Cabeamento Estruturado

Em instalações internas ou terceirizadas, alguns procedimentos devem ser seguidos à risca pelos técnicos. Um deles se trata da implantação de cabeamento estruturado, que conecta em redes roteadores, impressoras, switches, telefones, estações e servidores, por exemplo.

No post de hoje, iremos detalhar as principais padrões e normas de cabeamento estruturado para instalação desse tipo de estrutura, que utiliza o conector RJ45 e o cabo UTP, a fim de conferir maior organização, segurança, otimização de recursos e fácil gerenciamento à empresa.

O cabeamento estruturado está calcado na disposição de uma rede que permite integração de serviços de dados e voz. Esse tipo de estrutura apresenta facilidade no redirecionamento por caminhos distintos dos sinais em um mesmo complexo (fator importante em estruturas que serão alteradas posteriormente).

Em outras palavras, os sinais de dados, voz e multimídia (triple-play) podem ser transmitidos a partir de um mesmo cabo de uma mesma infraestrutura (tomadas, conectores, painéis).

Ainda que o funcionamento se assemelhe à conexão simples de uma tomada, permitindo a alimentação elétrica de um equipamento independentemente do tipo de aplicação, existem alguns padrões e normas de cabeamento estruturado a serem levados em consideração no momento de implantação da estrutura. A principal padronização é regida pela Telecommunications Industry Association (TIA) e pela Eletronic Industries Alliance (EIA). Há, ainda, recomendações de órgãos funcionais para a otimização do funcionamento de uma estrutura de cabeamento estruturado.

Principais Padrões e Normas de Cabeamento Estruturado

O padrão EIA/TIA-568-B, equivalente à norma brasileira NBR 14.565, por exemplo, categoriza o sistema de cabeamento a partir da largura de banda, comprimento, atenuação e desempenho desse tipo de tecnologia. A norma ISO é outro procedimento que garante a padronização de cabos, conectores e procedimento como um todo. Esses dois padrões ganharam força na década de 90, com a chegada do cabo de par trançado ao ambiente das telecomunicações.

Já a norma ANSI/BICSI 005-2013 dá conta de toda a segurança eletrônica – e espaços de telecom correlatos – da infraestrutura de cabeamento estruturado. As recomendações, que orientam sobre as práticas de instalação (altura de montagem das ferramentas de segurança, por exemplo), análise e gerenciamento de riscos foi inicialmente proposta nos Estados Unidos. No entanto, de acordo com a entrevista publicada no portal Cabling News, há grandes chances de o Brasil em breve exigir cumprimento do padrão.

No início de 2014, a Associação Brasileira de Normas Técnicas (ABNT) também aprovou a primeira norma para instalação de cabeamento estruturado em projetos residenciais, conforme noticiou a revista Home Theater. A NBR 16264 estipula procedimentos recomendados para projetar e instalar redes domésticas, passando a servir de referência para empresas e profissionais desse mercado. Uma característica interessante dessa norma é que ela pode ser utilizada em situações de litígio entre usuários, empresas de projetos e construtoras, tanto em casas, quanto de edifícios (veja mais sobre redes FTTx neste post). Essa foi a primeira normatização brasileira.

O portal Segurança e Tecnologia da Informação listou, em linhas gerais, todas as normatizações para cabeamento estruturado. São elas:

ANSI

TIA:

TIA 526-14A: Cabeamento de Fibra Ótica;

TIA 568A-A1-1998: Atraso de Propagação em cabos, componentes links básicos e canais;

TIA 568A-A4-1999: Cabos Patch;

Cores: BV,V,BL,A,BA,L,BM,M (T568A);

Cross: BL,L,BV,A,BA,V,BM,M (T568B);

EIA

ISO

ABNT

IEEE

Topologias de Redes

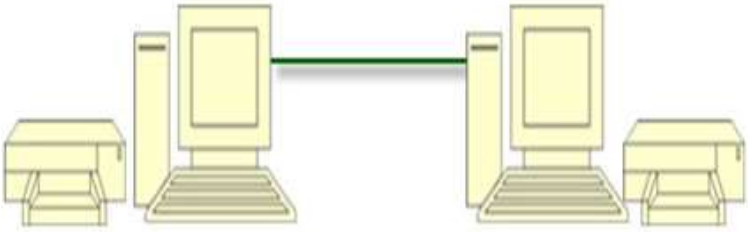
As redes de computadores possibilitam que indivíduos possam trabalhar em equipes, compartilhando informações, melhorando o desempenho da realização de tarefas, e estão presentes no dia-a-dia de todos nós. São estruturas sofisticadas e complexas, que mantém os dados e as informações ao alcance de seus usuários. É a topologia de redes que descreve como as redes de computadores estão interligadas, tanto do ponto de vista físico, como o lógico. A topologia física representa como as redes estão conectadas (layout físico) e o meio de conexão dos dispositivos de redes (nós ou nodos). Já a topologia lógica refere-se à forma com que os nós se comunicam através dos meios de transmissão.

