academia de tecnologia

REDES

academia de tecnologia

INDICE

1. Informações Gerais

REDE GLOBO DE TELEVISÃO	
Rua Lopes Quintas, 303	Jardim Botânico
Rio de Janeiro - RJ	
CEP: 22460-901	
Tel.: (21) 2540-3300	

1.1 Responsáveis

Setor	Tecnologia
Supervisor	Evaldo Jesus evaldo@tvglobo.com.br
Instrutor	Daniel Spalla daniel.spalla@tvglobo.com.br

2. OBJETIVO

Este curso tem por objetivo prover conceitos básicos de redes que possibilitem o entendimento de teorias e boas práticas, assim como compartilhar a vivência e expandir parte do conhecimento da cultura de redes dentro da área de Tecnologia da TV Globo.

Com isso, esperasse que ao final do curso todos os participantes tenham o mínimo de conhecimento de rede para uma eventual necessidade de uso em sua área de atuação ou de identificar, inicialmente, um problema.

3. REDES DE COMPUTADORES

A primeira coisa que devemos entender ao começar a estudar redes é a sua definição. Quando falamos em redes de computadores, a maioria das pessoas pensa em uma série de computadores ligados entre si por meio de cabos para trocarem dados ou então pensa em grandes redes como a Internet. A disciplina de Redes de Computadores de fato estuda estas coisas, mas ela também estuda muito mais coisas, pois o assunto de redes de computadores é algo bastante amplo e possui uma quantidade enorme de aplicações.

Uma boa definição de **Rede de Computadores** é: *Uma rede de computadores é um conjunto de dois ou mais dispositivos (também chamados de **nós**) que usam um conjunto de regras (protocolo) em comum para compartilhar recursos (hardware, troca de mensagens) entre si, através de uma determinada conexão, podendo ser: por fio de cobre, fibra ótica, ondas de rádio, infravermelho e também via satélite.*

Perceba que qualquer tipo de dispositivo capaz de enviar ou receber dados pode ajudar a compor uma rede, não apenas um computador. Por essa razão, quando falamos em componentes de rede, nos referimos a eles como "**nós"**, e não computadores.

O termo redes de computadores está cada vez mais em desuso com as novas tecnologias e dispositivos que estão sendo interconectados na internet pública. Estes dispositivos conhecidos como sistemas finais não são unicamente compostos de computadores de mesa, mas também de uma grande variedade de equipamentos que incluem telefones celulares, sistemas de automação residencial ou industrial, computadores portáteis e aparelhos eletrônicos diversos.

Estes sistemas finais são interconectados e percorrem uma rota ou caminho que passa por enlaces de comunicação (cabos, ondas, fibras ópticas etc) e também por comutadores de pacotes (switches, hubs, roteadores etc). O primeiro é o meio físico responsável pela transmissão em si enquanto o segundo faz o encaminhamento dos pacotes aos seus destinos.

Os sistemas finais acessam a internet por meio de ISP (provedores de serviço de internet) de nível baixo que são interconectados por ISP de nível alto, compostos por roteadores e sistemas de fibra óptica de altíssima velocidade, obedecendo a certas convenções de nomeação e endereço a fim de padronizar o acesso à rede.

Os protocolos controlam o envio e recebimento das informações e envolvem todos os dispositivos que compõem a internet, sendo o mais famoso deles o conjunto de protocolos conhecido como TCP/IP. Este protocolo, cujo nome vem dos protocolos mais importantes de pilha, TCP e IP, foi desenvolvido originalmente pela Universidade da Califórnia para o Departamento de Defesa dos EUA (DoD). Atualmente o TCP/IP é o protocolo padrão para redes locais e remotas.

3.1 VANTAGENS DO USO DAS REDES

- Compartilhamento de arquivos de trabalho
- Compartilhamento de programas
- Compartilhamento de periféricos
- Compartilhamento de impressoras
- Compartilhamento de acesso à Internet

3.2 DESVANTAGENS DO USO DAS REDES

- Ataque de vírus
- Problemas generalizados
- Invasão de hackers internos e externos

3.3 CLASSIFICAÇÃO DE REDES

As redes podem ser classificadas de diferentes maneiras: Pelo tipo de arquitetura, extensão geográfica, tipo de topologia e pelo tipo do meio de comunicação.

Arquitetura de Rede:

- Arcnet (Attached Resource Computer Network)
- Ethernet
- Token ring
- FDDI (Fiber Distributed Data Interface)
- ISDN (Integrated Service Digital Network)
- Frame Relay
- ATM (Asynchronous Transfer Mode)
- X.25
- DSL (Digital Subscriber Line)

Extensão geográfica:

- SAN (Storage Area Network)
- LAN (Local Area Network)
- WLAN (Wireless Local Area Network)
- PAN (Personal Area Network)
- MAN (Metropolitan Area Network)
- WMAN Wireless Metropolitan Area Network
- WAN (Wide Area Network)
- WWAN (Wireless Wide Area Network)
- RAN (Regional Area Network)
- CAN (Campus Area Network)

Topologia:

- Rede em anel (Ring)
- Rede em barramento (Bus)
- Rede em estrela (Star)
- Rede em malha (Mesh)
- Rede em ponto-a-ponto (ad-hoc)
- Rede em árvore

Meio de transmissão:

Rede por cabo

- Rede de Cabo coaxial
- Rede de Cabo de fibra óptica
- Rede de Cabo de par trançado

Rede sem fios

- Rede por infravermelhos
- Rede por micro-ondas
- Rede por rádio

3.4 HISTÓRIA DA INTERNET

A Internet começou com um projeto do Departamento de Defesa (DoD – Department of Defense) do governo estadunidense que, em 1966, por meio da Agencia de Pesquisas e de Projetos Avançados (ARPA – Advanced Research Projects Agency), iniciou um projeto para a interligação de computadores em centros militares e de pesquisa. Este sistema de comunicação e controle distribuído com fins militares recebeu o nome de ARPANET, tendo como principal objetivo teórico formar uma arquitetura de rede sólida e robusta capaz, mesmo com a queda de alguma estação, de funcionar com os computadores e ligações de comunicação restantes. Em 1969, são instalados os primeiros quatro nós dessa rede, localizados na Universidade de Los Angeles (UCLA), na Universidade da Califórnia em Santa Bárbara (UCSB), no Instituto de Pesquisas de Standford (SRI) e na Universidade de Utah.

No início, a ARPANET trabalhava com diversos protocolos de comunicação, com enfoque no NCP (Network Control Protocol). No entanto, em primeiro de janeiro de 1983, quando a rede atingiu a marca de 562 hosts, todas as máquinas da ARPANET passaram a adotar como padrão os protocolos TCP/IP. Essa mudança ocasionou o crescimento ordenado da rede, pois eliminou restrições dos protocolos anteriores.

A Internet também teve outros importantes atores que influenciaram o seu surgimento, dentre eles: os professores universitários (ex: Ken King), os estudantes/investigadores (ex.: Vint Cerf), as empresas de tecnologia (ex.: IBM) e alguns políticos norte-americanos (ex.: Al Gore); caindo-se, portanto, a tese que vigorava anteriormente que enfatizava somente a vertente militar da sua criação.

3.5 MODELO OSI

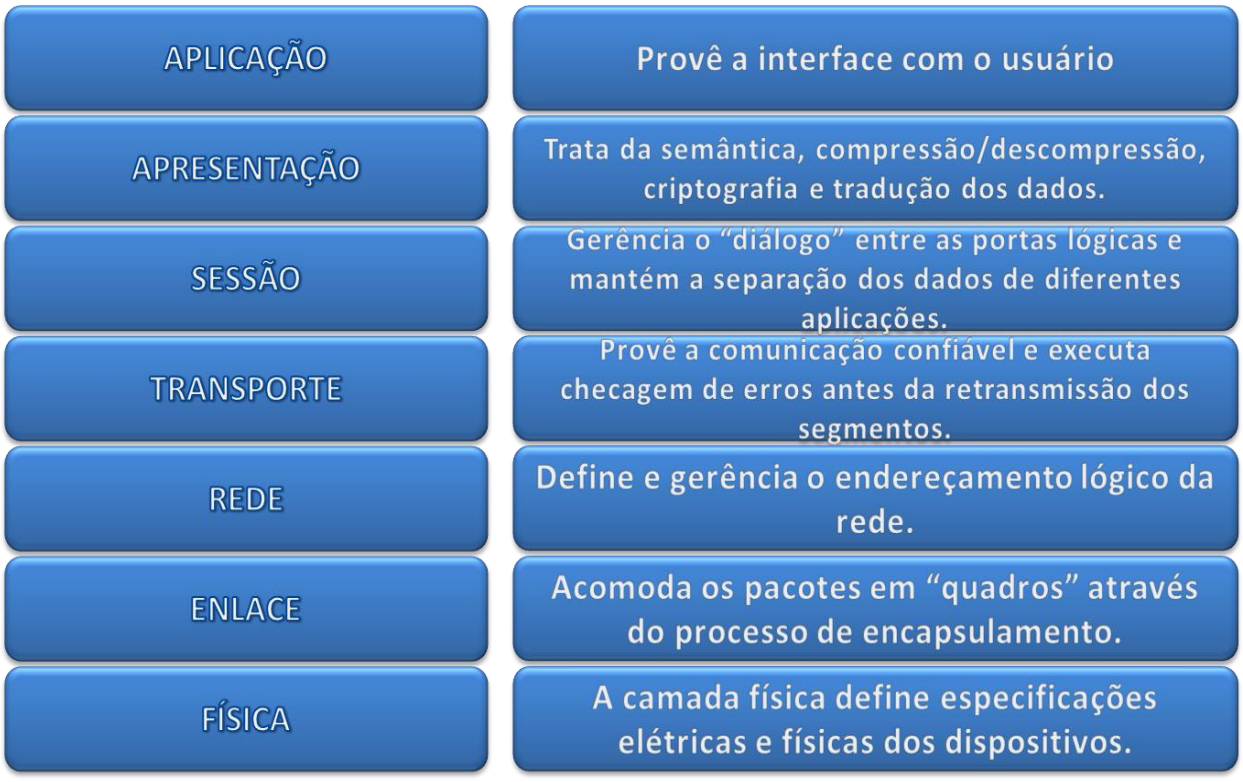
Com o surgimento das redes de dados, os fabricantes possuíam protocolos próprios para a comunicação dos seus computadores. Por exemplo, ou as empresas utilizavam soluções proprietárias da IBM ou soluções da DEC (hoje HP).

Então, a Organização Internacional para a Normalização (do inglês: International Organization for Standardization - ISO), foi uma das primeiras organizações a definir formalmente uma arquitetura padrão com objetivo de facilitar o processo de interconectividade entre máquinas de diferentes fabricantes, assim em 1984 lançou o padrão chamado Interconexão de Sistemas Abertos (do inglês: Open Systems Interconnection - OSI) ou Modelo OSI.

A Organização Internacional para a Normalização (ISO) começou a desenvolver a sua estrutura de arquitetura OSI, com quatro componentes principais: um modelo abstrato de rede, o chamado Modelo de Referência Básico ou sete camadas do modelo, e um conjunto de protocolos específicos e outros dois de menor relevância.

O modelo OSI descreve como os dados são transmitidos, sendo uma peça chave para o estudo e entendimento dos conceitos de transmissão em rede. Este modelo garante a compatibilidade, interação entre tecnologias, simplifica o aprendizado, reduz a complexidade, padroniza interfaces, permite a criação de estruturas modulares e acelera a evolução.

Este modelo separa a rede em sete camadas, cada uma descrevendo uma função, permitindo o entendimento de como a informação trafega em uma rede.



