000:0000:140B
pode ser escrito como: 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B

Neste exemplo é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço.

Se o endereço acima fosse escrito como 2001:DB8::130F::140B, não seria possível determinar se ele corresponde:

a 2001:DB8:0:0:130F:0:0:140B,
a 2001:DB8:0:0:0:130F:0:140B
ou 2001:DB8:0:130F:0:0:0:140B.

Esta abreviação pode ser feita também no fim ou no início do endereço, como ocorre em 2001:DB8:0:54:0:0:0:0 que pode ser escrito da forma 2001:DB8:0:54::.

Outra representação importante é a dos prefixos de rede. Em endereços IPv6 ela continua sendo escrita do mesmo modo que no IPv4, utilizando a notação CIDR.

O exemplo de prefixo de sub-rede apresentado a seguir indica que dos 128 bits do endereço, 64 bits são utilizados para identificar a sub-rede.

Prefixo 2001:db8:3003:2::/64
Prefixo global 2001:db8::/32
ID da sub-rede 3003:2

Esta representação também possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes.

Com relação à representação dos endereços IPv6 em URLs (*Uniform Resource Locators*), estes agora passam a ser representados entre colchetes, de modo a não haver ambiguidades caso seja necessário indicar o número de uma porta juntamente com a URL. Observe os exemplos a seguir:

http://[2001:12ff:0:4::22]/index.html
http://[2001:12ff:0:4::22]:8080

Tipos de Endereços IPv6

Existem no IPv6 três tipos de endereços definidos:

- **Unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface;
- **Anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço *anycast* é utilizado em comunicações de *um-para-um-de-muitos*.
- **Multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de *um-para-muitos*.

Diferente do IPv4, no IPv6 não existe endereço *broadcast*, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída à tipos específicos de endereços *multicast*.

Endereços Unicast
Os endereços *unicast* são utilizados para comunicação entre dois nós. Exemplos: telefones VoIPv6; computadores em uma rede privada; etc. Sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4.

Os endereços *unicast* IPv6 são divididos em: *Global Unicast*; *Unique-Local*; e *Link-Local*. Existem também alguns tipos para usos especiais, como endereços IPv4 mapeados em IPv6, endereço de *loopback* e o endereço não-especificado, entre outros.

- **Global Unicast** – equivalente aos endereços públicos IPv4, o endereço global unicast é globalmente roteável e acessível na Internet IPv6. Ele é constituído por três partes: o prefixo de roteamento global, utilizado para identificar o tamanho do bloco atribuído a uma rede; a identificação da sub-rede, utilizada para identificar um enlace em uma rede; e a identificação da interface, que deve identificar de forma única uma interface dentro de um enlace. Sua estrutura foi projetada para utilizar os 64 bits mais a esquerda para identificação da rede e os 64 bits mais a direita para identificação da interface. Assim, exceto casos específicos, todas

as sub-redes em IPv6 tem o mesmo tamanho de prefixo, 64 bits (/64), o que possibilita 2^{64} = 18.446.744.073.709.551.616 dispositivos por sub-rede.
Atualmente, está reservada para atribuição de endereços a faixa 2000::/3 (001), que corresponde aos endereços de **2000::** a **3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff**. Isto representa 13% do total de endereços possíveis com IPv6, o que nos permite criar 2^{64-3} = 2.305.843.009.213.693.952 ($2{,}3\times10^{18}$) sub-redes (/64) diferentes ou 2^{48-3} = 35.184.372.088.832 ($3{,}5\times10^{13}$) redes /48.

- **Link Local** – pode ser usado apenas no enlace específico onde a interface está conectada. O endereço *link local* é atribuído automaticamente utilizando o prefixo FE80::/64. Os 64 bits reservados para a identificação da interface são configurados utilizando o formato *IEEE EUI-64*. Vale ressaltar que os roteadores não devem encaminhar pacotes que possuam como origem ou destino um endereço link-local para outros enlaces.
- **Unique Local Address (ULA)** – endereço com grande probabilidade de ser globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces. Um endereço ULA não deve ser roteável na Internet global. Um endereço ULA, criado utilizado um ID global alocado pseudo-randomicamente, é composto das seguintes partes:
    - **Prefixo:** FC00::/7.
    - **Flag Local (L):** se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central (ainda a definir).
    - **Identificador global:** identificador de 40 bits usado para criar um prefixo globalmente único.
    - **Identificador da Interface:** identificador da interface de 64 bits.