Topologias Físicas

A topologia física pode ser representada de várias maneiras e descreve por onde os cabos passam e onde as estações, os nós, roteadores e gateways estão localizados. As mais utilizadas e conhecidas são as topologias do tipo estrela, barramento e anel.

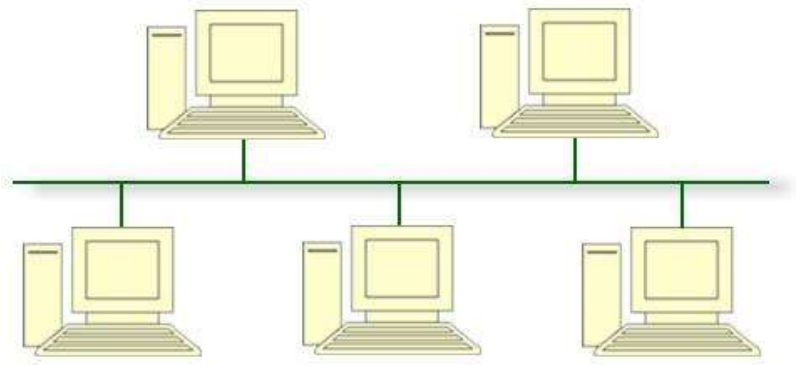
Ponto a Ponto

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



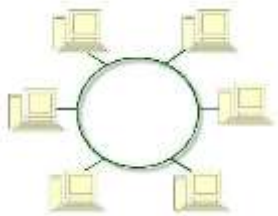
Barramento

Esta topologia é bem comum e possui alto poder de expansão. Nela, todos os nós estão conectados a uma barra que é compartilhada entre todos os processadores, podendo o controle ser centralizado ou distribuído. O meio de transmissão usado nesta topologia é o cabo coaxial.



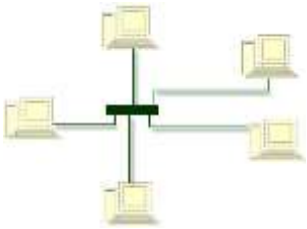
Anel ou Ring

A topologia em anel utiliza em geral ligações ponto-a-ponto que operam em um único sentido de transmissão. O sinal circula no anel até chegar ao destino. Esta topologia é pouco tolerável à falha e possui uma grande limitação quanto a sua expansão pelo aumento de "retardo de transmissão" (intervalo de tempo entre o início e chegada do sinal ao nó destino).



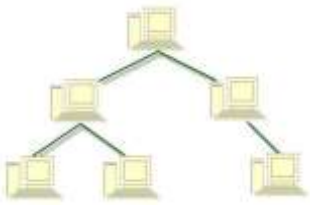
Estrela

A topologia em estrela utiliza um nó central (comutador ou switch) para chavear e gerenciar a comunicação entre as estações. É esta unidade central que vai determinar a velocidade de transmissão, como também converter sinais transmitidos por protocolos diferentes. Neste tipo de topologia é comum acontecer o overhead localizado, já que uma máquina é acionada por vez, simulando um ponto-a-ponto.



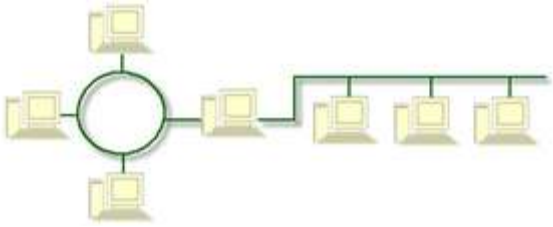
Árvore

A topologia em árvore é basicamente uma série de barras interconectadas. É equivalente a várias redes estrelas interligadas entre si através de seus nós centrais. Esta topologia é muito utilizada na ligação de Hub's e repetidores.