3.5.1 FÍSICA – CAMADA 1

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 (HBA usado em redes de área de armazenamento) e muito mais. A camada física é responsável por definir se a transmissão pode ser ou não realizada nos dois sentidos simultaneamente. Sendo a camada mais baixa do modelo OSI, diz respeito a transmissão e recepção do fluxo de bits brutos não-estruturados em um meio físico. Ela descreve as interfaces elétricas, ópticas, mecânicas e funcionais para o meio físico e transporta sinais para todas as camadas superiores.

3.5.2 ENLACE – CAMADA 2

Esta camada detecta e, opcionalmente, corrige erros que possam acontecer na camada física. É responsável pela transmissão e recepção (delimitação) de quadros e pelo controle de fluxo. Ela também estabelece um protocolo de comunicação entre sistemas diretamente conectados.

Na rede ethernet cada placa de rede possui um endereço físico, que deve ser único na rede. Em redes do padrão IEEE 802, e outras não IEEE 802 como a FDDI, esta camada é dividida em outras duas camadas: Controle de ligação lógica (LLC), que fornece uma interface para camada superior (rede), e controle de acesso ao meio físico (MAC), que acessa diretamente o meio físico e controla a transmissão de dados.

3.5.3 REDE – CAMADA 3

É responsável por controlar a operação da rede de um modo geral. Suas principais funções são o roteamento dos pacotes entre fonte e destino, mesmo que estes tenham que passar por diversos nós intermediários durante o percurso, o controle de congestionamento e a contabilização do número de pacotes ou bytes utilizados pelo usuário.

3.5.4 TRANSPORTE – CAMADA 4

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 camada de transporte separa as camadas de nível de aplicação (camadas 5 a 7) das camadas de nível físico (camadas de 1 a 3).

3.5.5 SESSÃO – CAMADA 5

Responsável pela troca de dados e a comunicação entre hosts, 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.

3.5.6 APRESENTAÇÃO – CAMADA 6

A camada de apresentação é responsável pela entrega e formatação da informação para a camada de aplicação para posterior processamento ou apresentação. Ela libera a camada de aplicação de questões relacionadas às diferenças sintáticas na representação de dados dentro dos sistemas do usuário final. Um exemplo de um serviço de apresentação seria a conversão de um arquivo de computador de texto codificado em EBCDIC para um arquivo codificado em ASCII. Ela também é responsável pela compressão e criptografia dos dados.

3.5.7 APLICAÇÃO - CAMADA 7

A camada de aplicação corresponde às aplicações (programas) no topo da camada OSI que serão utilizadas 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).

Tudo nesta camada é relacionado ao software. Alguns protocolos utilizados nesta camada são: HTTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping, etc.

3.6 TIPOS DE REDES

3.6.1 LAN

A rede LAN é formada por computadores interligados por meio de cabos, ondas de rádio ou infravermelho, em um mesmo local físico, dispensando a necessidade de modems. O conjunto de elementos que permitem a comunicação entre os computadores define o meio, o qual pode utilizar diversas tecnologias, tais como: Ethernet, Token Ring, Token Bus, FDDI (Fiber Distributed Data Interface) ou ATM.

A tecnologia mais utilizada é conhecida por Ethernet. Isto acontece em razão de 32 Redes de Computadores sua simplicidade de instalação, seu baixo custo e, principalmente, em virtude dos investimentos realizados pela indústria nesta tecnologia, que a levou ao topo entre as concorrentes. A Ethernet é um canal físico por onde os dados podem fluir de um computador para outro. A velocidade com a qual os dados conseguem fluir pelo barramento determina a sua largura de banda, assim quanto maior o valor da largura de banda, mais dados pode ser transferido em um mesmo intervalo de tempo. As larguras de banda mais comuns para o padrão Ethernet estão representadas na Tabela abaixo:

Largura de banda	**Descrição**
10 Mbps	Transmite 10 milhões de bits por segundo.
100 Mbps	Transmite 100 milhões de bits por segundo
1 Gbps	Transmite 1 bilhão de bits por segundo
10 Gbps	Transmite 10 bilhões de bits por segundo

3.6.2 WLAN

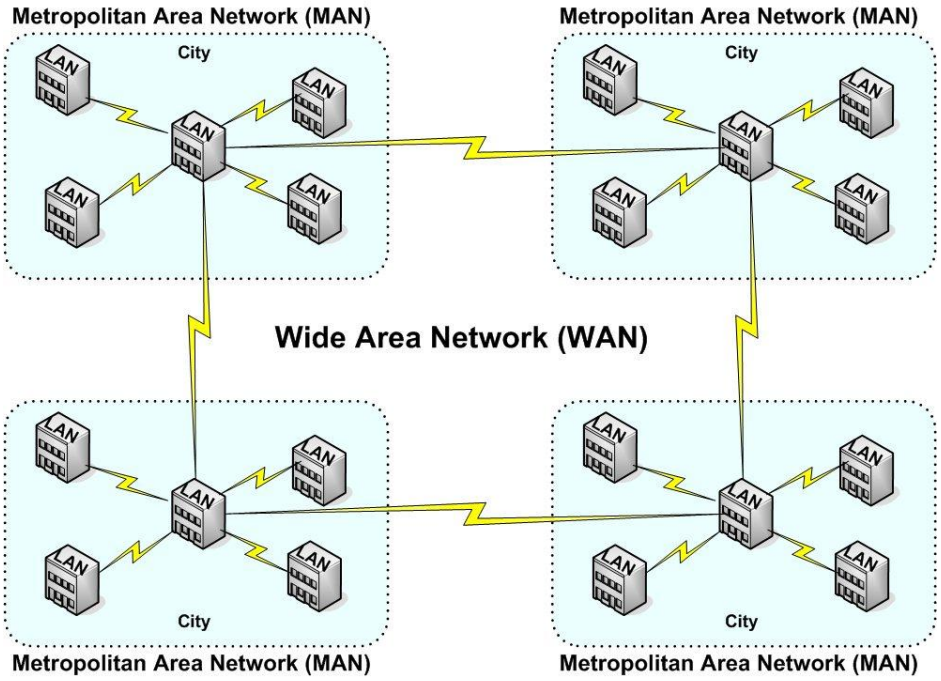
Wireless LAN ou **WLAN** (*Wireless Local Area Network* - Rede de área local sem-fio) é uma rede local que usa ondas de rádio para fazer uma conexão Internet ou entre uma rede

3.6.3 MAN

Uma rede de área metropolitana, ou MAN (em inglês: metropolitan area network), interliga várias redes geograficamente próximas (até algumas dezenas de quilômetros) num circuito urbano. Assim, que nós distantes comuniquem-se como se fizessem parte de uma mesma rede local.

3.6.4 WAN

As redes WAN (Wide Area Network) são formadas pela interligação de pequenas ou grandes redes LANs. Cada ponta da rede WAN possui a mesma estrutura de uma rede LAN, e a conexão entre elas é feita por meio de linhas telefônicas, fibras ópticas ou ondas de rádio. A Internet pode ser considerada uma grande rede WAN, pois interliga milhões de pequenas redes LANs ao redor do mundo. Como regra básica, uma WAN sempre é formada pela interligação de pelo menos dois modems, os quais devem estar ligados a roteadores, equipamentos ativos responsáveis pela interligação de duas redes diferentes, eles serão comentados no decorrer deste livro. O objetivo do roteador é redirecionar os dados que recebe para outra rede, fazendo um novo pacote desses dados, permitindo assim a conexão de duas redes com protocolos diferentes. Essa característica do roteador de criar um novo pacote de dados com os que chegam, permite que este equipamento ativo remonte os pacotes, de forma que redes com arquiteturas diferentes tais como Ethernet e Token Ring, possam interagir entre si.



3.7 ELEMENTOS DE REDE

Podemos classificar os elementos de rede como elementos ativos e passivos. Ambos os elementos são denominados como nós ou host de rede. Abaixo alguns exemplos:

ATIVOS:

São todos os elementos que são responsáveis pelo encaminhamento, controle e direcionamento das informações de redes. Os principais ativos de redes são: Placas de redes, Roteadores, Swicthes, Access Points (AP), Firewalls.

- **Roteadores**: Roteador (router em inglês) é um dispositivo que encaminha pacotes de dados entre redes de computadores, criando um conjunto de redes de sobreposição. Um roteador é conectado a duas ou mais linhas de dados de redes diferentes. Quando um pacote de dados chega, em uma das linhas, o roteador lê a informação de endereço no pacote para determinar o seu destino final. Em seguida, usando a informação na sua política tabela de roteamento ou encaminhamento, ele direciona o pacote para a rede de próxima em sua viagem. Os roteadores são os responsáveis pelo "tráfego" na Internet. Um pacote de dados é normalmente encaminhado de um roteador para outro através das redes que constituem a internetwork até atingir o nó destino. E, portanto o roteador é tipicamente um dispositivo da camada 3 do Modelo OSI.
- **Swicthes**: É um elemento ativo que age no nível 2 do modelo OSI, é um equipamento que interliga os computadores em uma rede, os cabos de rede de cada computador se ligam a ele, que então direciona os dados enviados de um computador especificamente para outro.

  Existem dois tipos básicos de switches que podem ser usados em redes locais de computadores: os gerenciáveis (L3) e os não gerenciáveis (L2). Enquanto os switches não gerenciáveis são dispositivos indicados para o uso em redes pequenas no lugar dos hubs, os switches gerenciáveis oferecem um conjunto de características avançadas com maiores funcionalidades, sendo imprescindíveis em redes de maior porte.
- **Firewalls**: Um firewall (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc. Os firewalls são geralmente associados a redes TCP/IP.

PASSIVOS:

São dispositivos que não interferem com os dados ou sinais que passam por ele e que permitem a interligação do equipamento ativo: Ups, bastidores, calhas, réguas de alimentação de bastidores, patch panel’s, cabos, conectores entre outros.

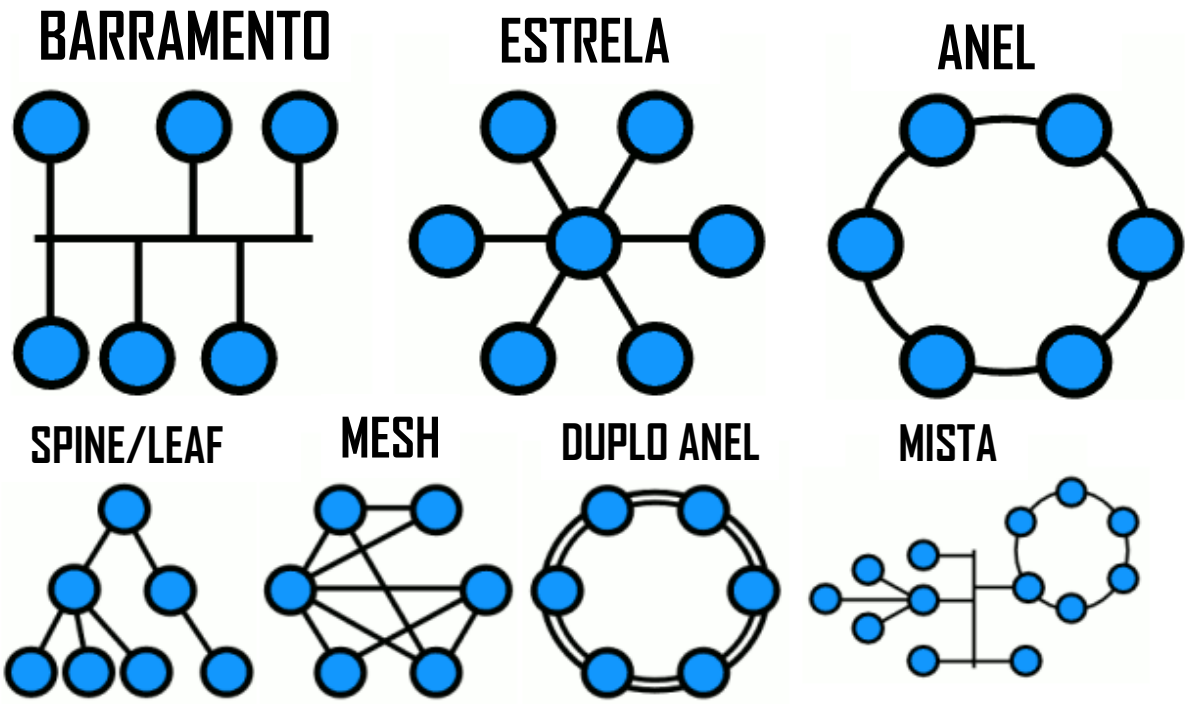
3.8 TOPOLOGIA

A **topologia de rede** é o canal no qual o meio de rede está conectado aos computadores e outros componentes de uma rede de computadores. Essencialmente, é a estrutura topológica da rede, e pode ser descrito física ou logicamente. Há várias formas nas quais se podem organizar a interligação entre cada um dos nós (computadores) da rede. Existem duas categorias básicas de topologias de rede:

- Topologia física
- Topologia lógica

A topologia física é a verdadeira aparência ou layout da rede, enquanto que a lógica descreve o fluxo dos dados através da rede. A topologia física representa como as redes estão conectadas (layout físico) e o meio de conexão dos dispositivos de redes (nós ou nodos). A forma com que os cabos são conectados, e que genericamente chamamos de topologia da rede (física), influencia em diversos pontos considerados críticos, como a flexibilidade, velocidade e segurança.

A topologia lógica refere-se à maneira como os sinais agem sobre os meios de rede, ou a maneira como os dados são transmitidos através da rede a partir de um dispositivo para o outro sem ter em conta a interligação física dos dispositivos. Topologias lógicas são frequentemente associadas à Media Access Control, métodos e protocolos. Topologias lógicas são capazes de serem reconfiguradas dinamicamente por tipos especiais de equipamentos como roteadores e switches.



4. MEIOS FÍSICOS DE TRANSMISSÃO

Para definir os meios físicos é necessário entender o comportamento dos bits. Um bit viaja partir de um sistema através de uma série de links e roteadores até atingir o sistema de destino. Nesse caminho, o bit é transmitido diversas vezes. O sistema de origem transmite o bit, o primeiro roteador recebe o bit e o transmite e assim por diante. Enquanto viaja da origem para o destino, o bit passa por uma série de transmissores e receptores. Cada bit é enviado pela propagação de ondas eletromagnéticas ou pulsos ópticos através de um meio físico. Os meios físicos podem ter formas distintas e não precisam ser do mesmo tipo em todo o caminho. Exemplos de meios físicos incluem par-trançado, cabo coaxial, cabo de fibra-óptica, espectro de rádio terrestre, e, espectro de rádio por satélite. Os meios físicos dividem-se em duas categorias: meios encapsulados e não encapsulados. Nos meios encapsulados, as ondas percorrem um material sólido. Os exemplos desse tipo de meio são: cabo de fibra-óptica, par-trançado e cabo coaxial. Nos meios não encapsulados, as ondas propagam-se na atmosfera e no espaço. Exemplos: LAN wireless e canal digital de satélite. O custo do link físico é relativamente baixo comparado a outros custos da rede. O custo de instalação do link físico pode ser muito superior ao custo do material. Por essa razão, muitos construtores instalam tipos variados de cabos em todas as salas de um edifício. Mesmo que, inicialmente, só um meio seja usado, existe uma boa chance de outro meio ser usado no futuro. Dessa forma, economiza-se dinheiro evitando a colocação de fios no futuro.

4.1 TIPOS DE CABEAMENTO

Cabeamento é a conexão efetuada entre as redes de computadores dentre outras. O primeiro tipo de cabeamento que surgiu foi o cabo coaxial. Há poucos anos, esse tipo de cabeamento era o que havia de mais avançado. Com o passar do tempo, por volta dos anos 1990, o cabo coaxial foi ficando para trás com o surgimento dos cabos de par trançado. Esse tipo de cabo veio a se tornar muito usado devido a sua flexibilidade e também pela necessidade de se ter um meio físico com uma taxa de transmissão mais elevada e com maior velocidade. Posteriormente, surgiram padronizações das interfaces e meios de transmissão, de modo a tornar o cabeamento independente da aplicação e do layout da rede e para facilitar sua reconfiguração e expansão.

Em redes de computadores, os principais tipos de cabeamento são:

- Coaxial
- Par trançado
- Fibra ótica

4.1.1 PAR TRANÇADO

O cabeamento por par trançado (Twisted pair) é um tipo de cabo que possui pares de fios entrelaçados um ao redor do outro para cancelar as interferências eletromagnéticas (EMI). Foi inventado por Alexander Graham Bell no final do século XIX.

Os cabos UTP foram padronizados pelas normas da EIA/TIA-568-B e são divididos em 10 categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores, veja abaixo um resumo simplificado dos cabos UTP.

Nome	Padrão	Largura de banda	Aplicações	Notas
Cat.1		0.4 MHz	Telefonia e linhas de modem	Não é descrita nas recomendações da EIA/TIA. Obsoleto[2]
Cat.2		4 MHz	Sistemas legados, IBM 3270	Não é descrita nas recomendações da EIA/TIA. Obsoleto.[2]
Cat.3	UTP	16 MHz	10BASE-T e 100BASE-T4 Ethernet	Descrito na EIA/TIA-568. Não recomendado para taxas maiores que 16 Mbit/s. Cabos de telefonia.
Cat.4	UTP	20 MHz	16 Mbit/s Token Ring	Obsoleto.
Cat.5	UTP	100 MHz	100BASE-TX & 1000BASE-T Ethernet	Muito usados nas redes LAN
Cat.5e	UTP	125 MHz	100BASE-TX & 1000BASE-T Ethernet	Melhoria da Cat5.
Cat.6	UTP	250 MHz	10GBASE-T Ethernet	
Cat.6a	U/FTP, F/UTP	500 MHz	10GBASE-T Ethernet	Adiciona blindagem. ISO/IEC 11801:2002.
Cat.7	F/FTP, S/FTP	600 MHz	Telefonia, CCTV, 1000BASE-TX no mesmo cabo. 10GBASE-T Ethernet.	Cabo blindado. ISO/IEC 11801 2nd Ed.
Cat.7a	F/FTP, S/FTP	1000 MHz	Telefonia, CATV, 1000BASE-TX no mesmo cabo. 10GBASE-T Ethernet.	Usa os 4 pares. ISO/IEC 11801 2nd Ed. Am. 2.
Cat.8.1	U/FTP, F/UTP	1600-2000 MHz	Telefonia, CATV, 1000BASE-TX no mesmo cabo. 40GBASE-T Ethernet.	Em desenvolvimento.
Cat.8.2	F/FTP, S/FTP	1600-2000 MHz	Telefonia, CATV, 1000BASE-TX no mesmo cabo. 40GBASE-T Ethernet.	Em desenvolvimento.

4.1.2 PADRÃO DE CORES

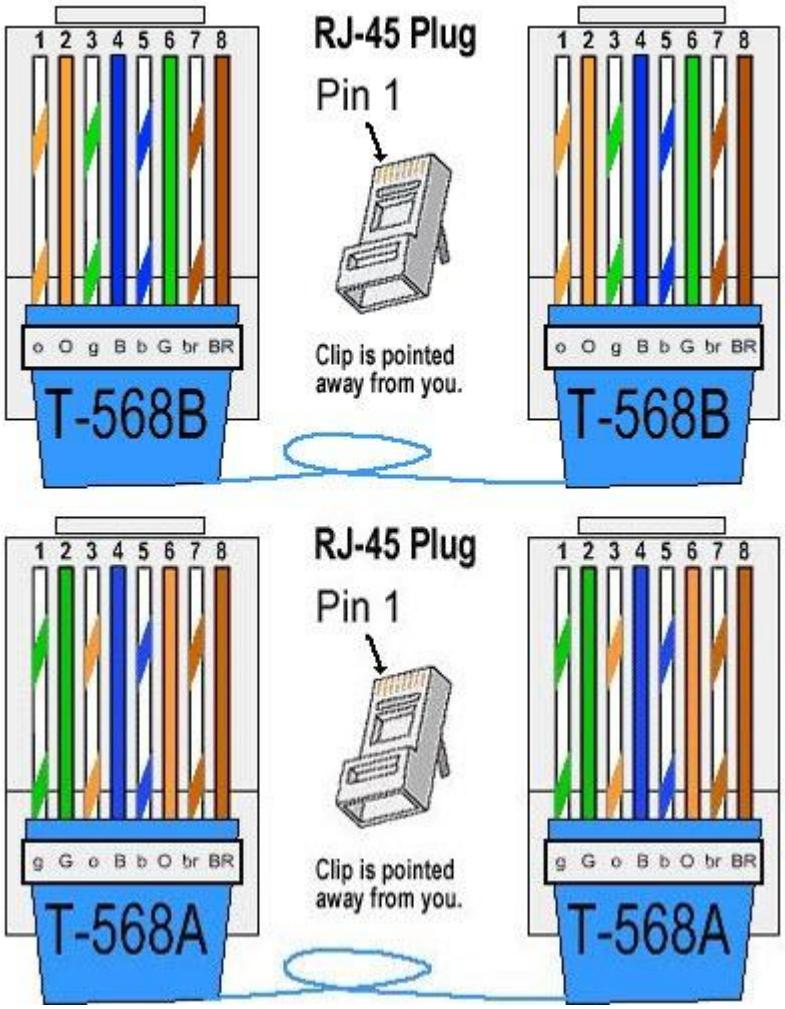
A norma EIA/TIA-568-B prevê duas montagens para os cabos, denominadas T568A e T568B.

A montagem T568A usa a sequência branca do verde, verde, branca do laranja, azul, branca do azul, laranja, branca do castanho, castanho.

A montagem T568B usa a sequência branca do laranja, laranja, branca do verde, azul, branca do azul, verde, branca do castanho, castanho.

As duas montagens são totalmente equivalentes em termos de desempenho, cabendo ao montador escolher uma delas como padrão para sua instalação. É boa prática que todos os cabos dentro de uma instalação sigam o mesmo padrão de montagem.

Um cabo cujas duas pontas usam a mesma montagem é denominado Direto (cabo), e serve para ligar estações de trabalho e roteadores a switches ou hubs. Um cabo em que cada ponta é usada uma das montagens é denominado Crossover, e serve para ligar equipamentos do mesmo tipo entre si.