  Deste modo, a estrutura de um endereço ULA é **FDUU:UUUU:UUUU::** onde U são os bits do identificador único, gerado aleatoriamente por um algoritmo específico. Sua utilização permite que qualquer enlace possua um prefixo /48 privado e único globalmente. Deste modo, caso duas redes, de empresas distintas, por exemplo, sejam interconectadas, provavelmente não haverá conflito de endereços ou necessidade de renumerar a interface que o esteja usando. Além disso, o endereço ULA é independente de provedor, podendo ser utilizado na comunicação dentro do enlace mesmo que não haja uma conexão com a Internet. Outra vantagem, é que seu prefixo pode ser facilmente bloqueado, e caso um endereço ULA seja anunciado acidentalmente para fora do enlace, através de um roteador ou via DNS, não haverá conflito com outros endereços.

Endereços Anycast

Um endereço IPv6 *anycast* é utilizado para identificar um grupo de interfaces, porém, com a propriedade de que um pacote enviado a um endereço *anycast* é encaminhado apenas a interface do grupo mais próxima da origem do pacote.

Os endereços *anycast* são atribuídos a partir da faixa de endereços *unicast* e não há diferenças sintáticas entre eles. Portanto, um endereço *unicast* atribuído a mais de uma interface transforma-se em um endereço *anycast*, devendo-se neste caso, configurar explicitamente os nós para que saibam que lhes foi atribuído um endereço *anycast*. Além disso, este endereço deve ser configurado nos roteadores como uma entrada separada (prefixo /128 – *host route*).

Este esquema de endereçamento pode ser utilizado para descobrir serviços na rede, como servidores DNS e *proxies* HTTP, garantindo a redundância desses serviços. Também se pode utilizar para fazer balanceamento de carga em situações onde múltiplos hosts ou roteadores provem o mesmo serviço, para localizar roteadores que forneçam acesso a uma determinada sub-rede ou para localizar os Agentes de Origem em redes com suporte a mobilidade IPv6.

Todos os roteadores devem ter suporte ao endereço *anycast Subnet-Router*. Este tipo de endereço é formado pelo prefixo da sub-rede e pelo IID preenchido com zeros (ex.: 2001:db8:cafe:dad0::/64). Um pacote enviado para o endereço *Subnet-Router* será entregue para o roteador mais próximo da origem dentro da mesma sub-rede.

Também foi definido um endereço *anycast* para ser utilizado no suporte a mobilidade IPv6. Este tipo de endereço é formado pelo prefixo da sub-rede seguido pelo IID **dfff:ffff:ffff:fffe** (ex.: **2001:db8::dfff:ffff:ffff:fffe**). Ele é utilizado pelo Nó Móvel, quando este precisar localizar um Agente Origem em sua Rede Original.

Endereços Multicast

Endereços *multicast* são utilizados para identificar grupos de interfaces, sendo que cada interface pode pertencer a mais de um grupo. Os pacotes enviados para esses endereços são entregues a todos as interfaces que compõe o grupo.

No IPv4, o suporte a *multicast* é opcional, já que foi introduzido apenas como uma extensão ao protocolo. Entretanto, no IPv6 é requerido que todos os nós suportem *multicast*, visto que muitas funcionalidades da nova versão do protocolo IP utilizam esse tipo de endereço.

Seu funcionamento é similar ao do *broadcast*, dado que um único pacote é enviado a vários hosts, diferenciando-se apenas pelo fato de que no *broadcast* o pacote é enviado a todos os hosts da rede, sem exceção, enquanto que no *multicast* apenas um grupo de hosts receberá esse pacote. Deste modo, a possibilidade de transportar apenas uma cópia dos dados a todos os elementos do grupo, a partir de uma árvore de distribuição, pode reduzir a utilização de recurso de uma rede, bem como otimizar a entrega de dados aos hosts receptores.

Aplicações como videoconferência, distribuição de vídeo sob demanda, atualizações de softwares e jogos on-line, são exemplos de serviços que vêm ganhando notoriedade e podem utilizar as vantagens apresentadas pelo *multicast*.

Os endereços *multicast* não devem ser utilizados como endereço de origem de um pacote. Esses endereços derivam do bloco **FF00::/8**, onde o prefixo **FF**, que identifica um endereço *multicast*, é precedido por quatro bits, que representam quatro *flags*, e um valor de quatro bits que define o escopo do grupo *multicast*. Os 112 bits restantes são utilizados para identificar o grupo *multicast*.

