-- CURSO TÉCNICO DE INFORMÁTICA --
MÓDULO I

REDES DE COMPUTADORES

Bem vindo!

Esta é a primeira disciplina de nosso curso, onde iremos abordar as Redes de Computadores, sua importância atual, benefícios, suas aplicações, modos de operação, protocolos e sua contribuição para a comunicação de dados. A disciplina contém 60 horas de duração, divididas em 9 capítulos, como dispostos nesta apostila. Além de toda fundamentação teórica e exercício propostos, a apostila contém seções especiais, explicadas abaixo:

RESUMÃO

Ao final de cada capítulo ou de um conjunto de capítulos, teremos nesta seção um resumo sucinto do conteúdo abordado, para você, aluno, lembrar-se dos tópicos principais vistos naquele capítulo.

VADE MECUM

Do latim "vai comigo", trata-se de uma seção de anotações em formato único de perguntas que estimulam o raciocínio sobre as respostas. O objetivo é que o aluno carregue consigo um bloco contendo estas perguntas.

ALÉM DISSO...

Seção contendo sugestões de pesquisa em forma de termos, pertinentes ao conteúdo visto ou em forma de mídias (livros, filmes, etc.), convidando o aluno a avançar no tema discutido no capítulo.

Bons estudos!

1. INTRODUÇÃO AS REDES DE COMPUTADORES

As redes de computadores não são novas. Trata-se de uma invenção da década de 60, de origem americana, concebida para fins militares. Os combatentes queriam uma forma de comunicação que não tivesse ponto central, de modo a não ser destruída facilmente, mas que fosse possível estabelecer comunicação em ambientes adversos. Daí em diante, as redes expandiram-se rapidamente, primeiro de modo acadêmico, depois de modo popular, trazendo benefícios pessoais e corporativos para todos:

- Qualquer coisa para qualquer pessoa em qualquer lugar e qualquer hora. Misturam-se notícias, negócios, entretenimentos e comunicação em um único lugar.
- Economia de dinheiro. Empresas deixam de visitar clientes pessoalmente, deixam de atender em espaços físicos, reduzem gastos com comunicação.
- Compartilhamento de recursos torna-se essencial. Não precisa haver uma impressora para cada computador na empresa. Informações não precisam ser guardadas localmente em cada máquina. Dados não precisam ser replicados para todas as estações. Tudo é dividido com todos.

Breve histórico

Em dezembro de 1969, com objetivos militares, entra no ar a ARPANET, rede criada pela ARPA, uma agência americana de pesquisas. A rede tinha inicialmente 4 núcleos interligados com velocidade de 50 kbps (saiba que a chamada 'Internet discada' possui velocidade máxima de 56 kbps). A ARPANET foi crescendo e em 1972 já possuía 34 núcleos espalhados. Em 1983, já estável e bem sucedida, contava com 200 núcleos.

Então, outra agência americana, a NSF, se interessou pela coisa e criou a NSFNET, operando supercomputadores que logo foi conectada à ARPANET, originando nossa grande aliada Internet. O avanço foi exponencial e em 1990, já estavam interconectadas cerca de 3 mil redes e 200 mil computadores. Em 1992, foi conectado o milionésimo computador. A sequência da história todos nós conhecemos. É possível viver hoje sem Internet?

Mas o que é Redes de Computadores, afinal?

Se estiver procurando uma definição técnica, vamos lá. Redes de computadores são coleções de dispositivos interconectados, seja de modo remoto ou local, a fim de compartilhar recursos e prover comunicação através do tráfego de dados entre estes dispositivos.

1.1. Internet

Ah... a Internet. Como já lemos, a Internet foi criada a partir da junção entre a ARPANET e A NSFNET. O ponto principal foi a utilização do protocolo TCP/IP (o qual estudaremos mais profundamente no capítulo sobre protocolos) como protocolo oficial de comunicação da ARPANET. A partir daí, a rede abriu-se para pesquisas e passou a se conectar com outras redes existentes.

- SPAN (*Space Physics Analysis Network*): rede de física espacial da NASA.
- HEPNET (*High-Energy Physics Network*): rede de física nuclear de alta energia para pesquisadores
- BITNET (*Because It's There Network*): rede de *mainframes* da IBM
- EARN (*European Academic and Research Network*): rede acadêmica europeia.

Como você deve imaginar, lendo esses dados, a Internet era utilizada para fins acadêmicos, compartilhada entre pesquisadores, indústrias e órgãos governamentais. O grande *boom* veio em meados de 1990, quando Tim Berners-Lee, um cientista do CERN (organização europeia de pesquisa nuclear) lançou a tecnologia WWW (*World Wide Web*) que unia o protocolo TCP/IP ao HTTP, permitindo trafegar hipertexto (códigos) na rede. Ocorreu então uma grande "invasão" de pessoas sem objetivos acadêmicos, empurradas pela curiosidade e pela novidade.

A empresa americana Netscape desenvolveu em 1992, o protocolo HTTPS, que possibilitava trafegar informações na rede de maneira segura, o que dava abertura para negócios serem implantados sobre a estrutura da Internet. Dentre as principais aplicações oferecidas,

O primeiro navegador!

O navegador é o *software* que nos permite consumir o conteúdo da Internet, interpretando as linhas de códigos daquele determinado site. Hoje existem centenas deles como o *Internet Explorer*, da Microsoft e o *Chrome* da Google. Por anos, reinou o *Netscape Navigator,* desenvolvido para Windows.