4.1.3 FIBRA ÓTICA

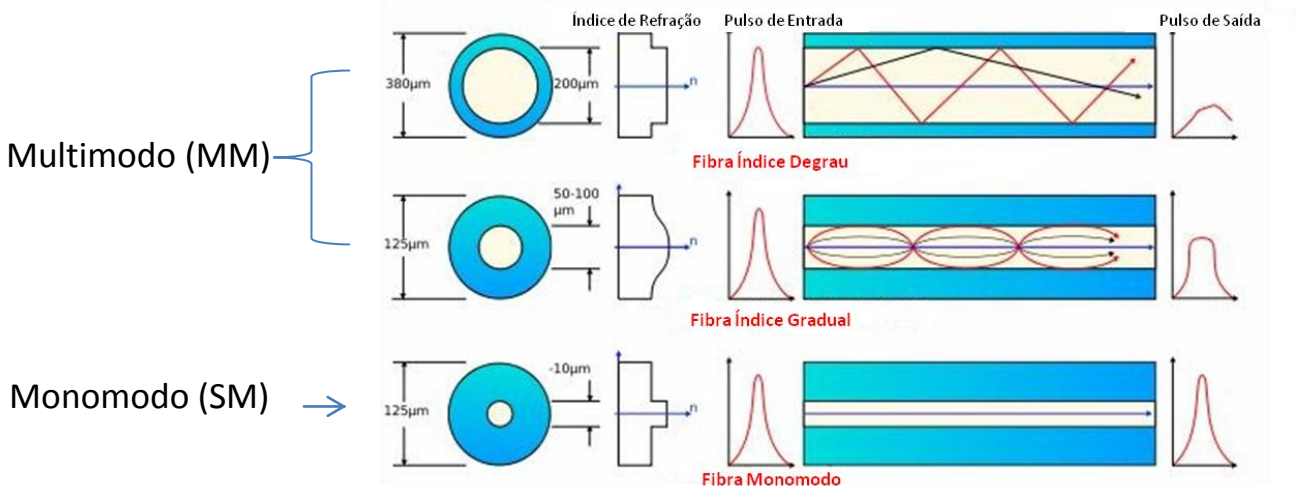
Fibra ótica é um filamento flexível e transparente fabricado a partir de vidro ou plástico extrudado e que é utilizado como condutor de elevado rendimento de luz, imagens ou impulsos codificados. Têm diâmetro de alguns micrómetros, ligeiramente superior ao de um cabelo humano. Por ser um material que não sofre interferências eletromagnéticas, a fibra ótica possui uma grande importância em sistemas de comunicação de dados.

Há dois tipos de denominação recorrentes às fibras óticas, os quais possuem características e finalidades próprias. Um deles é a fibra óptica **monomodo**. Esta apresenta um caminho possível de propagação e é a mais utilizada em transmissão a longas distâncias (devido a baixas perdas de informação). Já a fibra **multimodo**, permite a propagação da luz em diversos modos e é a mais utilizada em redes locais (LAN), devido ao seu custo moderado.

- Transmissão

Mesmo confinada a um meio físico, a luz transmitida pela fibra óptica proporciona o alcance de taxas de transmissão (velocidades) elevadíssimas, da ordem de 10^9 à 10^{10}bits por segundo (cerca de 40 Gbps), com baixa taxa de atenuação por quilômetro. Mas a velocidade de transmissão total possível ainda não foi alcançada pelas tecnologias existentes. Como a luz se propaga no interior de um meio físico, sofrendo ainda o fenômeno de reflexão, ela não consegue alcançar a velocidade de propagação no vácuo, que é de 300.000 km/segundo, sendo esta velocidade diminuída consideravelmente.

Para transmitir dados pela fibra ótica, são necessários equipamentos especiais, que contêm um componente foto emissor, que pode ser um diodo emissor de luz (LED) ou um diodo laser. O foto emissor converte sinais elétricos em pulsos de luz que representam os valores digitais binários (0 e 1). Tecnologias como WDM (CWDM e DWDM) fazem a multiplexação de vários comprimentos de onda em um único pulso de luz chegando a taxas de transmissão de 1,6 Terabits/s em um único par de fibras.



4.1.4 MODELOS DE CONECTORES

Abaixo alguns modelos de conectores de fibra óticas utilizados pelo mercado.

5. ETHERNET

Ethernet é uma arquitetura de interconexão para redes locais - Rede de Área Local (LAN) - baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a camada física, em 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.

Presume-se que ela tenha sido originalmente desenvolvida, a partir do projeto pioneiro atribuído a Xerox Palo Alto Research Center. Entende-se, em geral, que a Ethernet foi inventada em 1973, quando Robert Metcalfe escreveu um memorando para os seus chefes contando sobre o potencial dessa tecnologia em redes locais.[2] Contudo, Metcalfe afirma que, na realidade, a Ethernet foi concebida durante um período de vários anos. Em 1976, Metcalfe e David Boggs (seu assistente) publicaram um artigo, Ethernet: Distributed Packet-Switching For Local Computer Networks.Metcalfe deixou a Xerox em 1979 para promover o uso de computadores pessoais e redes locais (LANs), e para isso criou a 3Com. Ele conseguiu convencer DEC, Intel, e Xerox a trabalhar juntas para promover a Ethernet como um padrão, que foi publicado em 30 de setembro de 1980. Competindo com elas na época estavam dois sistemas grandemente proprietários, token ring e ARCNET. Em pouco tempo ambos foram afogados por uma onda de produtos Ethernet. No processo a 3Com se tornou uma grande companhia, e além de se ter tornado conhecida como U.S Robotics, também uma fabricante de processadores digitais.

5.1.1 CSMA/CD

CSMA/CD, do inglês Carrier Sense Multiple Access with Collision Detection, é um protocolo de telecomunicações que organiza a forma como os dispositivos de rede compartilham o canal utilizando a tecnologia Ethernet.

O CSMA/CD identifica quando a média está disponível (idle time) para a transmissão. Neste momento a transmissão é iniciada. O mecanismo CD (Collision Detection) ao mesmo tempo obriga que os nós escutem a rede enquanto emite dados, razão pela qual o CSMA/CD é também conhecido por (LWT) “Listen While Talk“ traduzido como "escute enquanto fala".

Se o mesmo detecta uma colisão, toda transmissão é interrompida e é emitido um sinal (“jam” de 48 bits) para anunciar que ocorreu uma colisão. Para evitar colisões sucessivas o nó espera um período aleatório e volta a tentar transmitir.

5.1.1.1 DETECÇÃO DAS COLISÕES

Como o CD tem a capacidade de “ouvir” enquanto “fala”, o mesmo compara se a amplitude do sinal recebido é a mesma do sinal enviado. Desta forma, quando se ouve algo diferente do que foi dito, é identificada uma colisão.

Colisões são consideradas um problema, ou um erro de transmissão, apenas quando ocorrem mais de 16 vezes consecutivas, ou seja, se um determinado nó tenta retransmitir um mesmo frame mais de 16 vezes, resultando sempre em uma colisão, então tal transmissão é cancelada passa a ser considerado um grande problema.

5.1.2 DOMÍNIO DE COLISÃO

O domínio de colisão é uma área lógica onde os pacotes podem colidir uns contra os outros, em particular no protocolo Ethernet. Quanto mais colisões ocorrem, menor é a eficiência da rede. Em uma rede comutada, todos os pacotes broadcast “transmitidos” são enxergados por todos os elementos conectados à rede, mesmo que um dispositivo não seja o destinatário.

Um domínio de colisão pode existir num único segmento da rede (como numa rede em barramento) ou numa porção ou total de uma rede maior (note-se que a utilização de hubs faz propagar o domínio de colisão a todos os seus segmentos). Em redes Ethernet, ao utilizar um hub, temos uma topologia lógica de barramento e as estações comportam-se como se estivessem todas ligadas em um único meio físico. Isso simplifica a transmissão de dados e reduz o investimento em equipamentos intermediários, mas em compensação traz um grave problema: as colisões de pacotes que ocorrem sempre que duas (ou mais) estações tentam transmitir dados ao mesmo tempo.

6. SWITCH

6.1 MAC

O endereço MAC (Media Access Control) é o endereço físico único de uma interface de rede. Todos os dispositivos que estão conectados à rede local Ethernet, possuem interfaces endereçadas: estações de trabalho, impressoras, roteadores e switches, etc. O IEEE controla o espaço de endereçamento Ethernet e distribui faixas de endereços aos fabricantes. Cada faixa consiste de um identificador de 24 bits (3 primeiros dos 6 bytes - pares hexadecimais), chamado “Organizationally Unique Identifier” (OUI). Cada fabricante adquire um ou mais OUIs e produz interfaces de rede cujos endereços são compostos do seu OUI concatenado com um número de 24 bits (3 últimos bytes) que identifica a interface. Apesar de ser único, praticamente todo hardware hoje permite a alteração do endereço MAC. Isso acontece devido ao fato de as interfaces de rede terem o MAC gravado em memória ROM, a qual é depois copiada para a RAM, com a inicialização da placa de rede, o que abre brechas para sua modificação. Tal modificação é conhecida como MAC spoofing, uma técnica em que se altera o endereço MAC, muitas vezes para fins maliciosos ilegais.

6.2 SPANNIG TREE

Spanning Tree Protocol (referido com o acrónimo STP) é um protocolo para equipamentos de rede que permite resolver problemas de loop em redes.

O protocolo STP possibilita a inclusão de ligações redundantes entre os computadores, 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.

Para isso, o algoritmo de Spanning Tree determina qual é o caminho mais eficiente (de menor custo) entre cada segmento separado por bridges ou switches. Caso ocorra um problema nesse caminho, o algoritmo irá recalcular entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente. O nome deriva do algoritmo spanning tree em teoria dos grafos.

6.2.1 BRIDGE PROTOCOL DATA UNITS (BPDUS)

Para viabilizar o cálculo do caminho de menor custo, é necessário que cada comutador tenha conhecimento de toda a topologia da rede. A disponibilidade dessas informações é assegurada pela troca de quadros especiais chamados BPDUs - Bridge Protocol Data Units - entre os comutadores. Os BPDUs são frames enviados para troca de informações tais como o bridge ID e o custo de caminho de um nó para a raiz. O frame BPDU utiliza o endereço único MAC unicast da porta como endereço de origem, e o endereço de destino é o endereço MAC multicast da Spanning Tree.

6.2.2 OPERAÇÃO DA SPANNING TREE

1) Eleição de um switch root, quando haverá apenas este switch root na rede. Neste elemento, todas as portas são designadas (designated ports), estando preparadas para o envio e recepção de tráfego.

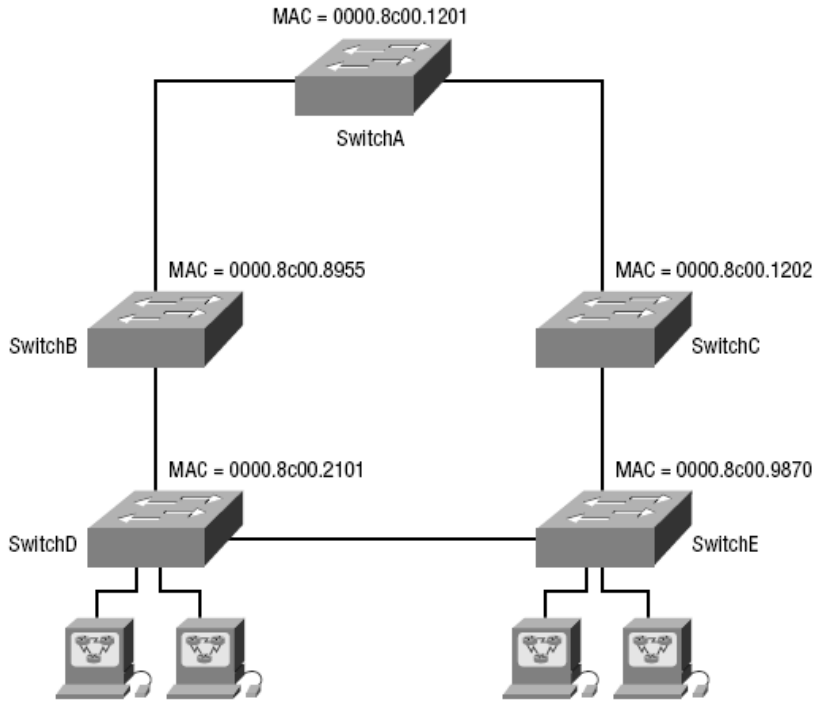
2) O STP seleciona uma porta root nos switches nonroot: esta porta é que apresentar o menor custo em conexão com o root switch.