Endereços IPv6 Especiais

Existem alguns endereços IPv6 especiais utilizados para fins específicos:

- **Endereço Não-Especificado (Unspecified):** é representado pelo endereço **0:0:0:0:0:0:0:0** ou **::0** (equivalente ao endereço IPv4 unspecified **0.0.0.0**). Ele nunca deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço. Ele pode, por exemplo, ser utilizado no campo Endereço de Origem de um pacote IPv6 enviado por um host durante o processo de inicialização, antes que este tenha seu endereço exclusivo determinado. O endereço unspecified não deve ser utilizado como endereço de destino de pacotes IPv6;
- **Endereço Loopback:** representado pelo endereço unicast **0:0:0:0:0:0:0:1** ou **::1**(equivalente ao endereço IPv4 *loopback* **127.0.0.1**). Este endereço é utilizado para referenciar a própria máquina, sendo muito utilizado para testes internos. Este tipo de endereço não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nós. Além disso, um pacote IPv6 com um endereço *loopback* como destino não pode ser enviado por um roteador IPv6, e caso um pacote recebido em uma interface possua um endereço *loopback* como destino, este deve ser descartado;

- **Endereços IPv4-mapeado:** representado por **0:0:0:0:0:FFFF:wxyz** ou **::FFFF:wxyz**, é usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde **wxyz** representa os 32 bits do endereço IPv4, utilizando dígitos decimais. É aplicado em técnicas de transição para que nós IPv6 e IPv4 se comuniquem. Ex.**::FFFF:192.168.100.1.**

Algumas faixas de endereços também são reservadas para uso específicos:

- **2002::/16:** prefixo utilizado no mecanismo de transição 6to4;
- **2001:db8::/32:** prefixo utilizado para representar endereços IPv6 em textos e documentações.
- **2001:0000::/32:** prefixo utilizado no mecanismo de transição TEREDO;
  - Teredo é um mecanismo desenvolvido pela Microsoft que permite conectividade IPv6 para hosts com endereços IPv4 mesmo que estejam conectados na Internet por meio de NAT. Esta técnica realiza o encapsulando datagramas IPv6 dentro de pacotes IPv4 utilizando UDP (*User Datagram Protocol*).
    Para estabelecer um túnel Teredo é preciso que uma estação de trabalho se conecte a um servidor Teredo que irá fornecer um endereço IPv6 e determinar qual o tipo de NAT que está sendo utilizado na conexão. Os endereços Teredo iniciam com o prefixo 2001:0::/32.
    Após definido o endereço IPv6 da estação de trabalho, o servidor Teredo estabelecerá uma conexão inicial com o host IPv6 de destino, este host manterá a conexão com a estação de trabalho de origem através de um *Relay* Teredo mais próximo.

Outros endereços, utilizados no início do desenvolvimento do IPv6 tornaram-se obsoletos e não devem mais ser utilizados:

- **FEC0::/10:** prefixo utilizado pelos endereços do tipo *site local*, desenvolvidos para serem utilizados dentro de uma rede específica sem a necessidade de um prefixo global, equivalente aos endereços privados do IPv4. Sua utilização foi substituída pelos endereços ULA;
- **::wxyz:** utilizado para representar o endereço IPv4-compatível. Sua função é a mesma do endereço IPv4-mapeado, tornando-se obsoleto por desuso;
- **3FFE::/16:** prefixo utilizado para representar os endereços da rede de teste *6Bone*. Criada para ajudar na implantação do IPv6, está rede foi desativada em 6 de junho de 2006 (06/06/06).

Políticas de alocação e designação

Na hierarquia das políticas de atribuição, alocação e designação de endereços, cada RIR (*Regional Internet Registry*) recebe da IANA um bloco /12 IPv6.

O bloco **2800::/12** corresponde ao espaço reservado para o LACNIC alocar na América Latina. O NIC.br por sua vez, trabalha com um /16 que faz parte deste /12.

A alocação mínima para ISPs (*Internet Service Provider*) é um bloco /32, no entanto, alocações maiores podem ser feitas mediante apresentação de justificativa de utilização. Um aspecto importante que merece destaque é que diferente do IPv4, com IPv6 a utilização é medida em relação ao número de designações de blocos de endereços para usuários finais, e não em relação ao número de endereços designados aos usuários finais.