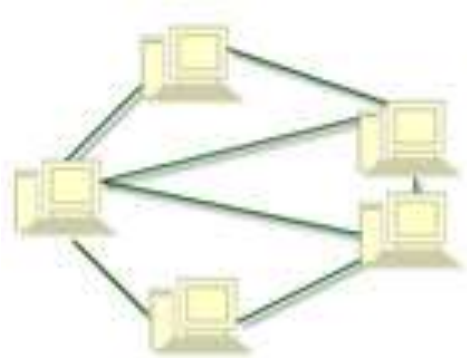
Estrutura Mista ou Híbrida

A topologia híbrida é bem complexa e muito utilizada em grandes redes. Nela podemos encontrar uma mistura de topologias, tais como as de anel, estrela, barra, entre outras, que possuem como características as ligações ponto a ponto e multiponto.



Grafo (Parcial)

A topologia em grafo é uma mistura de várias topologias, e cada nó da rede contém uma rota alternativa que geralmente é usada em situações de falha ou congestionamento. Traçada por nós, essas rotas têm como função rotear endereços que não pertencem a sua rede.



Topologias Lógicas

A topologia lógica descreve o fluxo de dados através da rede. Os dois tipos de topologias lógicas mais comuns são o Broadcast e a passagem Token. Na primeira o nó envia seus dados a todos os nós espalhados pela rede (Ethernet). Já na passagem de Token, um sinal de Token controla o envio de dados pela rede (Token Ring).

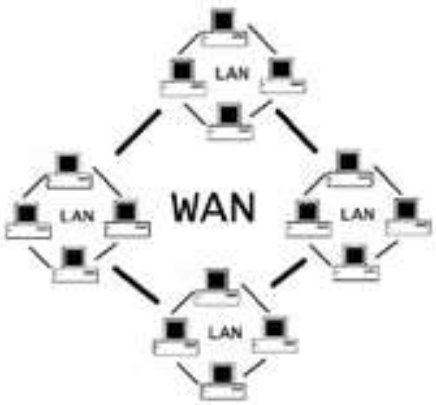
O que é uma rede LAN e uma rede WAN?

Os temos LAN e WAN são comumente encontrados nas telas de configurações de modens, roteadores e access points. O termo LAN se refere à configuração da rede local provida pelo roteador enquanto WAN se refere à configuração da rede externa, da internet, que não faz parte da rede interna.

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

WAN é Wide Área Network. Significa uma rede que cobre uma área física maior, como o campus de uma universidade, uma cidade, um estado ou mesmo um país. É usado frequentemente nas configurações dos roteadores para se referir à rede externa à empresa, que não é considerada parte da LAN, como foi dito acima.

WAN também é usado para se referir à rede da internet em geral, apesar desta ser uma designação genérica demais. As redes WAN se tornaram necessárias pois grandes empresas com milhares de computadores precisavam trafegar grande quantidade de informações entre filiais em diferentes localidades geográficas. Esta nova demanda não podia ser satisfeita dentro das capacidades de uma rede LAN e novos protocolos para atender aos exigências de velocidade e qualidade das redes WAN foram criados.



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.

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.

WAN – Rede de Longa Distância

A Wide Area Network, ou Rede de Longa Distância, vai um pouco além da MAN e consegue abranger uma área maior, como um país ou até mesmo um continente.

WLAN – Rede Local Sem Fio

Para quem quer acabar com os cabos, a WLAN, ou Rede Local Sem Fio, pode ser uma opção. Esse tipo de rede conecta-se à internet e é bastante usado tanto em ambientes residenciais quanto em empresas e em lugares públicos.

WMAN – Rede Metropolitana Sem Fio

Esta é a versão sem fio da MAN, com um alcance de dezenas de quilômetros, sendo possível conectar redes de escritórios de uma mesma empresa ou de campus de universidades.

WWAN – Rede de Longa Distância Sem Fio

Com um alcance ainda maior, 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 SANs, ou Redes de Área de Armazenamento, são utilizadas para fazer a comunicação de um servidor e outros computadores, ficando restritas a isso.

PAN – Rede de Área Pessoal

As redes do tipo PAN, ou Redes de Área Pessoal, são usadas para que dispositivos se comuniquem dentro de uma distância bastante limitada. Um exemplo disso são as redes Bluetooth e UWB.

Como Funcionam os WLANs

Através da utilização portadora de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa frequência específica e rejeita as outras portadoras de frequências diferentes.

Num ambiente típico, como o mostrado na Figura 1, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roamingsemelhante a um sistema de telefonia celular.