3) Em cada segmento é designada uma porta, cada porta é selecionada no elemento que tenha o menor custo no caminho em direção ao root. As portas não designadas estão em estado “bloqueado” para justamente interromper o loop.

4) Os switches trocam mensagens de configuração entre si em intervalos regulares de 2 segundos.

5) Os switches trocam esta mensagem usando frames multicast, chamados bridge protocol data unit (BPDU). Este quadro carrega também a informação de bridge ID (BID).

6) O BID é formado por uma prioridade (2 bytes) e um bridge MAC address (6 bytes). A prioridade, de acordo com o IEEE 802.1D, é 32.768 sendo um valor default para todos os switches, a menos que este valor seja manipulado. O switch root, por default, é o que tiver menor BID.



6.2.3 STATUS POSSÍVEIS DAS PORTAS:

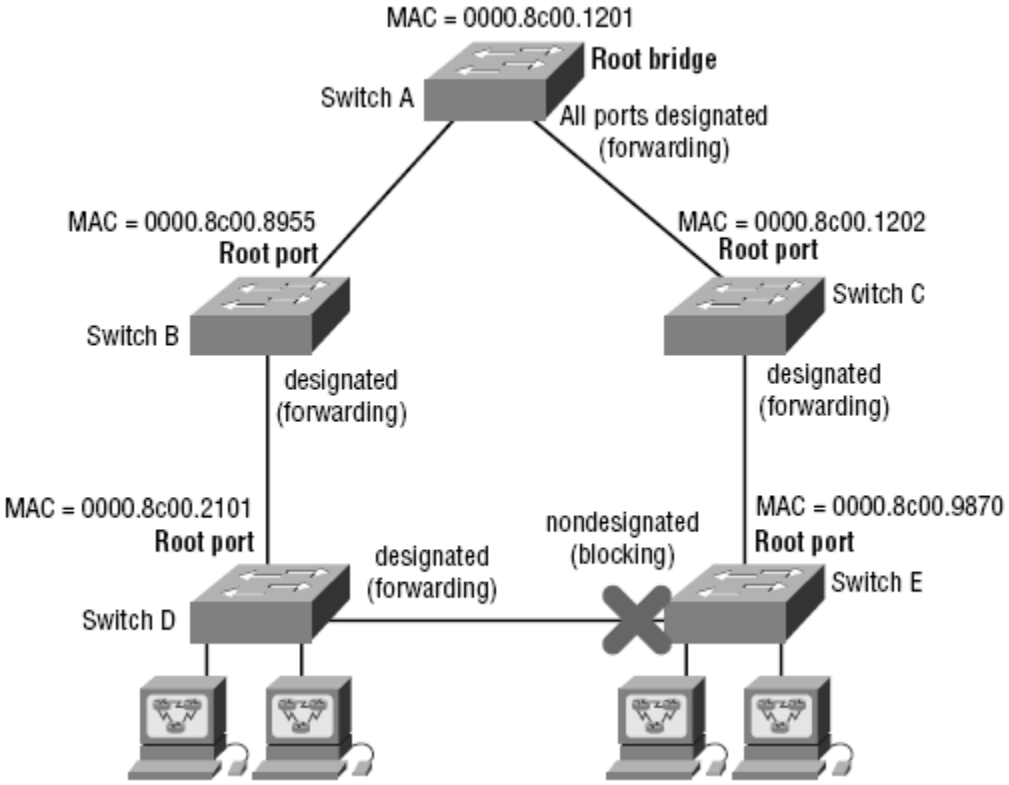
Blocking – Estado inicial de todas as portas ao iniciar o mecanismo STP, aguardando BPDUs;

Listening – Nesta etapa, é feita a seleção do root, são selecionadas as portas roots e os elementos nonroot, além de serem designadas as portas em cada segmento. O tempo gasto na mudança de estado entre listening e learning é chamado de foward delay e tem valor default de 15 segundos.

Learning and forwarding - Caso a porta seja designated ou uma porta root no final do estado de aprendizado, a porta mudará para o estado de forwarding (envia e recebe dados). Outras portas entrarão em estado blocked.

Blocked – A transição de blocked para forwarding ocorre entre 30 e 50 segundos.

A convergência ocorre quando as portas já realizaram as transições de estado e já foram classificadas, estando disponíveis ou bloqueadas. A convergência é necessária para a operação normal da rede.



6.3 VLAN

Dentro de uma rede de computadores, uma VLAN é quando você cria uma separação entre partes da rede. Você literalmente divide a rede em pedaços separados, aonde um pedaço não fala com o outro (pelo menos não diretamente). Assim temos um único switch que se conecta a todos os computadores da rede, porém o administrador informa ao switch quais computadores (ou impressoras, servidores, telefones IP, etc.) se falam diretamente e quais não podem se falar.

A VLAN tem como sua função básica a separação das redes. Antes da criação de VLANs todos os elementos da rede se falavam e se escutavam. Em uma rede muito grande, isso gerava um domínio de colisão muito grande, que podia chegar até a parada total da rede. Além disso, como todos escutavam uns aos outros a segurança das informações na rede ficam mais comprometidas.

Com a utilização dos switches, passou-se a poder criar redes locais virtuais (Virtual LAN). Isto significa que dentro de um switch, podemos criar várias redes virtuais, ou seja, domínio de colisão específico para sua função (Servidores, Usuários, Impressoras, etc). Com isso um problema gerado em uma VLAN não será propagado para outra VLAN.

Vantagens do uso de VLAN:

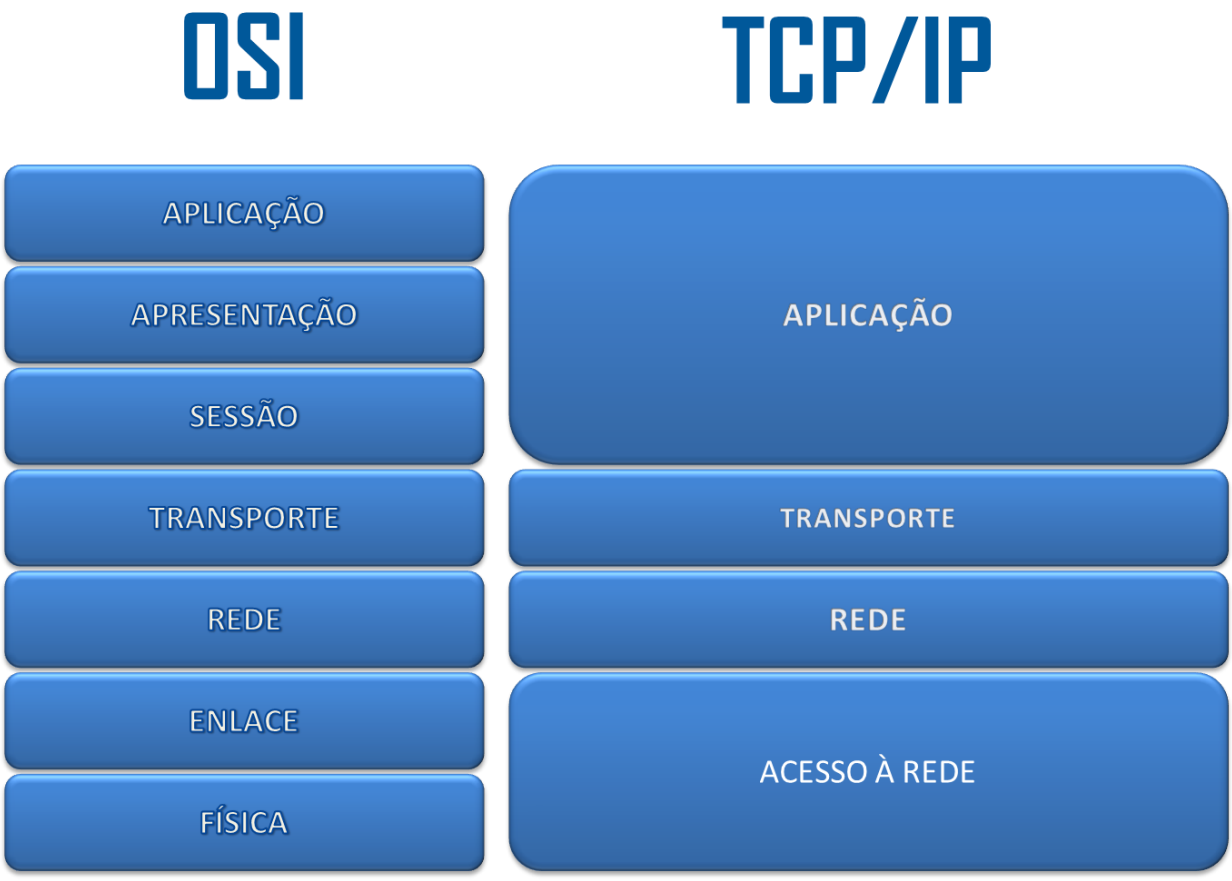
- Redução do tamanho e aumento do número de domínio de broadcast;
- Agrupamento lógico de usuários (Contabilidade, Presidência, Engenharia) e de recursos (Impressoras, Servidores, Câmeras);
- Organização por localidade;
- Melhor gerencia e aumento de segurança da rede local;
- Flexibilidade e escalabilidade.

7. PROTOCOLO

7.1 TCP/IP

O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI), onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração.

Em comparação ao modelo OSI o modelo TCP/IP está dividido em apenas quatro camadas:



Camada de aplicação (FTP, SMTP, TELNET, HTTP, HTTPS, etc)

Camada de transporte (TCP, UDP, etc)

Camada de rede (IP)

Camada física (Ethernet, etc)

7.2 IP

O endereço IP é uma sequência de números composta de 32 bits. Esse valor consiste em um conjunto de quatro sequências de 8 bits. Cada uma destas é separada por um ponto e recebe o nome de octeto ou simplesmente byte, já que um byte é formado por 8 bits. O número 172.31.110.10 é um exemplo. Cada octeto é formado por números que podem ir de 0 a 255, não mais do que isso. A divisão de um IP em quatro partes facilita a organização da rede.

Para que seja possível existir tantos IPs para uso em redes locais quanto para utilização na internet, contamos com um esquema de distribuição estabelecido pelas entidades IANA (Internet Assigned Numbers Authority) e ICANN (Internet Corporation for Assigned Names and Numbers) que, basicamente, divide os endereços em três classes principais e mais duas complementares. São elas:

- Classe A: 0.0.0.0 até 127.255.255.255 - permite até 128 redes, cada uma com até 16.777.214 dispositivos conectados;
- Classe B: 128.0.0.0 até 191.255.255.255 - permite até 16.384 redes, cada uma com até 65.536 dispositivos;
- Classe C: 192.0.0.0 até 223.255.255.255 - permite até 2.097.152 redes, cada uma com até 254 dispositivos;
- Classe D: 224.0.0.0 até 239.255.255.255 - multicast;
- Classe E: 240.0.0.0 até 255.255.255.255 - multicast reservado.

7.2.1 ENDEREÇOS IP PRIVADOS

Existem conjuntos de endereços das classes A, B e C que são privados. Isto significa que eles não podem ser utilizados na internet, sendo reservados para aplicações locais. São, essencialmente, estes:

- Classe A: 10.0.0.0 à 10.255.255.255;
- Classe B: 172.16.0.0 à 172.31.255.255;
- Classe C: 192.168.0.0 à 192.168.255.255.