Mas o pioneiro de todos foi o MOSAIC, desenvolvido pela *National Center for Supercomputing Applications* (NCSA). Com ele, era possível visitar os primeiros sites, clicar nos primeiros *links* e assistir os primeiros vídeos da Internet (Não! Não existia *Youtube*!).

podemos destacar:

1.1.1. Correio eletrônico

Foi criado ainda na fase inicial da ARPANET, baseando-se em protocolos POP, IMAP e SMTP, para trafegar entre computadores, textos planos ou codificados em formato de mensagem.

1.1.2. News

Fóruns especializados de discussões, divididos em vários assuntos onde usuários trocam informações e mensagens.

1.1.3. *Login* remoto

Possibilidade de obter acesso restrito a um computador remoto através de abertura de conexão utilizando programas específicos para isso.

1.1.4. Transferência de arquivos

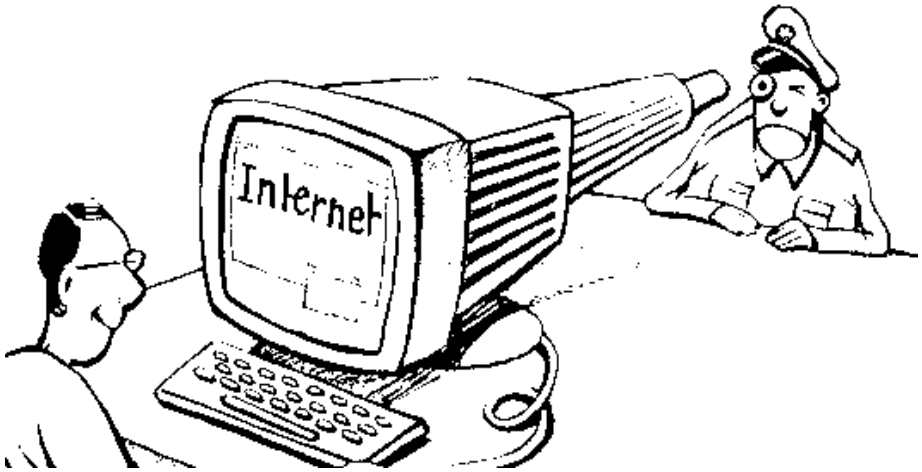
Através do protocolo FTP, é possível copiar arquivos entre máquinas que estejam conectadas à Internet.

1.1.5. Ambiente diverso

Criado um simulacro do universo real, destacam-se os *shoppings* eletrônicos, ensinos à distâncias, *home banking*, mídias sob demanda, etc.

1.2. Desafios

Redes, sejam pessoais ou corporativas, não surgem por acaso. A motivação está, em sua maioria, na resolução de problemas cotidianos e absorção das vantagens proporcionadas. Aliado a isso, o ambiente ao redor das redes trazem desafios a serem superados para o sucesso da rede.



- Planejamento: espaço físico, capacidade, número de usuários, etc. Tudo deve ser planejado.
- Organização: papel do administrador é fundamental na organização física, lógica e operacional.
- Segurança: proteção contra ataques, tráfegos de informações sigilosas, políticas de privacidade, etc.
- Administração de Recursos x Usuários: a rede deve servir à todos de maneira satisfatória.
- Desenvolvimento / Aquisição de Novos Equipamentos e Softwares
- Atualização: a rede deve acompanhar a evolução da tecnologia.
- Integração: expansão de conexões com outros serviços é essencial.

RESUMÃO

- Redes são coleções de dispositivos interligados de modo local ou remoto, para trocar informações.
- Surgiu da ARPANET para fins militares.
- A ARPANET uniu-se a NSFNET, dando origem à Internet.
- Em 1990 surgiu o WWW que transformou a Internet e atraiu centenas de milhares de usuários (e continua atraindo até hoje...)
- Vantagens principais resumem-se a economia financeira e comunicação facilitada.
- Serviços destacados são correio eletrônico, a transferência de arquivos (*downloads*), fóruns de discussões e ambientes integrados de lazer, negócios, entretenimento e relacionamento interpessoal.
- Redes devem ser planejadas, pois demandam dedicação dos administradores para satisfazer os usuários de seus serviços.

VADE MECUM

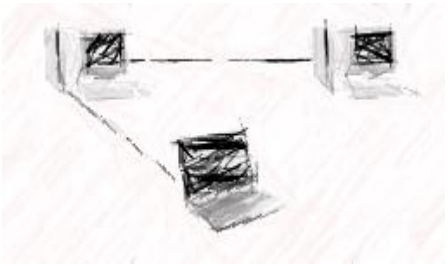
- Porque Redes sugerem economia?
- Quem foi Tim-Berners-Lee?
- O que foi o MOSAIC?
- O que foi a ARPANET?
- O que foi a NSFNET?
- Porque planejar uma Rede?

ALÉM DISSO...

Interessou-se em saber como funcionam as redes? O site WARRIORS OF THE NET produziu um dos vídeos mais famosos sobre o funcionamento das redes. Para conhecer, acesse a página do site em (http://www.warriorsofthe.net) e procure por MOVIES. (há uma versão legendada em PT-BR).