O NIC.br recomenda utilizar:

- **/64 a /56 para usuários domésticos:** Para usuários móveis pode-se utilizar /64, pois normalmente apenas uma rede é suficiente. Para usuários residenciais recomenda-se redes maiores. Se o provedor optar por, num primeiro momento, oferecer apenas /64 para usuários residenciais, ainda assim recomenda-se que no plano de numeração se reserve um /56.
- **/48 para usuários corporativos.** Empresas muito grande podem receber mais de um bloco /48.

Para planejar a rede é preciso considerar que para cada rede física ou VLAN com IPv6 é preciso reservar um /64. Esse é o tamanho padrão e algumas funcionalidades, como a autoconfiguração dependem dele. É preciso considerar também a necessidade de expansão futura, assim como a necessidade de agregação nos protocolos de roteamento.

Concluindo

Mesmo com todos os benefícios, a transição dos protocolos IPv4 para o IPv6 apresenta algumas dificuldades, como o tamanho do endereço que passou de 32bits para 128 bits.

De imediato percebemos que isso torna muito difícil que se decore algum endereço. As empresas terão que atualizar seus equipamentos de redes e os técnicos terão que se atualizar para que continuem dando suporte. Mesmo assim já começa a existir uma necessidade de que a Internet adote o IPv6 pois o IPv4 mostra limitações para suprir os serviços de multimídia, videoconferência, telefonia-ip e transmissões de TV.

A utilização por definitivo do IPv6 ainda deve demorar muitos anos. Alguns estudos apontam para o final da próxima década. Por isso é muito importante que empresas e instituições comecem os estudos para a utilização do IPv6 não só para se preparar para a adequação de suas máquinas para o futuro mas também para que busque novos serviços. Até lá, o IPv6 vem surgindo em “bolhas” por todo o mundo.

O IPv4 não será substituído pelo IPv6. As “bolhas IPv6” devem crescer e se tornar maior que a rede IPv4. Os equipamentos IPv4 serão gradualmente desativados por obsolescência. As redes IPv4 serão englobadas pelo IPv6, formando “bolhas IPv4” que tenderão a desaparecer (por obsolescência do IPv4 e gigantismo do IPv6).

O IPv6 já vem habilitado por padrão nos sistemas operacionais modernos, como versões atualizadas de Windows, Linux, MacOS ou BSD. Esta é a forma para novos serviços de comunicação. Para verificar se o sistema operacional em execução está preparado para o IPv6, basta realizar um ping para o *loopback* e analisar sua resposta:

```
C:\Windows\system32>ping ::1

Disparando ::1 com 32 bytes de dados:
Resposta de ::1: tempo<1ms
Resposta de ::1: tempo<1ms
Resposta de ::1: tempo<1ms
Resposta de ::1: tempo<1ms

Estatísticas do Ping para ::1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Windows\system32>_
```

Ataques a Redes

Ataques a computadores são tipos de crimes virtuais que visam, principalmente, roubar informações ou prejudicar computadores alheios. Todo computador em rede está potencialmente suscetível a ataques.

As técnicas mais usadas para invasão são através de e-mails, arquivos compartilhados e páginas da web infectadas. Suas conseqüências são bastante variadas: algumas têm como instrução infectar computadores alheios para, em seguida, danificar seus componentes, seja excluindo arquivos, seja alterando o funcionamento da máquina ou até mesmo deixando o computador vulnerável a outros tipos de ataques. Existem também aqueles que não visam prejudicar a máquina, mas sim, seu usuário, como os softwares que têm como objetivo capturar informações sigilosas, como senhas e números de contas bancárias e cartões de créditos.

Há termos que definem o tipo de script utilizado e sua forma de ação. A seguir, temos listadas as formas mais comuns de termos utilizados em ataques às redes:

- *Malware*: Termo geralmente aplicado a qualquer software desenvolvido para causar danos em computadores. Estão nele incluídos vírus, cavalos-de-tróia e vermes.

- Vírus: Pequenos programas de computador criados para causar danos na máquina infectada, apagando dados, capturando informações ou alterando o funcionamento da máquina. O nome vem da grande semelhança que estes programas têm com os vírus biológicos, pois, depois de infectar um computador, ele se instala em um programa e o usa como hospedeiro para se multiplicar e se disseminar para outros computadores. Podem anexar-se a quase todos os tipos de arquivos. Podem mostrar apenas mensagens ou imagens, sem danificar arquivos da máquina infectada, mas consumindo a capacidade de armazenamento e de memória ou diminuindo o desempenho do computador infectado. Podem também destruir arquivos, reformatar o disco rígido, ou até a destruição total do sistema operacional.