7.3 ENTENDA ENDEREÇOS IP

Um endereço IP é um endereço usado para identificar exclusivamente um dispositivo em uma rede IP. O endereço é constituído por 32 bits binários, que podem ser divisíveis em uma porção de rede e a porção de alojamento com a ajuda de uma máscara de sub-rede. Os 32 bits são divididos em quatro octetos (1 octeto = 8 bits). Cada octeto é convertido em decimal e separados por um ponto. Por esta razão, um endereço IP é expresso em formato decimal pontilhado (por exemplo, 172.16.81.100). O valor em cada octeto varia de 0 a 255 decimal, ou 00000000 - 11111111binário.

Aqui está como binários são convertidos para decimal: O bit mais a direita, ou bit menos significativo, de um octeto tem um valor de 2^0. O bit mais a esquerda têm um valor de 2^1. Isto continua até que a o bit mais a esquerda, ou bit mais significativo, o qual tem um valor de $2^{7.}$ Assim, se todos os bits forem um, o equivalente decimal seria 255, como mostrado aqui:

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)

Aqui é uma amostra de conversão de octeto quando nem todos os bits são definidos como 1.

0 1 0 0 0 0 0 1

0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)

E este exemplo mostra um endereço IP representado em ambos binários e decimais.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

7.3.1 MÁSCARA DE REDE

A máscara de rede especifica a gama de IPs (domínio de colisão) que pode ser abrangida por um determinado endereço, e é especialmente necessária no processo de encaminhamento (*routing*). Ainda, com simples cálculos, pode-se gerir eficientemente o espaço de endereçamento disponível, o que nos primeiros tempos da existência da Internet era muito importante, já que os endereços eram alugados em grupos.

A notação formal de uma máscara de rede é o formato típico de um endereço IP e, aplicada com uma operação AND sobre um endereço IP, devolve a rede a que este pertence. Por exemplo,

```
Host   192.168. 20.5    =     11000000.10101000.00010100.00000101
Mask  255.255.255.0    =     11111111.11111111.11111111.00000000
 ------------ ----------------------------------------------------------------------------
Rede  192.168. 20.0    =     11000000.10101000.00010100.00000000
```

Ou seja, o IP 192.168.20.5 pertence, aparentemente, à rede 192.168.20.0. Para simplificar a representação, convencionou-se que a máscara de rede poderia acompanhar o IP especificando o número de bits '1' contíguos, separada por uma barra '/'. Por exemplo, a rede anterior podia ser representada como 192.168.20.0/24.

O espaço de endereçamento também é ditado pela máscara de rede, e é equivalente à negação dos seus bits a '0', excetuando o primeiro e último endereço (endereços de rede e *broadcast*, respectivamente). Por exemplo, uma máscara de 255.255.255.192 irá disponibilizar 62 endereços.

A utilização da máscara de rede foi particularmente útil numa altura em que era comum alugar blocos de endereços IP. Os operadores tinham, assim, que distinguir nos seus routers cada um desses blocos, isso era feito através da máscara de rede.

Suponha-se que dispomos dos seguintes endereços: de 192.168.10.0 a 192.168.10.255, e que existem cinco clientes interessados. Os requisitos de cada um deles são:

Cliente	Quantidade
A	65
B	24
C	4
D	8
E	12

Pelas nossas contas, vamos precisar de 65+24+4+6+12=111 endereços, tendo que organizar a nossa rede em função dos blocos associados.

- Para A vamos precisar de 65 endereços. Como os blocos funcionam em potências de 2, iremos reservar uma rede de 128 endereços.
- Para B será suficiente uma de 32.
- Para C deverá ser uma rede de 8, já que os 4 oferecidos pelo bloco imediatamente inferior corresponderiam, na verdade, a 2 endereços utilizáveis.
- Para D idem — uma rede de 8.
- Para E seria necessário uma rede de 16 endereços.

Vamos verificar as contas: 128+32+8+8+16=192<256, pelo que podemos satisfazer todos os clientes com a nossa pequena rede. Em termos de divisão,

```
Rede A: 192.168.10.  0 / 25 = 255.255.255.128  (0-127)
Rede B: 192.168.10.128 / 27 = 255.255.255.224  (128-159)
Rede C: 192.168.10.160 / 29 = 255.255.255.248  (160-167)
Rede D: 192.168.10.168 / 29 = 255.255.255.248  (168-175)
Rede E: 192.168.10.176 / 28 = 255.255.255.240  (176-191)
```

Pelas contas anteriores e olhando para a nossa divisão, sabemos que o IP 192.168.10.163/29 iria pertencer ao cliente C. Vamos verificar:

```
  192.168. 10.163    =    11000000.10101000.00001010.10100011
& 255.255.255.248    =    11111111.11111111.11111111.11111000
 --------------- -----------------------------------
  192.168. 10.160    =    11000000.10101000.00001010.10100000
```

e que o IP 192.168.10.169/29 iria pertencer ao cliente D:

```
  192.168. 10.169    =    11000000.10101000.00001010.10101001
& 255.255.255.248    =    11111111.11111111.11111111.11111000
 --------------- -----------------------------------
  192.168. 10.168    =    11000000.10101000.00001010.10101000
```

E também podemos verificar que ainda nos sobra espaço para uma rede de 64 endereços. Esta rede é o subespaço que sobrou das contas anteriores: 192+64=256! Agora, podemos facilmente deduzir que a rede seria 192.168.10.192/26.

7.4 ROTEAMENTO

Em termos gerais, o roteamento é o processo de encaminhar pacotes entre redes conectadas. Para redes baseadas em TCP/IP, o roteamento faz parte do protocolo IP e é usado em combinação com outros serviços de protocolo de rede para fornecer recursos de encaminhamento entre hosts localizados em segmentos de rede diferentes em uma rede maior baseada em TCP/IP.

Existem dois modos de administração da tabela de roteamento e são conhecidos como: roteamento estático e roteamento dinâmico.

7.4.1 ROTEAMENTO ESTÁTICO

O roteamento estático normalmente é configurado quando uma tabela de roteamento estático é construída manualmente pelo administrador do sistema, uma rede com um número limitado de roteadores para outras redes poderem ser configuradas com roteamento estático, e pode ou não ser divulgada para outros dispositivos de roteamento na rede. Tabelas estáticas não se ajustam automaticamente à alterações na rede, portanto devem ser utilizadas somente onde as rotas não sofrerem alterações. Algumas vantagens do roteamento estático são melhor controle e segurança obtida pela divulgação somente das rotas necessárias e também a redução do broadcast, multicast ou unicast flooding introduzidos na rede pela troca de mensagens dos protocolos de roteamento dinâmicos.

7.4.2 ROTEAMENTO DINÂMICO

Diferentemente do roteamento estático onde a tabela de rotas é informada manualmente, no roteamento dinâmico os próprios roteadores decidem por qual caminho deverão enviar as informações. Baseado em parâmetros previamente configurados. Essas decisões são baseadas de duas formas basicamente, chamadas de Link State ou Distance Vector.

Os principais protocolos de roteamento dinâmico são: RIP, OSPF, BGP, EIGRP (cisco)

Questões comuns a qualquer algoritmo de roteamento:

- Determinação de caminho (path determination)
- Métrica(metrics)
- Número de saltos (hop count)
- Largura de banda (bandwidth)
- Carga (load)
- Retardo (delay)
- Alcançabilidade (reachability)
- Custo (cost)
- Convergência (convergence)

7.5 GATEWAY

Para que um host de uma rede consiga falar com outro host em outra rede, é necessário que haja um gateway configurado em ambos os hosts. Gateway é o host intermediário geralmente destinado a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos. Como exemplos de gateway têm os routers (ou roteadores) e firewalls, já que ambos servem de intermediários entre o utilizador e a rede. Um proxy também pode ser interpretado como um gateway (embora em outro nível), já que serve de intermediário também.

Cabe ao gateway traduzir e adaptar os pacotes originários da rede de origem para que estes possam atingir o destinatário, mas também traduzir as respostas e devolvê-las.

7.6 DHCP

O DHCP, Dynamic Host Configuration Protocol (Protocolo de configuração dinâmica de host), é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, Máscara de sub-rede, Default Gateway (Gateway Padrão), Número IP de um ou mais servidores DNS, Sufixos de pesquisa do DNS entre outras informações.

Resumidamente, o DHCP opera da seguinte forma:

Um cliente envia um pacote UDP em broadcast (destinado a todas as máquinas) com uma requisição DHCP (para a porta 67);

O servidor DHCP que capturar este pacote irá responder (se o cliente se enquadrar numa série de critérios) para a porta UDP 68 do Host solicitante com um pacote contendo configurações onde constará, pelo menos, um endereço IP, uma máscara de rede e outros dados opcionais, como o gateway, servidores de DNS, etc...

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede.

7.7 DNS

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

Ou seja, os servidores de diretórios responsáveis por prover informações como nomes e endereços das máquinas são normalmente chamados servidores de nomes. Na Internet, o serviço de nome usado é o DNS, que apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta. Um recurso da internet, um site da Web, pode ser identificado de duas maneiras: pelo seu nome de domínio, “www.g1.com.br” ou pelo endereço de IP dos equipamentos que o hospedam “186.192.90.5”. Endereços de IP são usados pela camada de rede para determinar a localização física e virtual do equipamento. Nomes de domínio, porém, são mais mnemônicos para o usuário e empresas. É então necessário um mecanismo para traduzir um nome de domínio em um endereço IP. Esta é a principal função do DNS.

8. TROUBLESHOOTING

Troubleshooting é uma forma de resolver problemas, muitas vezes aplicada na reparação de produtos ou processos falhados. É uma busca sistemática e lógica pela raiz de um problema, de modo a que possa ser resolvido e o produto ou processo possa ficar novamente operacional.

Na pesquisa da solução de um problema de rede normalmente utilizamos alguns programas (ferramentas) que nos auxiliam na identificação dos problemas. Podemos utilizar o “Ping”, “Tracer route”, “Nslookup”, “Telnet” e “arp cache”.

Quando começamos uma análise de um problema devemos verificar algumas questões

8.1 PING

O ping é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos. É um comando disponível praticamente em todos os sistemas operacionais. Seu funcionamento consiste no envio de pacotes para o equipamento de destino e na "escuta" das respostas. Se o equipamento de destino estiver ativo, uma "resposta" (o "pong", uma analogia ao famoso jogo de ping-pong) é devolvida ao computador solicitante.