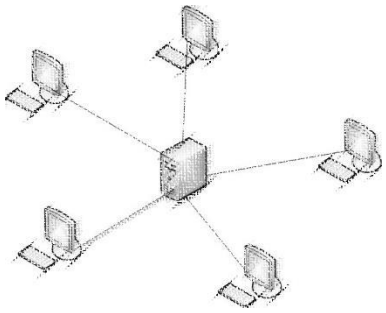
2. TIPOS DE REDES E ARQUITETURAS

Ao planejar a implantação de uma rede, temos comumente dois cenários a seguir. Ter ou não ter a presença de um computador servidor: eis a questão. Redes sem servidor são chamadas de ponto-a-ponto (*peer-to-peer,* P2P) e operam com todos os computadores integrantes realizando o gerenciamento local de modo independente. Isso traz grandes vantagens, como por exemplo,



ter que replicar dados para todas as máquinas, congestionando a rede (um usuário precisa ser cadastrado em todas as máquinas). São indicadas fortemente para compartilhar dispositivos (impressoras, discos, etc), nunca serviços (banco de dados, por exemplo), pois sofre com falta de sincronismo dos comportamentos dinâmicos característico dos serviços oferecidos em rede. Os benefícios maiores das redes ponto-a-ponto podem ser apontados na simplicidade de sua instalação em redes pequenas (até 10 estações) e no seu baixo de custo (poucos cabos).

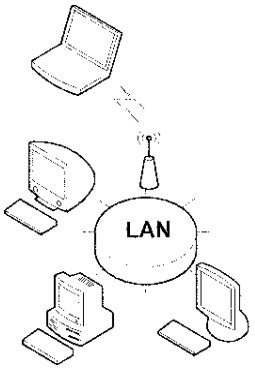
Já as redes chamadas de cliente/servidor (*client/server*) possuem um computador central, com arquitetura de hardware superior a de um micro comum, para realizar o gerenciamento e compartilhamento dos recursos. É ideal para usar em redes pequenas e de médio porte que



necessitam compartilhar serviços, tendo em vista que o maior benefício de um servidor é o tempo de resposta das tarefas solicitas pelas máquinas clientes. Dentre os objetivos de uma rede *client/server,* podemos destacar servidores de arquivos, de impressão, de banco de dados. Apesar de possuir um custo mais alto em relação a redes ponto-a-ponto, são altamente mais seguras, ideal para ambientes corporativos.

As redes podem variar de alcance, pois a potência do sinal está diretamente relacionada com o tipo de cabo utilizado, número de usuários e distância geográfica ente equipamentos. Partindo desse princípio, podemos classificar as redes das seguintes formas:

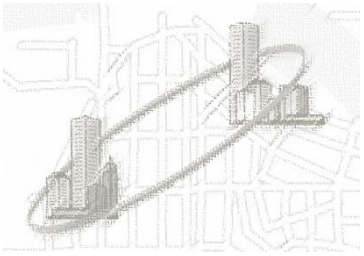
2.1. LAN (*Local Area Network*)



As redes locais estão presentes nas maiorias das corporações. Trata-se de uma estrutura de computadores interligadas, com equipamentos próximos, ocupando um único espaço físico, seja uma sala ou um edifício. Abrangem uma área limitada geograficamente, no geral indicada como 10 km no máximo e podem ser implantadas tanto em arquitetura ponto-a-ponto, quanto cliente/servidor.

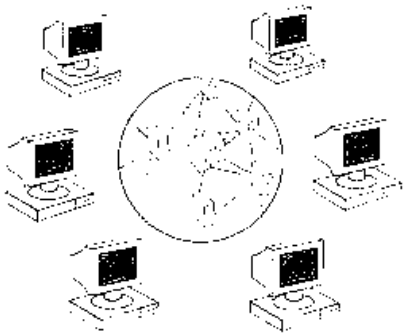
2.2. MAN (*Metropolitan Area Network*)

Redes metropolitanas interconectam equipamentos com capacidades maiores de processamento



a distantes superiores a 10 km. Seu conceito baseia-se em LAN's trocando dados entre si, formando uma única rede. É bastante aplicado em empresas com filiais ou unidades distantes que precisam trocar dados, mas também podem ser encontrados em comunicações interurbanas (como acontece com SP e RJ). Redes metropolitanas são comumente implantadas com um servidor central para gerenciamento, ideal para seu modelo com vários pontos clientes.

2.3. WAN (*Wide Area Network*)



Quando a NSF se estabeleceu com conexões em importantes cidades americanas, operando potentes supercomputadores, surgia a primeira rede estendida a utilizar os mesmos padrões e protocolos da Internet atual. Um *WAN* interliga equipamentos distantes geograficamente, geralmente referenciados como de país para país ou de continente para continente. Como ainda não havia comunicação via satélite, as redes estendidas foram ideais para um cenário de comunicação a longas distâncias, de forma rápida e eficiente. Pode trabalhar tanto com conexões ponto-a-ponto, quanto cliente/servidor, utilizando-se de serviços terceirizados na infraestrutura.

2.4. SAN (*Storage Area Network*)

Trata-se de uma estrutura computacional interligada sob tecnologia RAID, cujo objetivo é armazenar informações para deixá-las disponíveis para consulta. O foco são os dispositivos de armazenamento, desprezando-se capacidades de processamento das máquinas envolvidas. Redes SAN são comparadas com outros sistemas de armazenamento como DAS (*Direct Attached Storage*, uma espécie de HD gigante) e o NAS (*Network Attached Storage*, um dispositivo que pode acondicionar vários discos em rede), porém redes SAN provêm mais espaço de armazenamento e recursos de redundância, além de comportar-se como rede única de armazenamento com acesso transparente, ideal para

Compartilhamento P2P!

Redes ponto-a-ponto são bastante populares na troca de arquivos entre usuários. Vários softwares de sucesso como *Kazaa*, *Emule*, *LimeWire*, *Ares*, entre outros ajudam na tarefa de baixar arquivos diretamente do computador de outro usuário e vice-versa, formando uma grande rede de dados, muitas vezes indisponíveis em servidores da Internet.

grandes aplicações Web. A grande desvantagem é o custo bastante elevado para implantação.