- Vermes (*Worms*): É um programa completo, não precisando de um hospedeiro para entrar em ação, como o vírus. Primeiro, ele controla os recursos que permitem o transporte de arquivos e informações, depois o verme cria cópias e envia para outros computadores. Seu grande perigo é sua enorme capacidade de replicação. Pode ser projetado para fazer muitas coisas, como, por exemplo, excluir arquivos em um sistema, enviar documentos por e-mail ou podem provocar danos apenas com o tráfego de rede, como é o exemplo do verme *Mydoom*, que causou lentidão generalizada na Internet no auge do seu ataque. Podem também trazer embutidos programas que geram algum problema ou que tornam o computador infectado vulnerável a outros ataques. Há

também um tipo de verme, como é o caso do *Sobig*, que abre o computador para ataques via Internet, transformando os computadores infectados em computadores zumbis que são utilizados para enviar e-mail ou para atacar outros computadores. Há também um tipo de verme, o *Doomjuice*, que utiliza as brechas deixadas por outros tipos de vermes, para se espalhar.

- Cavalo de Tróia (*Trojan Horse*): Diferentemente dos vírus e dos vermes, não se duplica. Alguns são programados para se autodestruir após algum tempo ou com algum comando do cliente. A infecção ocorre através de arquivos anexos a e-mails, mensagens instantâneas, downloads, por CDs ou disquetes. O programa é quase sempre uma animação ou imagens pornográficas, mas é durante a exibição dessas imagens que o computador está sendo infectado. São famosos pela facilidade de uso: com ele qualquer pessoa pode controlar o computador de outros, sendo conhecido como "*ferramentas de script kid*". Sua função é abrir o computador para o ataque de um eventual invasor, passando para este o controle da máquina infectada. Os *cavalos de tróia* são divididos em duas partes: o servidor e o cliente. O servidor geralmente fica oculto em algum arquivo, que, quando executado, permite que o servidor seja instalado no computador da vítima, sem que esta saiba. Daí por diante o cliente passa a ter controle do computador infectado.

- Programa espião (*Spyware*): É um programa automático de computador que recolhe informações sobre o usuário e repassa para uma entidade externa na internet que não tem como objetivos a dominação ou a manipulação do sistema do usuário. Seu intuito é permanecer desapercebido no sistema. Ele Pode ser obtido por download de websites, mensagens de e-mail, mensagens instantâneas e conexões diretas para o compartilhamento de arquivos, podendo também estar contidos em vírus. Costumava ser legalmente embutido em software e freeware, sendo removidos quando era feito a compra do software ou de uma versão mais completa e paga.

- *Phishing*: É um golpe on-line de falsificação. Seus criadores geralmente usam falsas páginas de inscrição para serviços comuns da Internet para tentar conduzir o receptor a revelar informações sigilosas e pessoais, como números de contas bancárias, cartões de crédito e senhas. Usam também *spam*, *websites* e mensagens instantâneas com pretextos falsos para fazer com que as supostas vítimas baixem e executem arquivos que permitem o roubo futuro de informações ou o acesso não autorizado.

- *Pharming*: é o termo atribuído ao ataque baseado na técnica *DNS cache poisoning* (envenenamento de *cache DNS*) que consiste em corromper o *DNS* (*Domain Name System*) em uma rede de computadores, fazendo com que a *URL* (*Uniform Resource Locator* - Localizador Uniforme de Recursos) de um *site* passe a apontar para um servidor diferente do original.

- *Spam*: São mensagens de e-mail indesejadas, geralmente, anúncios não solicitados e enviadas em massa. Pode ser usado para transmitir todo tipo de praga eletrônica além de alguns poderem conter links para websites com conteúdo não desejados. Há vários tipos de spam. Um dos mais conhecidos são os chamados *hoaxes*, que são histórias falsas recebidas por e-mails, seus conteúdos podem ser correntes, apelos sentimentais ou religiosos, campanhas ou ainda falsos vírus que ameaçam destruir, infectar ou formatar o disco rígido do computador. Tem como objetivo capturar endereços de e-mail que são passados ou vendidos para *spammers* (pessoas que passam *spams*). Há também as correntes (*chain letters*), mensagens que prometem sorte, riqueza ou algum outro tipo de benefício àqueles que a repassarem para um número mínimo de pessoas em um tempo pré-determinado, e que dizem que aqueles que forem capazes de interromper a corrente sofrerão muitos infortúnios. Outra forma do spam são os chamados golpes ou *scam*, que nada mais são do que golpes que garantem oportunidades de empregos, negócios, empréstimos

facilitados, etc. Com tantos tipos diferentes e modos distintos de persuasão, o spam acaba se tornando um dos mais perigosos tipos de golpes existente na Internet.