Exemplo 1:
D:\Users>ping 10.68.11.1

Disparando 10.68.11.1 com 32 bytes de dados:
Resposta de 10.68.11.1: bytes=32 tempo=1ms TTL=255
Resposta de 10.68.11.1: bytes=32 tempo=1ms TTL=255
Resposta de 10.68.11.1: bytes=32 tempo=1ms TTL=255
Resposta de 10.68.11.1: bytes=32 tempo=1ms TTL=255

Estatísticas do Ping para 10.68.11.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 1ms, Média = 1ms

8.2 TRACEROUTE

Traceroute é uma ferramenta de diagnóstico que rastreia a rota de um pacote através de uma rede de computadores utilizando os protocolos IP e o ICMP. Como resultado ele irá mostrar o nós por onde o pacote passará até o seu destino final. Também mostrará o tempo de resposta de todos os nós. Caso algum roteador no caminho não saiba chegar ao destino solicitado, um asterisco será mostrado como resposta.

```
$traceroute wikipedia.org
traceroute to wikipedia.org (66.230.200.100), 64 hops max, 44 byte packets
 1  124.ae0.xr1.3d12.xs4all.net (194.109.21.1)  0.305 ms  0.360 ms  0.405 ms
 2  0.so-6-0-0.xr1.tc2.xs4all.net (194.109.5.10)  0.634 ms  0.716 ms  0.673 ms
 3  ams-ix-c00.wvfiber.net (195.69.145.58)  0.638 ms  0.601 ms  0.551 ms
 4  lon-c00-pos-4-0.OC48-ams-pos11-0.wvfiber.net (63.223.28.201)  7.512 ms  7.427 ms  7.494 ms
 5  nyc60-pos-1-0.OC48-lon-c00-pos-3-0.wvfiber.net (63.223.28.145)  84.108 ms  83.804 ms  83.995 ms
 6  66.216.1.181 (66.216.1.181)  83.435 ms  83.278 ms  83.348 ms
 7  ash-c01-tge-3-3.TG-nyc-c01-1-1.wvfiber.net (66.216.1.161)  89.563 ms  89.554 ms  89.551 ms
 8  atl-c01-tge-3-1.TG-ash-c01-3-1.wvfiber.net (66.216.1.157)  103.701 ms  103.606 ms  103.596 ms
 9  cpp-hostway.wvfiber.net (63.223.8.26)  103.678 ms  103.609 ms  103.630 ms
10  e1-12.co2.as30217.net (64.156.25.105)  113.014 ms  113.044 ms  113.084 ms
11  10ge5-1.csw5-pmtpa.wikimedia.org (84.40.25.102)  113.153 ms  113.251 ms  113.180 ms
12  rr.pmtpa.wikimedia.org (66.230.200.100)  113.069 ms  113.172 ms  113.003 ms
```

8.3 NSLOOKUP - RESOLUÇÃO DE NOMES

Através do NSLOOKUP podemos fazer a verificação da resolução de nome de um domínio, host ou IP. nslookup é uma ferramenta, comum ao Windows e ao Linux, utilizada para se obter informações sobre registros de DNS de um determinado domínio, host ou IP.

Exemplo de nslookup para o domínio WIKIPEDIA.ORG

>nslookup wikipedia.org

Server: UnKnown

Address: 192.168.0.100

Non-authoritative answer:

Name = wikipedia.org

Address: 66.230.200.100

Em uma busca nslookup padrão, o servidor DNS do provedor de acesso é consultado, e retorna as informações sobre o domínio ou host pesquisado.

A informação "Non-authoritative answer" (Não é resposta de autorização) significa que o servidor DNS do provedor de acesso não responde por este domínio, em outras palavras, isto significa que uma consulta externa foi realizada, aos servidores DNS do domínio WIKIPEDIA.ORG.

Exemplo de nslookup para o mesmo domínio WIKIPEDIA.ORG, agora realizando a consulta diretamente ao servidor DNS deste domínio, NS1.WIKIMEDIA.ORG:

>nslookup wikipedia.org NS1.WIKIMEDIA.ORG

Servidor: UnKnown

Address: 211.115.107.190

Nome = wikipedia.org

Address: 66.230.200.100

Note que a informação "Não é resposta de autorização" não aparece mais. Isto ocorre, pois agora, ao invés do servidor DNS do provedor de acesso local, foi consultado o servidor DNS que possui os registros do domínio WIKIPEDIA.ORG.

8.4 TESTE DE PORTA

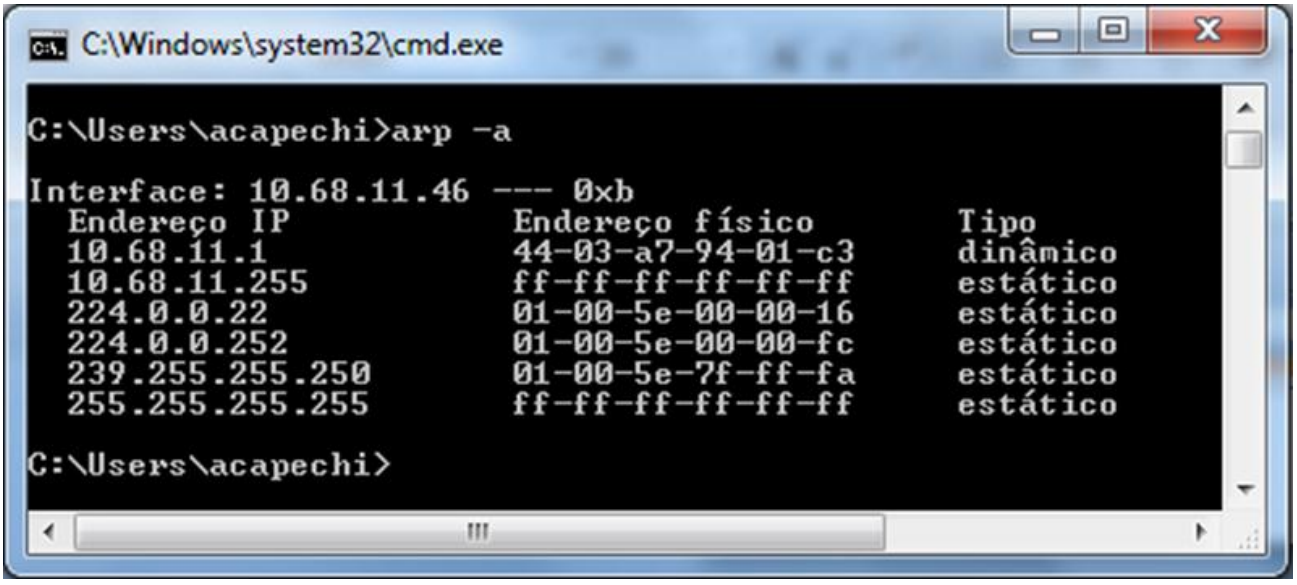
Para verificar se uma conexão está sendo realizada ou não, podemos executar um telnet no endereço de destino direcionando a porta que precisa ser testada.

Por exemplo: se quisermos testar uma conexão de uma página web podemos rodar um programa telnet direcionando para a porta 80.

8.5 ARP

Address Resolution Protocol ou ARP é um protocolo usado para encontrar um endereço da camada de ligação de dados (Ethernet, por exemplo) a partir do endereço da camada de rede (como um endereço IP). O emissor difunde em broadcast um pacote ARP contendo o endereço IP de outro host e espera uma resposta com um endereço MAC respectivo. Cada máquina mantém uma tabela de resolução em cache para reduzir a latência e carga na rede. O ARP permite que o endereço IP seja independente do endereço Ethernet, mas apenas funciona se todos os hosts o suportarem.

No Windows podemos utilizar o comando “arp –a” para tentar identificar o endereço mac de IP.



9. WIRELESS

9.1 Wi-Fi (IEEE 802.11)

Wi-Fi é uma marca registrada da *Wi-Fi Alliance*. É utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios (WLAN) baseados no padrão IEEE 802.11. Por causa do relacionamento íntimo com seu padrão de mesmo nome, o termo *Wi-Fi* é usado frequentemente como sinônimo para a tecnologia IEEE 802.11. O nome, para muitos, sugere que se deriva de uma abreviação de *wireless fidelity*, ou "fidelidade sem fio", mas não passa de uma brincadeira com o termo *Hi-Fi*, designado para qualificar aparelhos de som com áudio mais confiável, que é usado desde a década de 1950.

Wifi é um tipo de rede sem fio, em que se permite por meio de ondas de rádio conectar-se a internet e transmitir dados de dispositivo para outro, Wifi é a rede sem fio mais utilizada no mundo, pois, tem uma boa criptografia (WPA/WPA2, WPA-PSK/WPA2-PSK e WEP), a criptografia mais usada é a WPA/WPA2 e WPA-PSK/WPA2-PSK, que garantem uma boa segurança para rede. O Wifi pode ter um alcance muito grande, mas, isso vai depender do aparelho transmissor da rede, hoje em dia Wifi tem duas frequências muito conhecidas que são a 2.4 ghz e 5.1 ghz.

Os principais padrões na família IEEE 802.11 são:

IEEE 802.11a: Padrão Wi-Fi para frequência 5 GHz com capacidade teórica de 2 Mbps.

IEEE 802.11b: Padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 11 Mbps. Este padrão utiliza DSSS (Direct Sequency Spread Spectrum – Sequência Direta de Espalhamento de Espectro) para diminuição de interferência.

IEEE 802.11g: Padrão Wi-Fi para frequência 2,4 GHz com capacidade teórica de 54 Mbps.

IEEE 802.11n: Padrão Wi-Fi para frequência 2,4 GHz e/ou 5 GHz com capacidade de 150 a 600 Mbps. Esse padrão utiliza como método de transmissão MIMO-OFDM.

IEEE 802.11ac: ou Padrão 802.11ac é a nova geração da tecnologia de transmissão em redes locais sem fio (WI-FI WLAN) pertencentes a família 802.11 de alto desempenho, na frequência de 5GHz.

Este padrão foi desenvolvido entre 2011 e 2013, com previsão de lançamento somente para o início de 2014. O Padrão Trabalha com multiestações de transferência sem-fio de na escala de Gbit/s em link único de transferência, graças ao conceito de extensão de interface, já implementado no modelo 802.11n.

10. Bluetooth *(IEEE 802.15.1)*

Bluetooth consiste de uma pequena rede, chamada piconet, com um nó mestre e até sete nos escravos ativos (pode haver até 255 escravos não ativos), em uma distancia de 10m (podem existir varias piconets em um mesmo ambiente conectadas por um no de ponte, formando uma scatternet).

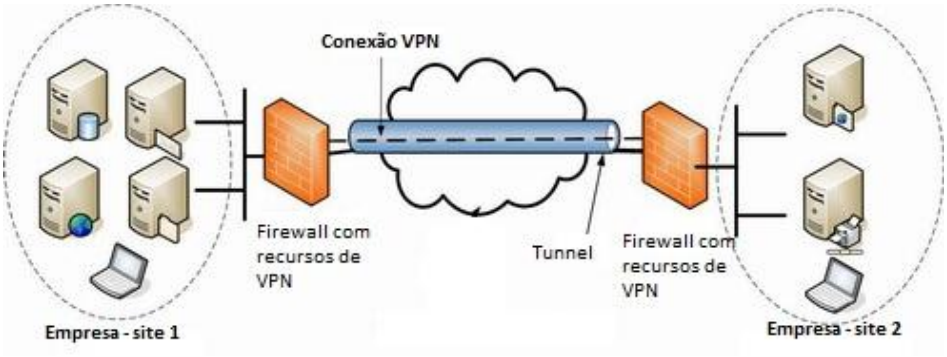
A comunicação é sempre feita mestre-escravo, não sendo possível a comunicação entre escravos. Opera na faixa de 2.4GHz, com taxa de dados bruta de 1Mbps.