2.5. PAN (*Personal Area Network*)

Redes pessoais (também conhecidas como *piconet*) baseiam-se no padrão IEEE 802.15, chamado comercialmente de *Bluetooth*, para criar interconexões entre equipamentos pessoais. Limita-se a curtas distâncias (geralmente 10m) e um total de 8 de equipamentos para que haja comunicação satisfatória entre os dispositivos. Há também o padrão IEEE 802.15.4 (chamado de *ZigBee*), que otimiza o consumo de bateria e permite mais dispositivos, apesar de trabalhar cerca de 3x mais lento que o padrão 802.15. Por fim, temos o uso de tecnologia RFID (*Radio Frequency Identification*), que dispensa o apoio de sistemas de energia (pilhas, baterias, fontes de alimentação) para fazer uso de sinais de rádio na comunicação entre dispositivos.

2.6. GAN (*Global Area Network*)

Redes globais são, na verdade, WAN's com cobertura mundial capaz de conectar sistemas em redes situados em diferentes países e continentes. O objetivo é oferecer conectividade abrangente através de terminais móveis (chamados *hotspots*). Terminais GAN designam serviço de comunicação móvel de alta velocidade, oferecendo não só ligações de voz, mas também transmissão de fax, dados e multimídia, envio de imagens, *e-mails* e navegação pela Internet.

RESUMÃO

- Redes podem sem implementadas em LAN (local), MAN (metropolitana), WAN (estendida), SAN (armazenamento), PAN (pessoal [bluetooth/zigbee/rfid]) ou GAN (rede global, dispositivos móveis).
- Temos ainda arquitetura ponto-a-ponto (redes sem servidor) onde uma máquina troca dados direto com outra máquina e arquitetura cliente/servidor onde uma máquina (servidor) recebe requisições (pedidos) de outra máquina (cliente).

VADE MECUM

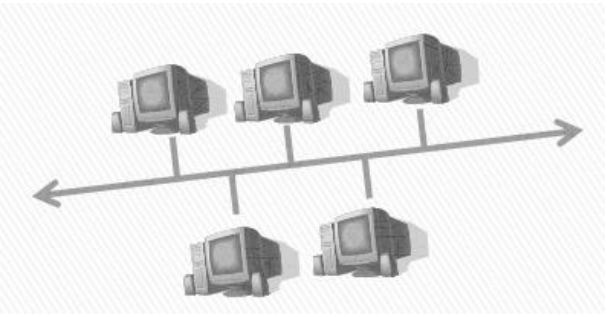
- Porque surgiram redes globais?
- Quando usar ponto a ponto?
- Porque usar SAN no lugar de NAS?
- RFID, o que é isso?
- Posso ter redes locais em casa?

3. TOPOLOGIAS

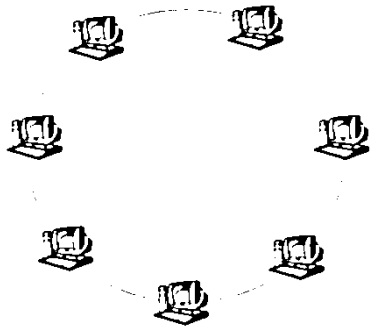
Redes podem ser classificadas em topologias, de acordo com a disposição física dos nós (estações). A escolha de uma topologia influencia diretamente nos equipamentos utilizados, custo da rede, complexidade de manutenção e desempenho geral.

3.1. Barramento (*Bus*)

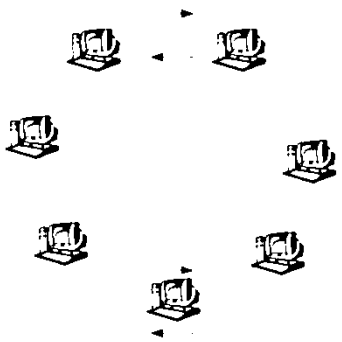
Topologias em barramento atualmente caíram em desuso nas corporações por apresentar falhas consideráveis. São caracterizadas pela utilização de um cabo principal (chamado *backbone*) em forma de barra como meio de transmissão de dados, onde as estações se acoplam por conectores específicos. O fluxo de dados é finalizado por terminadores presentes em cada ponta do barramento. Como o cabo é compartilhado, as mensagens enviadas passam por todas as estações (*broadcast*). Quando mais de uma máquina transmite dados ao mesmo tempo, ocorre uma colisão de pacotes na rede, fazendo com que sejam interrompidas as transmissões. Após um tempo aleatório, os nós voltam a transmitir. Trata-se de uma rede extremamente intolerante a falhas, pois se o cabo falhar, toda a rede é prejudicada. Possui também uma limitação quanto a velocidade de transmissão, condicionada ao número de nós presentes. Quanto mais máquinas conectadas, mais lenta ficará a transmissão.



3.2. Anel (*Ring*)

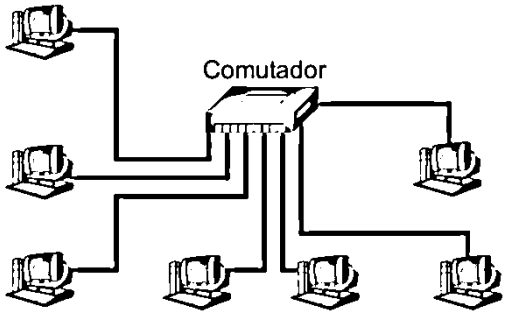


Trata-se de uma arquitetura ponto-a-ponto, sem terminadores, onde as estações são conectadas de forma circular. A topologia em anel resolveu um grande problema das tipologias em barramento, a colisão de pacotes. Apenas 1 máquina pode transmitir dados na rede. Para isso, o controle é feito através de um *token* (ficha), cuja estação que mantiver posse deste *token*, faz a transmissão. Topologias em anel, assim como barramento, ainda apresentam total dependência das estações e mostram-se intolerante a falhas, isto é, as estações devem estar ativas e funcionando para não comprometer o fluxo de dados. Esta dependência pode ser resolvida através do *beaconing*, uma técnica que utiliza 2 anéis, sendo um de reserva.