Um grupo de empresas está coordenando o desenvolvimento do protocolo IAPP (Inter-Access Point Protocol), cujo objetivo é garantir a a interoperabilidade entre fabricantes fornecendo suporte a roaming através das células. O protocolo IAPP define como os pontos de acesso se comunicarão através do backbone da rede, controlando os dados de várias estações móveis.

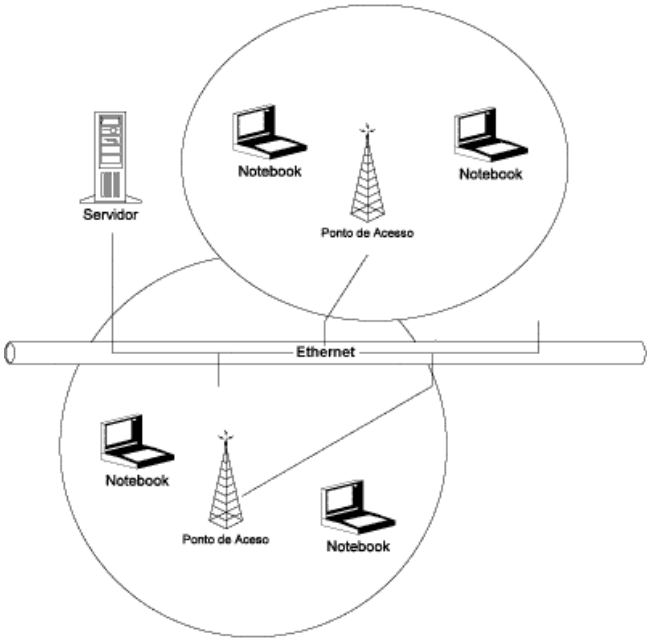


Figura 1 - Rede Wireless LAN típica

Tecnologias Empregados

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. A seguir, são apresentadas algumas das mais empregadas.

Sistemas Narrowband: Os sistemas narrowband (banda estreita) operam numa frequência de rádio específica, mantendo o sinal de de rádio o mais estreito possível o suficiente para passar as informações. O crosstalk indesejável entre os vários canais de comunicação pode ser evitado coordenando cuidadosamente os diferentes usuários nos diferentes canais de frequência.

Sistemas Spread Spectrum: São o mais utilizados atualmente. Utilizam a técnica de espalhamento espectral com sinais de rádio frequência de banda larga, provendo maior segurança, integridade e confiabilidade, em troca de um maior consumo de banda. Há dois tipos de tecnologias spread spectrum: a FHSS, Frequency-Hopping Spreap Spectrum e a DSSS, Direct-Sequence Spread Spectrum.

A FHSS usa uma portadora de faixa estreita que muda a frequência em um código conhecido pelo transmissor e pelo receptor que, quando devidamente sincronizados, o efeito é a manutenção de um único canal lógico.

A DSSS gera um bit-code (também chamado de chip ou chipping code) redundante para cada bit transmitido. Quanto maior o chip maior será a probabilidade de recuperação da informação original. Contudo, uma maior banda é requerida. Mesmo que um ou mais bits no chipsejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão.

Sistemas Infrared: Para transmitir dados os sistemas infravermelhos utilizam frequências muita altas, um pouco abaixo da luz visível no espectro eletromagnético. Igualmente à luz, o sinal infravermelho não pode penetrar em objetos opacos. Assim as transmissões por infravermelho ou são diretas ou difusas.

Os sistemas infravermelho diretos de baixo custo fornecem uma distância muito limitada (em torno de 1,5 metro). São comumente utilizados em PAN (Personal Area Network) como, por exemplo, os palm pilots, e ocasionalmente são utilizados em WLANs.

IEEE 802.11 Wireless Local Area Network

O grupo de trabalho IEEE 802.11, do Instituto dos Engenheiros Elétricos e Eletrônicos, é responsável pela definição do padrão para as redes locals sem fio WLANs.

O padrão proposto especifica três camadas físicas (PHY) e apenas uma subcamada MAC (Medium Access Control). Como apresentado abaixo, o draft provê duas especificações de camadas físicas com opção para rádio, operando na faixa de 2.400 a 2.483,5 mHz (dependendo da regulamentação de cada país), e uma especificação com opção para infravermelho.