- Ataque *DoS* (*Denial of service* - Ataque de negação de serviço): É um tipo de ataque onde se procura vulnerabilidades dos Sistemas Operacionais específicos. São tentativas de impedir usuários legítimos de utilizarem determinado serviço utilizando técnicas que podem sobrecarregar uma rede a tal ponto que seus usuários não consigam mais usá-la, ou derrubar uma conexão entre dois ou mais computadores. É importante frisar que quando um computador/site sofre ataque DoS, ele não é invadido, mas sim, sobrecarregado, independente do sistema operacional utilizado. Uma das formas de ataque mais conhecidas é a *SYN Flooding*, no qual um computador tenta estabelecer conexão com um servidor através de um sinal de solicitação *SYN* (*syncronize*). Estabelecida a conexão o servidor envia ao computador solicitante um sinal *ACK* (*acknowledgement*), o problema é que o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos.

- Ataque *DDoS* (*Distributed Deniel of Service*) é um tipo de ataque *DoS* mais complexo, pois envolve a quebra da segurança de vários computadores conectados a Internet. É um tipo de ataque que, para que seja bem sucedido, é necessária uma grande quantidade de computadores zumbis, podendo ser dezenas, centenas, ou até milhares de máquinas controladas, para então atacar uma determinada vítima. A forma mais comum de fazer isso é através de softwares maliciosos, como os vírus. Após ter acesso às máquinas, o atacante instala o software de *DDoS* que permite a ele controlar essas máquinas para atacar qualquer site. Esses ataques esgotam o *bandwidth* e capacidade de processamento dos roteadores, fazendo a vítima perder a conexão com a Internet enquanto o ataque estiver ocorrendo. Esse tipo de ataque é um dos mais eficazes que existem e já prejudicou sites como os da *CNN*, *Amazon*, *Yahoo*, *Microsoft* e *eBay*.

Porém, os ataques informatizados (*scripts* em redes) não são a única ameaça às redes e informações de um computador. Eles podem sofrer invasões por usuários não autorizados. Mesmo redes/hosts protegidos por *login/password* podem ter seu acesso liberado com ajuda da engenharia social

Social Engineering (Engenharia Social)**:** é um conjunto de técnicas utilizadas para obter informações importantes e sensíveis de uma corporação ou de um indivíduo por meio da enganação, realizada de forma pessoal (*face-to-face*) ou por meio de recursos de tecnológicos. O elemento mais vulnerável de qualquer sistema de segurança é o próprio indivíduo, ao qual possui traços comportamentais e psicológicos que o torna suscetível aos ataques de engenharia social.

As técnicas utilizadas pelos Engenheiros Sociais são diversificadas, entre elas estão: a exploração de confiança das pessoas utilizando da vaidade pessoal, da autoconfiança, da formação profissional, da busca de amizades e persuasão ou utilizando a engenharia social inversa, quando um *cracker* cria uma personalidade e aparece numa posição de autoridade, de modo que os usuários lhe pedirão informação que permite ao *cracker* extrair dos funcionários informações valiosas.

A utilização de meios como *pharming*, *phisching* e *footprint* também são comuns na engenharia social. O envio de emails maliciosos contendo vírus ou softwares como *keyloggers* (software que coletam senhas) ou de emails em nome de uma instituição bancária solicitando uma atualização cadastral fazem parte do *rool* de ações dos Engenheiros Sociais.

- ***Footprint*** é uma técnica de levantamento de dados e informações, que auxiliam a criar um perfil sobre um determinado site. Com este objetivo é possível descobrir falhas que possam ser exploradas e utilizadas por pessoas maliciosas.

Na engenharia social em ambientes corporativos, o exemplo de atuação mais comum é a do norte americano *Kevin Mitnick*, considerado por muitos como o maior *hacker* de todos os tempos. Após sair da prisão, escreveu dois livros: "A Arte de Enganar", no qual descreve técnicas de invasão de redes com histórias fictícias e "A Arte de Invadir", com histórias reais de amigos e *hackers* conhecidos (os dois estão disponíveis no Brasil). Atualmente o ex-hacker é dono de uma consultoria de segurança de sistemas, a *Mitnick Security Consulting*, nos Estados Unidos.