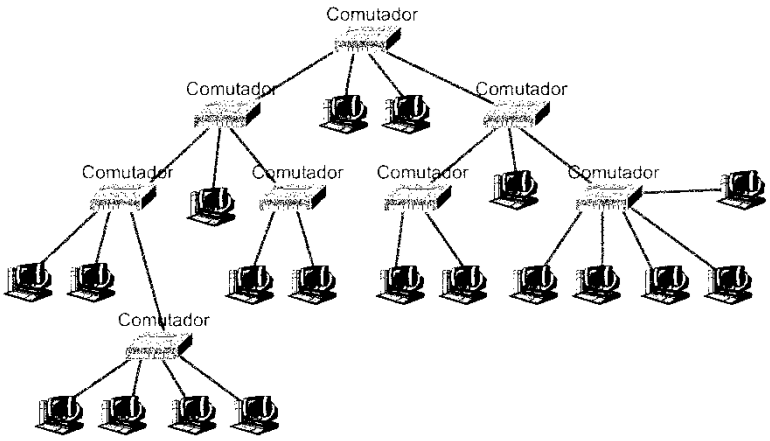
3.3. Estrela (*Star*)

Topologia amplamente usada no âmbito comercial e corporativo por apresentar várias facilidades em relação às outras topologias. Redes em estrela controlam fluxos através de um concentrador ou comutador de pacotes (roteador, *hub*, *switch*, *bridge*), o que ocasiona transmissão por difusão (o sinal vai direto para o destinatário) ao invés de transmitir ponto a ponto (o sinal passa por outras estações, antes de chegar ao destino) evitando *broadcasts* e dependência das estações, além de facilitar manutenções e adição de novos nós. Alcança também maiores taxas de transmissão, pois o meio de transmissão não é compartilhado, embora ainda possa apresentar colisão de pacotes.



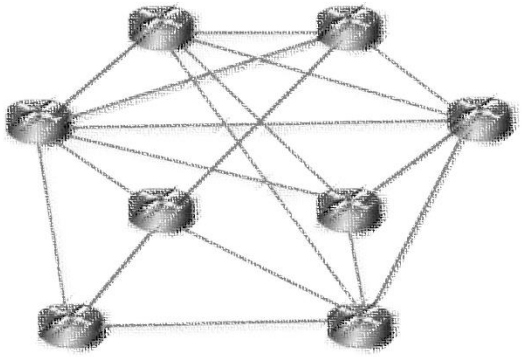
3.4. Árvore (*Tree*)

Também chamado de Topologia Hierárquica ou Estrela Estendida, é na verdade uma variação da topologia Estrela, na qual é possível dispor os comutadores de pacotes de forma hierárquica, podendo dividindo a rede em vários níveis, sem deixar de haver intercomunicação entre as sub-redes. Favorece também a expansão da rede e adição de novas estações, permitindo ainda um gerenciamento centralizado através de um comutador *máster*.



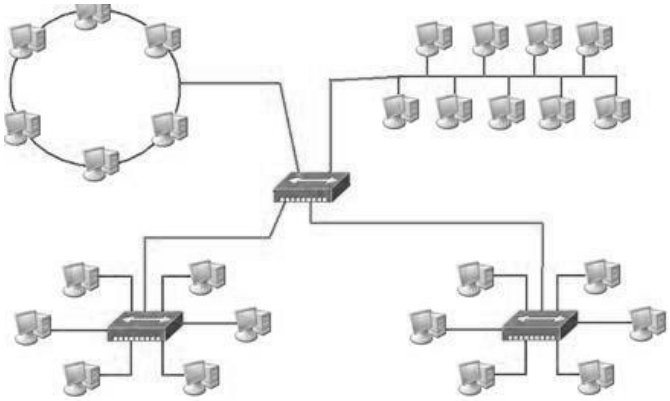
3.5. Malha (*Mesh*)

Topologias em malha seguem conceitos de redes distribuídas, embora o processamento seja centralizado. Apresenta estrutura parecida com topologias estrelas, porém sem a presença de um comutador de pacotes, o que faz a rede trabalhar com transmissões ponto-a-ponto. Redes *mesh* são bastante usadas em comunicações de longa distância por obter altas taxas de transferência, porém possui uma



arquitetura complexa, vários segmentos de redes com algoritmos robustos e custo de implantação elevado, o que inviabiliza seu uso em redes locais.

3.6. Mista (*Hybrid*)



Topologias híbridas ou mistas reúnem características de duas ou mais topologias em uma única estrutura de rede. O resultado é uma rede com manutenção extremamente complexa e descoberta de falhas dificultada por sua estrutura problemática. Seu uso pode ser encontrado em casos de barateamento da rede, onde não é possível comutar a rede toda ou adquirir concentradores por falta de recursos. Numa outra perspectiva, uma rede híbrida pode ser ideal para retirar vantagens de cada topologia envolvida em ambientes próprios.