Frequency Hopping Spread Spectrum Radio PHY:

Esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps utiliza 2 níveis da modulação GFSK (Gaussian Frequency Shift Keying), e a de 2 Mbps utiliza 4 níveis da mesma modulação;

Direct Sequence Spread Spectrum Radio PHY:

Esta camada provê operação em ambas as velocidades (1 e 2 Mbps). A versão de 1 Mbps utiliza da modulação DBPSK (Differential Binary Phase Shift Keying), enquanto que a de 2 Mbps usa modulação DBPSK (Differential Quadrature Phase Shift Keying);

Infrared PHY:

Esta camada fornece operação 1 Mbps, com 2 Mbps opcional. A versão de 1 Mbps usa modulação 16-PPM (Pulse Position Modulation com 16 posições), e a versão de 2 Mbps utiliza modulação 4-PPM.

No lado da estação, a subcamada MAC fornece os seguintes serviços: autenticação, desautenticação, privacidade e transmissão da MADU (MAC Sublayer Data Unit), e, no lado do sistema de distribuição: associação, desassociação, distribuição, integração e reassociação. As estações podem operar em dua siuações distintas:

Configuração Independente:

Cada estação se comunica diretamente entre si, sem a necessidade de instalação de infraestrutura. A operação dessa rede é fácil , mas a desvantagem é que a área de cobertura é limitada. Estações com essa configuração estão no serviço BSS (Basic Service Set);

Configuração de Infra-estrutura:

Cada estação se comunica diretamente com o ponto de acesso que faz parte do sistema de distribuição. Um ponto de acesso serve as estações em um BSS e o conjunto de BBS é chamado de ESS (Extended Service Set). Além dos serviços acima descritos, o padrão ainda oferece as funcionalidades de roaming dentro de um ESS e gerenciamento de força elétrica (as estações podem desligar seus transceivers para economizar energia). O protocolo da subcamada MAC é o CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence).

O que são?

Os protocolos são uma forma de padronizar todos os dispositivos que utilizam as redes Wi-Fi. Imagine o caos que seria se cada fabricante resolvesse criar uma tecnologia própria de transmissão de dados Wireless?

A criação dos padrões foi o jeito que a indústria encontrou para garantir que todos os aparelhos consigam se comunicar entre si utilizando a mesma tecnologia. Eles são gerenciados pelo IEEE (Instituto de Engenheiro e Eletricistas e Eletrônicos), que define as normas e especificações que as fabricantes devem usar.

Essas especificações são válidas não só para os roteadores, mas para qualquer outro aparelho que pretende usar Wi-Fi, seja televisões, smartphones ou dispositivos de Internet das Coisas.

Diferenças entre 802.11n e 802.11ac

Com a necessidade de avanço na tecnologia Wi-Fi, surgem novas especificações padronizadas pelo IEEE. Elas podem se diferenciar pela velocidade, pela faixa de espectro que usam e até mesmo pela quantidade de antenas que suportam, além, é claro, de novos recursos. A principal diferença entre os padrões n e ac é a velocidade. Enquanto os dispositivos que utilizam Wi-Fi n conseguem chegar a 450 Mbps, os dispositivos ac podem chegar a 1.300 Mbps, quase três vez mais rápido do que o padrão

anterior. Vale destacar que essa é a transferência de dados entre os dispositivos na rede e não a velocidade da Internet, que depende do provedor.

Outra diferenças está na quantidade de antenas. Enquanto o padrão n pode trabalhar com até quatro antenas, os roteadores ac comportam até oito antenas trabalhando simultaneamente. Com mais pontos de transmissão e recepção de sinal, menos congestionada fica a rede.

O padrão 802.11n opera em 2.4 GHz – também podendo trabalhar em 5 GHz. Já o 802.11ac trabalha em 5 GHz. Na prática, apesar de oferecer alcance menor, operar em 5 GHz que dizer trabalhar com menos interferências. Diversos dispositivos, de telefones sem fio a microondas, emitem sinais em 2.4 GHz, o que pode poluir a frequência, tornando o Wi-Fi instável. O ac também oferece uma largura de canal maior, até 160 MHz contra 40 MHz do n.

Modelo de referência da ISO, tem como principal objetivo ser um modelo padrão para protocolos de comunicação entre diversos tipos de sistema, garantindo a comunicação end-to-end, o Modelo OSI (em inglês Open Systems Interconnection) foi lançado em 1984 pela Organização Internacional para a Normalização (em inglês International Organization for Standardization).

Trata-se de uma arquitetura modelo que divide as redes de computadores em 7 camadas para obter camadas de abstração. Cada protocolo realiza a inserção de uma funcionalidade assinalada a uma camada específica.

Utilizando o Modelo OSI é possível realizar comunicação entre máquinas distintas e definir diretivas genéricas para a elaboração de redes de computadores independente da tecnologia utilizada, sejam essas redes de curta, média ou longa distância.