11. VPN

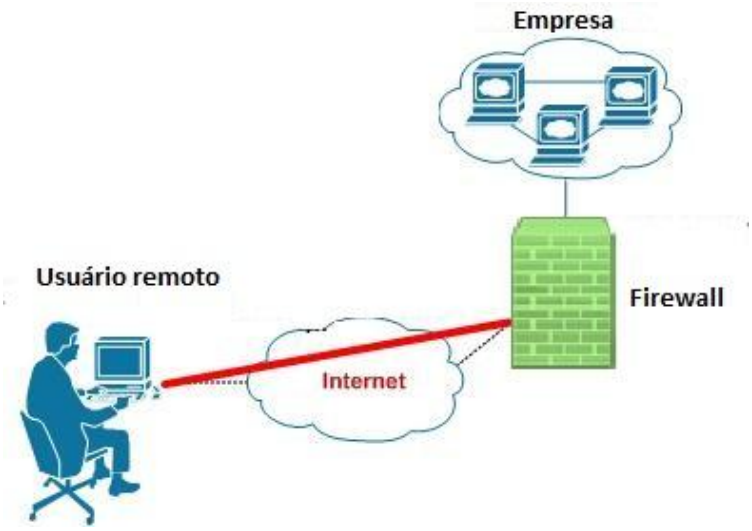
Virtual Private Network – Redes virtuais privadas

- Estabelece um canal seguro entre dois pontos. Aplicável para conectar áreas distantes da empresa, acessos de *home office*, acesso de empresas parceiras e acessos remotos . Foco em segurança, escalabilidade e disponibilidade.
- VPN é uma conexão que utiliza encriptação entre redes privadas utilizando, por exemplo, uma rede pública como a Internet.
- Pode utilizar duas técnicas: tunelamento e criptografia (assunto que será tratado na matéria de Segurança).
- Descrita na RFC 1918.
- É possível utilizar endereços privados diretamente em VPNs.
- Para equipamentos presentes na rede interna terem acesso à internet, o duplo endereçamento será necessário, assim como a tradução de endereços.
- Há dois tipos de VPN:

- *Site-to-site* – Os *hosts* normalmente não dispõem de um cliente VPN, e o tráfego é enviado através de um "gateway" VPN, que pode ser um roteador, um *firewall* ou outro equipamento com capacidade para tal. Este "gateway" é responsável por encapsular e encriptar o tráfego de saída e enviá-lo através de um túnel VPN na internet para o outro no destino. Ao ser recebido, o "gateway" abre o pacote, retirando os cabeçalhos do tunelamento e retira a codificação de segurança para entregar ao equipamento de destino.



- Acesso remoto – Atende a necessidade de usuários móveis conectando usuários individuais à rede alvo. Neste caso, o equipamento que necessita realizar conexão dispõe de um software cliente instalado. Este aplicativo é responsável por realizar o encapsulamento e encriptação antes de enviar o fluxo pela internet ao *gateway* VPN da rede destino. Neste ponto, o processo do gateway VPN é o mesmo do descrito no *site-to-site*.



12. NAT (Network Address Translation)

A conversão de endereços de rede (NAT) permite converter endereços IPv4 de computadores em uma rede em endereços IPv4 de computadores em outra rede. Um roteador IP com recurso de NAT instalado no ponto de conexão entre uma rede privada (como a rede de uma empresa) e uma rede pública (como a Internet), permite aos computadores da rede privada acessar os computadores da rede pública, graças ao serviço de conversão oferecido.

A tecnologia NAT foi desenvolvida para oferecer uma solução temporária para a escassez de endereços IPv4. O número de endereços IPv4 únicos disponíveis globalmente (ou seja, públicos) é pequeno demais para acomodar o número crescente de computadores que precisa acessar a Internet. Embora já exista uma solução em longo prazo — o desenvolvimento de endereços IPv6 — IPv6 ainda não é amplamente adotado. A tecnologia NAT permite aos computadores de qualquer rede usar endereços privados reutilizáveis para conectar a computadores com endereços públicos na Internet.

13. IPV6

13.1 Esgotamento dos endereços IPv4

As especificações do IPv4 reservam 32 bits para endereçamento, o que possibilita gerar mais de 4 bilhões de endereços distintos. Inicialmente, estes endereços foram divididos em três classes de tamanhos fixos da seguinte forma:

Classe A: definia o bit mais significativo como 0, utilizava os 7 bits restantes do primeiro octeto para identificar a rede, e os 24 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 1.0.0.0 até 126.0.0.0;

Classe B: definia os 2 bits mais significativo como 10, utilizava os 14 bits seguintes para identificar a rede, e os 16 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 128.1.0.0 até 191.254.0.0;

Classe C: definia os 3 bits mais significativo como 110, utilizava os 21 bits seguintes para identificar a rede, e os 8 bits restantes para identificar o host. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0;

Classe	Formato	Redes	Hosts
A	7 bits Rede, 24 bits Host	128	16.77.216
B	14 bits Rede, 16 bits Host	16.384	66.536
C	21 bits Rede, 8 bits Host	2.097.152	256

Embora o intuito dessa divisão tenha sido tornar a distribuição de endereços mais flexível, abrangendo redes de tamanhos variados, esse tipo de classificação mostrou-se ineficiente. A classe A atendia um número muito pequeno de redes e ocupava metade de todos os endereços disponíveis, enquanto que a classe C permitia criar muitas redes só que com poucos endereços disponíveis. Em outras palavras, ao mesmo tempo em que algumas classes acarretavam desperdícios, as outras não supriam a necessidade de endereços disponíveis. Para exemplificar o problema, imagine que se precise endereçar 300 dispositivos em uma rede. Nessa situação seria necessário obter um bloco de endereços da classe B, desperdiçando assim quase o total dos 65 mil endereços.

Outro fator que colaborava com o desperdício de endereços, foi a politica de distribuição de faixas classe A, as quais foram atribuídas integralmente a grandes instituições como IBM, AT&T, Xerox, HP, Apple, MIT, Ford, Departamento de Defesa Americano, entre muitas outras. Isso disponibilizava para cada uma 16.777.216 milhões de endereços que dificilmente seriam usadas por completo. Para complicar a situação, 35 faixas de endereços classe A foram reservadas para usos específicos como multicast, loopback e uso futuro.

Em 1990, já existiam 313.000 hosts conectados a rede e estudos já apontavam para um colapso devido a falta de endereços. Além disso, outros problemas também tornavam-se mais efetivos conforme a Internet evoluía, como o aumento da tabela de roteamento.

Devido ao ritmo de crescimento da Internet e da política de distribuição de endereços, em maio de 1992, 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C, já estavam alocados. Nesta época, a rede já possuía 1.136.000 hosts conectados.

Em 1993, com a criação do protocolo HTTP e a liberação por parte do Governo estadunidense para a utilização comercial da Internet, houve um salto ainda maior na taxa de crescimento da rede, que passou de 2.056.000 de hosts em 1993 para mais de 26.000.000 de hosts em 1997.

Diante desse cenário, a IETF (Internet Engineering Task Force) passa a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento. Então foram criadas algumas técnicas com o intuito de tentar resolver esse problema CIDR, DHCP e NAT. Porém nenhuma dessas técnicas conseguiu solucionar o problema, somente atrasá-lo um pouco.

13.2 Características IPv6

O endereçamento no IPv6 é de 128 bits, e inclui prefixo de rede e sufixo de *host*. No entanto, não existem classes de endereços, como acontece no IPv4. Assim, a fronteira do prefixo e do sufixo pode ser em qualquer posição do endereço.

Um endereço padrão IPv6 deve ser formado por um campo *provider ID*, *subscribe ID*, *subnet ID* e *node ID*. O *node ID* (ou identificador de interface) deve ter 64 bits, e pode ser formado a partir do endereço físico (MAC) no formato EUI 64.

Os endereços IPv6 são normalmente escritos como oito grupos de 4 dígitos hexadecimais. Por exemplo,

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7344
```

Se um grupo de vários dígitos seguidos for 0000, pode ser omitido. Por exemplo,

```
2001:0db8:85a3:0000:0000:0000:0000:7344
```

é o mesmo endereço IPv6 que:

```
2001:0db8:85a3::7344
```

Existem no IPv6 tipos especiais de endereços:

- *unicast* - cada endereço corresponde a uma interface (dispositivo).
- *multicast* - cada endereço corresponde a múltiplas interfaces. É enviada uma cópia para cada interface.
- *anycast* - corresponde a múltiplas interfaces que partilham um prefixo comum. Um datagrama é enviado para um dos dispositivos, por exemplo, o mais próximo.

Com o IPv6 todas as redes locais devem ter prefixos /64. Isso é necessário para o funcionamento da autoconfiguração e outras funcionalidades.

Usuários de qualquer tipo receberão de seus provedores redes /48, ou seja, terão a seu dispor uma quantidade suficiente de IPs para configurar aproximadamente 65 mil redes, cada uma

com endereços. É preciso notar, no entanto, que alguns provedores cogitam entregar aos usuários domésticos redes com tamanho /56, permitindo sua divisão em apenas 256 redes /64.

14. IoT (Internet das Coisas)

A Internet das Coisas (do inglês, Internet of Things) é uma revolução tecnológica a fim de conectar aparelhos eletrônicos do dia-a-dia, como aparelhos eletrodomésticos à máquinas industriais e meios de transporte à Internet, cujo desenvolvimento depende da inovação técnica dinâmica em campos tão importantes como os sensores, wireless, nanotecnologia e o amplo uso do IPv6.

14.1 Funcionamento

Primeiro, para ligar os objetos e aparelhos do dia-a-dia a grandes bases de dados e redes e à rede das redes, a Internet, é necessário um sistema eficiente de identificação. Só desta forma se torna possível coligir e registrar os dados sobre cada uma das coisas. A identificação por rádio frequência RFID oferece esta funcionalidade.

Segundo, o registro de dados beneficiará da capacidade de detectar mudanças na qualidade física das coisas usando as tecnologias sensoriais (sensor technologies). A inteligência própria de cada objeto aumenta o poder da rede de devolver a informação processada para diferentes pontos.

Finalmente, os avanços ao nível da miniaturização e da nanotecnologia significam que cada vez menores objetos terão a capacidade de interagir e se conectar. A combinação destes desenvolvimentos criará uma Internet das Coisas (Internet of Things) que liga os objetos do mundo de um modo sensorial e inteligente.

Assim, com os benefícios da informação integrada, os produtos industriais e os objetos de uso diário poderão vir a ter identidades electrónicas ou poderão ser equipados com sensores que detectam mudanças físicas à sua volta. Até mesmo partículas de pó poderão ser etiquetadas e colocadas na rede. Estas mudanças transformarão objetos estáticos em coisas novas e dinâmicas, misturando inteligência ao meio e estimulando a criação de produtos inovadores e novos serviços.

14.2 RFID

A tecnologia RFID que usa frequências de rádio para identificar os produtos é vista como “potenciadora” da Internet das Coisas. Embora algumas vezes identificada como a sucessora dos códigos de barras os sistemas RFID oferecem para além da identificação de objetos informações importantes sobre o seu estado e localização.

Estes sistemas foram primeiramente usados na indústria farmacêutica, em grandes armazéns e na saúde. As mais recentes aplicações vão dos desportos e atividades de tempos livres à segurança pessoal. Etiquetas (também chamadas de "tags") RFID estão a ser implantados debaixo da pele humana para fins médicos e também em passaportes e cartas de condução. Leitores RFID estão também sendo incluídos em celulares.

Para além do RFID, a capacidade de detectar mudanças no estado físico das coisas é também essencial para registar mudanças no meio ambiente. Por exemplo, os sensores usados numa peça de vestuário inteligente podem registrar as mudanças de temperatura no exterior e ajustar-se de acordo com elas.

Perspectiva-se um futuro em que poderemos usar roupa inteligente que se adapta às características da temperatura ambiente, a passagem por um sensor irá indicar-nos qual a manutenção que o nosso carro necessita, poderemos usar os óculos de sol para receber uma chamada de vídeo e os cuidados médicos poderão ser prestados antecipadamente, graças a diagnósticos mais eficientes e rápidos.

15. Referências Bibliográficas:

https://pt.wikibooks.org/wiki/Redes_de_computadores

http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf

https://novatec.com.br/livros/redescom/capitulo9788575221273.pdf

http://www.cisco.com/cisco/web/support/BR/104/1045/1045464_40.html

Metro Ethernet Forum – Technical Specification MEF 10, Ethernet Service Attributes Phase 1, November 2004, em http://www.metroethernetforum.org/, jun. 2016.

Cisco - http://www.cisco.com/web/BR/index.html; mai. 2016.

TechTarget - http://searchdatacenter.techtarget.com/; mar. 2016

Open Networking Foundation - https://www.opennetworking.org/; mar. 2016

http://ipv6.br/post/introducao/