RESUMÃO

- Topologia pode significar a forma geométrica com que a rede está disposta.
- As mais conhecidas são barramento (barra), anel (circular), estrela, árvore, malha e híbrida.
- Redes podem trabalhar de modo centralizado onde máquinas são dependentes de outras máquinas ou de um concentrador.
- Também podem operar de modo descentralizado/distribuído onde não há dependência, isto é, todas as máquinas e concentradores podem trabalhar mesmo que outro equipamento falhe.

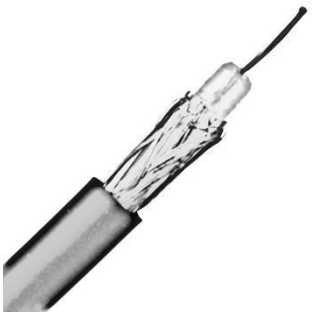
VADE MECUM

- Posso misturar topologias? Isso é bom ou ruim?
- Utilizar ou não um concentrador? Que vantagem terei nisso?
- Existe alguma topologia que seja 'melhor'?

4. TIPOS DE MEIOS FÍSICOS

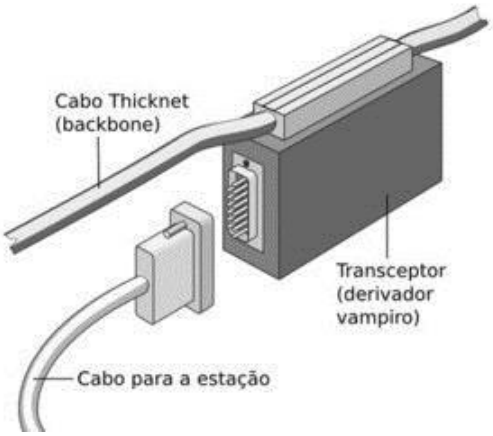
A transmissão de dados em uma rede pode ocorrer de várias formas, até mesmo pelo ar (embora não seja de forma física). Cada meio de transmissão trabalha de maneira particular, mas nenhum é descartável, sendo adequado a cada situação/ambiente.

4.1. Cabo Coaxial



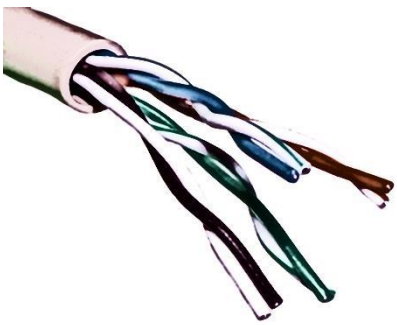
Os cabos coaxiais são bastante usados em redes antigas ou em ligações telefônicas. Trata-se de uma malha de cobre revestida externamente com plástico PVC. Nas pontas, estava presente um fio de cobre rígido representando o conector central. Domesticamente, os cabos coaxiais eram usados (ainda são) em antenas receptoras para televisores, sendo conectados na parte traseira do aparelho. Pela presença massiva de cobre, cabos coaxiais costumam causar inúmeros ruídos ou interferências quando em contato com outros aparelhos elétricos ou eletrônicos, o que o coloca em desvantagem em relação aos outros meios de transmissão. Nas topologias eram essencialmente usados em redes barramento, embora fosse possível implantá-los com redes em anel.

Nas redes barramento, o cabo *backbone* era do tipo coaxial grosso (chamado de *thicknet*, *thickwire* ou, na especificação técnica, RG-8), com o qual era possível alcançar até 500m. Coaxiais grossos são mais resistentes à ruídos, embora sejam pouco flexíveis. Em redes estruturadas, utiliza-se um conector AUI 15 pinos, chamado popularmente de “conector vampiro”.



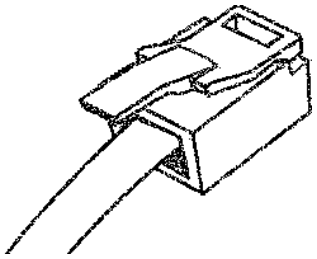
Para interligar as estações, era utilizado o cabo coaxial fino (chamado de *thinnet*, *thinwire* ou, na especificação técnica, RG-58), mais flexível e com distância máxima de 185m. Em uma das extremidades, o cabo conectava-se ao “vampiro” e na outra ligava-se à placa de rede da estação através de um conector do tipo BNC fêmea ou BNC tipo T.

4.2. Cabo Par Trançado Sem Blindagem (UTP)



Cabos UTP (*Unshielded Twited Pair*) estão presentes nas maiorias das redes domésticas e corporativas de pequeno/médio porte. Sua estrutura é feita de cobre fino, sendo cada via revestido com plástico isolante geralmente colorido, além de uma capa plástica que envolve todos os fios. Dentro do

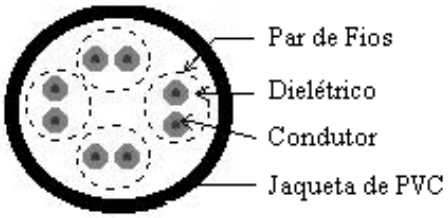
revestimento externo, os fios encontram-se trançados em pares, uns sobre os outros, dando origem ao nome. É um cabo extremamente flexível e barato, sendo de fácil instalação, o que justifica sua popularidade. Embora ainda sofra com ruídos pequenos e sua preparação seja um tanto quanto trabalhosa, é a melhor opção de transmissão, em análise de custo-benefício. Para garantia de sinal corrente, a maioria dos fabricantes recomenda a distância máxima de 90m, entre transmissor e receptor ou entre concentradores, embora fisicamente falando, os cabos UTP suportam até 100m.