Este modelo exige o cumprimento de etapas para atingir a compatibilidade, portabilidade, interoperabilidade e escalabilidade. São elas: a definição do modelo, definição dos protocolos de camada e a seleção de perfis funcionais. A primeira delas define o que a camada realmente deve fazer. A segunda faz a definição dos componentes que fazem parte do modelo, enquanto que a terceira é realizada pelos órgãos de padronização de cada país.

O Modelo OSI é composto por 7 camadas, sendo que cada uma delas realizam determinadas funções. As camadas são: Aplicação (Application), Apresentação (Presentation), Sessão (Session), Transporte (Transport), Rede (Network), Dados (Data Link) e Física (Physical).

Este conceito de modelo baseado em sete camadas foi fornecido por Charles Bachman em um de seus trabalhos. A evolução do projeto OSI começou a partir de experiência com a ARPANET, a Internet incipiente, a NPLNET, o EIN, o CYCLADES e também com o trabalho em IFIP WG6.1. A partir daí, com base neste modelo, um sistema de rede passou a ser dividido em camadas. Dentro de cada uma delas, uma ou mais entidades se encarregavam de implementar sua funcionalidade.

Atualmente, a ISO trabalha em parceria com outra organização, a União Internacional de Telecomunicações (em inglês International Telecommunications Union), publicando diversas especificações de protocolos que tem como base a arquitetura OSI.

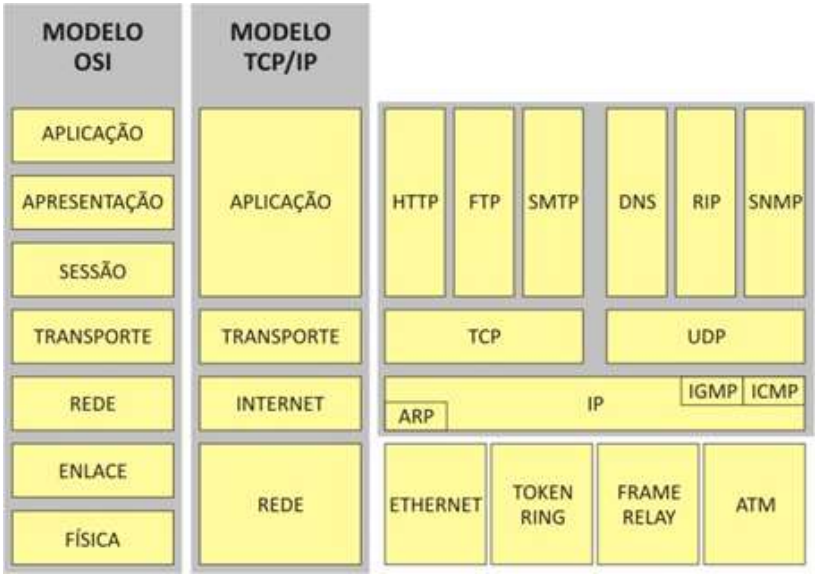
Modelo TCP/IP

O modelo TCP/IP – Transmission Control Protocol/Internet Protocol – é uma coleção de protocolos utilizados para realizar a comunicação de computadores em uma rede. Conheceremos sua definição, camadas e funcionamento.

Seu desenvolvimento inicial, em 1969, foi financiado pela Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos (DoD).

Imaginem um mundo em guerra, interligado por diferentes conexões como cabos, microondas, fibras óticas, links de satélite e, ainda a necessidade de trafegar informações e dados, independentemente da condição de qualquer nó ou rede.

Foi dentro desse complexo cenário que levou à criação do modelo TCP/IP e que tornou-se, desde então, o padrão no qual a Internet se desenvolveu.



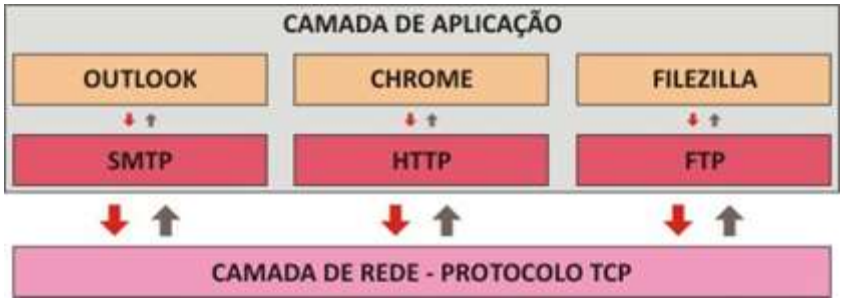
É importante perceber que algumas das camadas do modelo TCP/IP têm o mesmo nome das camadas no modelo OSI. Mas acredite, as camadas dos dois modelos têm funções e protocolos característicos.