Em telefonia, utilizam-se conectores do tipo RJ-11 com variação de tamanho e tipo. Nas redes de computadores, o mais popular é o RJ-45 (chamado de conector modular 8 vias). Cabos Par Trançado podem ser ainda categorizados como na tabela abaixo:

CATEGORIA	APLICAÇÕES
1	Antigo cabeamento telefônico.
2	Admite comunicação de até 4 Mbps. É equivalente à categoria IBM tipo 3.
3	Admite comunicação de até 10 Mbps.
4	Admite comunicação de até 16 Mbps.
5	Admite comunicação de até 100 Mbps ou 155 Mbps. Tem 4 pares com baixa interferência entre eles. É, hoje, o cabo UTP mais usado.

Atualmente, novos padrões categorias estão sendo implantadas. Categorias 5e ("*enhanced")* é uma melhoria da categoria 5, suportando trabalhar em frequências mais altas, em redes de transmissão Gbps (Gigabits por segundo). Igualmente para as categorias 6 e 6a ("*augmented*"), suportando velocidade de 1Gbps. Já as categorias 7 foram criadas para permitir a criação de redes de até 10 Gbps, usando 100m de fio de cobre.



4.3. Cabo Par Trançado Blindado (STP)

Os cabos STP (*Shilded Twisted Pair)* são uma adaptação do UTP para aumento de desempenho. Sua estrutura é idêntica, com fios de cobres trançados uns sobre os outros revestidos com plástico. A diferença está em camada metálica, chamada de malha, que envolve cada par, destinados a diminuir ruídos e interferências. Há ainda o SSTP (*Screened Shilded Twisted Pair*) ou SFTP (*Screened Foiled Twisted Pair*) que, além

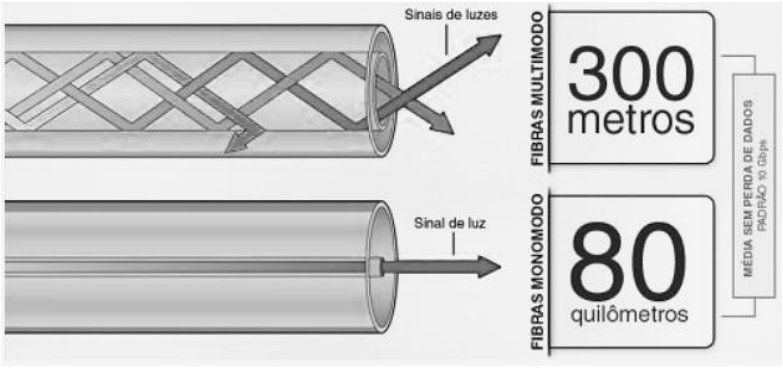
da blindagem individual dos pares, adiciona mais uma malha metálica envolvendo os todos os pares, provendo maior qualidade ao sinal transmitido, sendo ideal para ambientes com fortes interferências externas (como instalações prediais).

Os conectores também são RJ-45, porém com modelos blindados. Para cabos STP, é adotado o modelo de conector hermafrodita da IBM, classificados como na tabela abaixo:

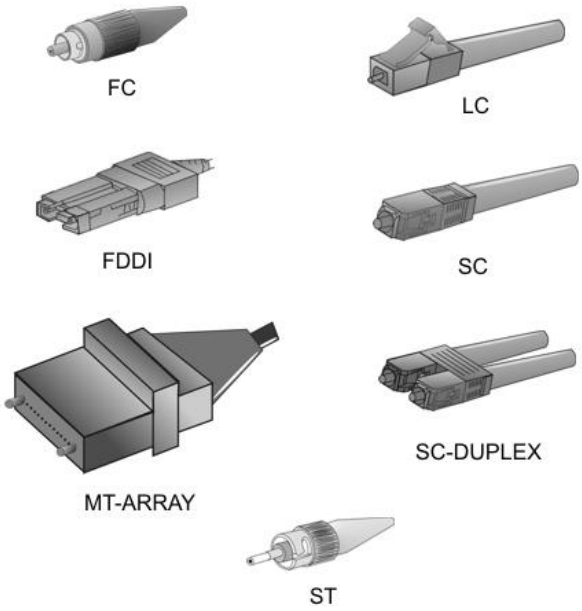
CATEGORIA	APLICAÇÕES
1	STP com 2 pares trançados blindados. Conectores AWG 22 com taxas de até 16 Mbps.
2	STP com 2 pares trançados blindados com conectores AWG 22 para dados e 4 pares trançados blindados AWG 26 para voz.
3	UTP com 4 pares trançados AWG 22 ou 24. Taxa de até 4 Mbps

4.4. Fibra Ótica

A fibra ótica apresenta-se como o meio de maior qualidade disponível, alcançando altas taxas de transmissão á grandes distâncias, sem ruídos ou perda de sinal. Os dados são transmitidos através de uma fonte de luz, LED ou Laser, passando dentro da fibra. A fibra em si, é um filamento revestido internamente com vidro ou polímero, formando um espelho para passagem de luz. Redes em fibra ótica permitem grandes distâncias com baixas perdas, sendo praticamente imunes a interferências ou linhas cruzadas, além de isolamento elétrico por utilizar material não condutor. Porém, devem ser manuseadas com grande cuidado, pois se quebram com facilidade. Por ser de dimensão minúscula, exigem equipamentos e conexões de alta precisão, o que influencia diretamente no custo de instalação e manutenção.



Fibras óticas podem ser classificadas em dois tipos. Os tipos Monomodo são mais eficientes, por conterem um filamento mais estreito, fazendo com que a luz passe em linha reta. Dessa forma, são alcançadas velocidade de até 100 Gbps com 1 km de cabo. Nas fibras Multimodo, o diâmetro central é mais espaçado, permitindo que a luz se propague de várias maneiras e por vários caminhos. Isso aumenta a atenuação do sinal, alcançando taxas menores. O custo também é influenciado, sendo os tipos Monomodo mais caros por sua maior eficiência em relação ao Multimodo.