Camadas do Modelo TCP/IP

O conjunto de protocolos TCP/IP é dividido em quatro camadas – aplicação, transporte, internet e rede **–** sendo cada uma responsável pela execução de tarefas distintas, para a garantir a integridade e entrega dos dados trafegados.

Camada de aplicação

Esta camada faz a comunicação entre os programas e os protocolos de transporte no TCP/IP.



Quando você solicita ao seu cliente de e-mail para fazer o download das mensagens que estão armazenados no servidor, você está fazendo uma solicitação à camada de aplicação do TCP/IP, que neste caso é servido pelo protocolo SMTP. Quando você abre uma página no seu navegador, ele vai requerer ao TCP/IP, na camada de aplicação, servido pelo protocolo HTTP, por isso que as páginas iniciam-se com http://.

A camada de aplicação possui protocolos importantes e conhecidos, como o HTTP, FTP, DNS e DHCP.

O HTTP é utilizado para a comunicação de dados da internet – WWW;

O FTP é utilizado para a transferência de arquivos de modo interativo;

O DNS é utilizado para resolver o nome de um host em endereço IP;

O DHCP é utilizado para oferecer dinamicamente endereços de rede.

Camada de transporte

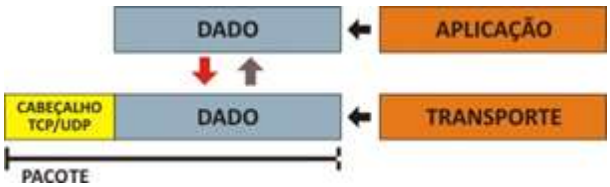
Esta camada é responsável por receber os dados enviados pela camada de aplicação e transformá-los em pacotes menores, a serem repassados para a camada de internet. Ela garante que os dados chegarão sem erros e na sequência correta.

É formado por dois protocolos o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente. Não possui confirmação de entrega e é geralmente usado na transmissão de informações de controle.

O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de fluxo e erro, a sequencia e a multiplexação de mensagens.

Tanto o UDP quanto o TCP recebem o dado da camada de aplicação e acrescentam um endereço virtual, chamado cabeçalho, a cada pacote, que é removido quando chega ao receptor. Neste cabeçalho existem informações importantes como o número da porta de entrada, a sequência do dado e a soma para verificação da integridade (checksum).



Camada de Internet

Ela é responsável pelo endereçamento e roteamento do pacote, fazendo a conexão entre as redes locais. Adiciona ao pacote o endereço IP de origem e o de destino, para que ele saiba qual o caminho deve percorrer.

Na transmissão, o pacote de dados recebido da camada de transporte é dividido em pedaços chamados datagramas. Os datagramas são enviados para a camada de interface com a rede (última camada), onde são transmitidos pelo cabeamento da rede através de quadros.

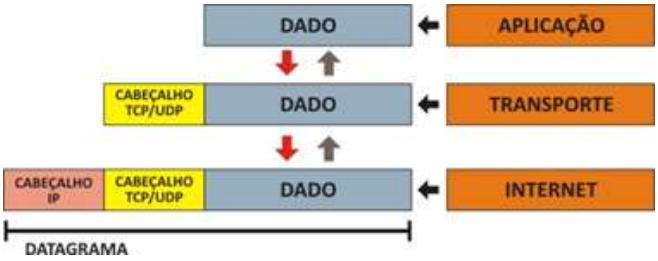
Os protocolos principais da camada da Internet são IP, ARP, ICMP e IGMP.

O IP é um protocolo roteável responsável pelo endereçamento IP, fragmentação e montagem dos pacotes;

O ARP é responsável pela resolução do endereço da camada de internet para o endereço da camada de interface de rede, tais como um endereço de hardware;

O ICMP é responsável por fornecer funções de diagnóstico e relatar erros devido à entrega bem sucedida de pacotes IP;

O IGMP é responsável pela gestão dos grupos de multicast IP.



Camada de interface com a rede

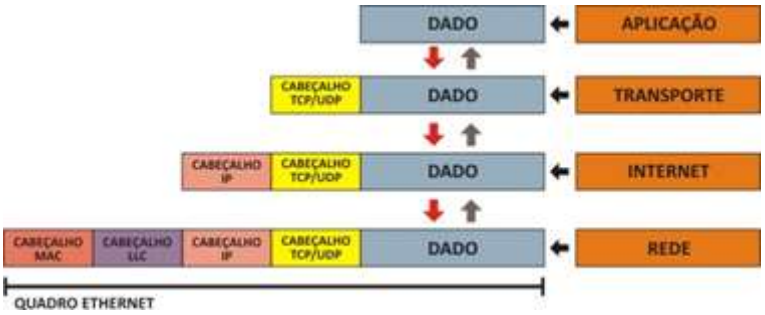
Essa camada é responsável pelo envio do datagrama recebido da camada de internet em forma de quadros através da rede física.

O Ethernet é o protocolo mais utilizado e possui três componentes principais:

Logic Link Control (LLC): responsável por adicionar ao pacote, qual protocolo da camada de internet vai entregar os dados para a serem transmitidos. Quando esta camada recebe um pacote, ela sabe para qual protocolo da camada de internet deve ser entregue.

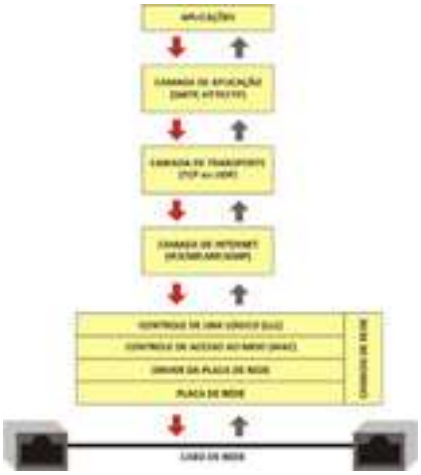
Media Access Control (MAC): responsável por montar o quadro que vai ser enviado pela rede e adiciona tanto o endereço origem MAC quanto o endereço destino, que é o endereço físico da placa de rede.

Physical: responsável por converter o quadro gerado pela camada MAC em eletricidade (se for uma rede cabeada) ou em ondas eletromagnéticas (se for uma rede wireless).



Funcionamento

Na imagem abaixo podemos ver a integração de todas as camadas do modelo TCP/IP acima citadas, para garantir o correto funcionamento da rede.



*Protolocos de rede: São procedimentos que controlam e regulam a comunicação, conexão e transferência de dados entre sistemas computacionais.

Qual a diferença entre um Switch de Rede e um roteador?

O que é um Switch de Rede?

Para entender os conceitos básicos de rede, primeiro precisamos te explicar o que é um switch de rede. Atualmente, a maioria das redes empresariais utilizam switches para conectar computadores, impressoras e servidores dentro de um prédio empresarial ou campus universitário. O switch funciona como um elemento que controla a comunicação entre os dispositivos conectados à rede, permitindo que estes se comuniquem de forma eficiente.

Estes equipamentos segmentam a rede possibilitado que o fluxo de informações trocado entre os dispositivos seja eficiente, e desta forma impactando positivamente na utilização da rede, reduzindo o custo operacional e melhorando a produtividade dos funcionários. Entenda os tipos de switch Ethernet e suas características.

Switch de rede não gerencíável.

Um switch não gerenciável não requer configuração para funcionar. Assim que é retirado da “caixa” basta ligar na energia e já estará funcionado.

Porém switches não gerenciáveis, possuem menos funcionalidade e menor capacidade que switches gerenciáveis. Os não gerenciáveis são usualmente encontrados em redes residenciais.

Switch de rede gerencíável.

Um switch de rede gerenciável requer configurações, porém oferece maior flexibilidade e capacidade. É possível ter maior controle da rede, monitorando e ajustando localmente ou de forma remota.

Qual a diferença entre Network Switch e Router?

De maneira simplificada, switches criam redes, enquanto os roteadores conectam essas redes. Roteadores conectam computadores à Internet, de modo que os usuários possam compartilhar uma conexão física. O roteador busca as melhores rotas/caminhos para enviar e receber dados, desta forma a informação tráfega rapidamente na Internet.

Como um Switch de Rede é útil para o meu negócio?

Switches e roteadores são peças fundamentais para toda a comunicação da empresa, abrangendo a comunicação de dados, voz, video e Wi-Fi. Estes dispositivos melhoram a rentabilidade da empresa, permitindo aumento de produtividade, redução de custos, melhoria da segurança da informação e dos serviços oferecido aos clientes.

_____

_____

_____

_____

_____

_____

_____

_____

_____