O revestimento das fibras óticas pode variar. Os tipos mais comuns são *Loose* em que as fibras ficam soltas, acondicionadas em um tubo preenchido com gel, sendo ligeiramente mais flexíveis. Os tipos *Tight* contêm fibras revestidas individualmente com capas plásticas. Existem diversos conectores para fibra ótica, variando conforme o tipo de fibra e sua velocidade, sendo o conector SC mais usado em novas instalações.

RESUMÃO

- Meios físicos mais comuns: coaxial, par trançado e fibra ótica.
- Coaxial: sofre *cross-talk*, alcança 185m (fino) e 500m (grosso). Conector BNC para estações e AUI (vampiro) para *backbones*.
- Par trançado: alcança até 100m e utiliza conector RJ-45. Pode ser revestido com uma malha metálica (blindagem) para diminuir o *cross-talk*.
- Fibra ótica: imune a *cross-talk*, alcança altas taxas de transmissão a grandes distâncias. Quebra-se com facilidade e tem custo maior que outros meios.

ALÉM DISSO...

Um dos assuntos mais controversos sobre cabeamentos são as emendas. Em pares trançados essa técnica é 'proibida', com risco de perda do cabo. Em fibras óticas, a emenda é considerada, utilizando equipamentos próprios, com leve perda de desempenho. Pesquise por 'Fusão em Fibra Ótica' para saber mais sobre o tema.

VADE MECUM

- Porque usar fibra ótica, se é mais caro?
- Posso emendar um cabo quebrado?
- O cabo da antena de minha televisão é o mesmo usado em redes?

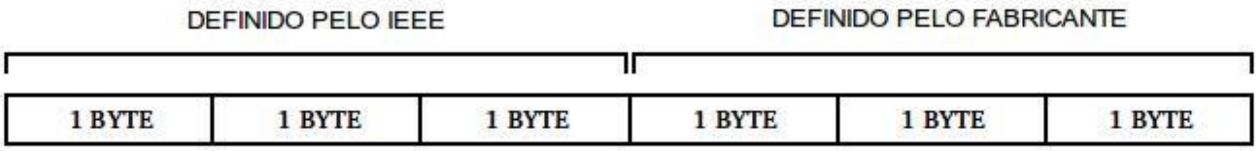
5. EQUIPAMENTOS DE REDE

Em redes complexas podem existir diversos equipamentos para realizar a interconexão com outras redes. Os que participam do núcleo de processamento são chamados de ativos, enquanto os que auxiliam (geralmente associados a partes não elétricas ou eletrônicas) o funcionamento da rede são chamados de passivos.

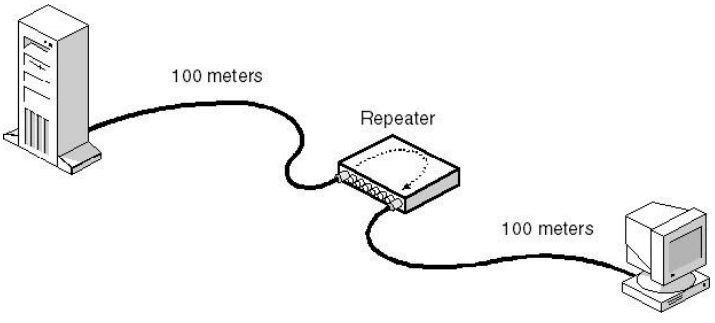
5.1. NIC (*Network Interface Card*)

Popularmente chamada de placa de rede, o NIC é o dispositivo de hardware responsável pela comunicação entre as estações da rede. É o primeiro e mais básico dispositivo de qualquer rede, pois exercem tarefas essenciais como preparar e endereçar os dados para envio, controlar o fluxo e fazer a conexão com outra estação. As placas de rede contém uma espécie de memória interna que armazena os dados que chegam pela rede e vai repassando-os para que o processador da estação manipulá-los. Cada placa de rede possui um endereço de identificação único chamado MAC (*Media Access Control*), sendo através dele que os pacotes de rede sabem seu destino, controlando a circulação de dados na rede.

O endereço MAC compõe uma sequencia de 48 bits ou 6 bytes representados na forma hexadecimal (Ex: 00 00 5E 00 01 03). Os 3 primeiros bytes são pré-definidos pelo IEEE (*Institute of Electrical and Electronics Engineers*) para identificação do fabricante e os 3 bytes restantes o próprio fabricante os define, sendo responsável então por controlar a numeração das placas que produz.



5.2. Repetidor

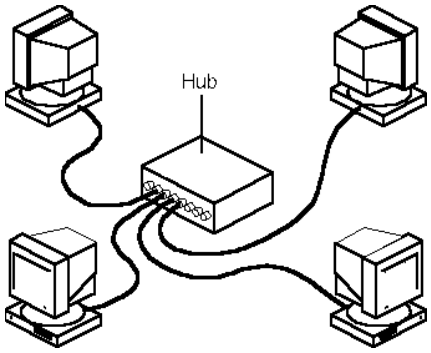


Repetidores são dispositivos usados para aumentar o comprimento da rede, visto que os cabos tem limitação de distância para transmissão do sinal. Seu funcionamento é simples, baseando-se em receber um sinal por uma porta de entrada e amplificá-lo ou regenerá-lo, transmitindo as mesmas informações para uma porta de saída. Pegamos de exemplo um lance

de cabos par trançado cujo limite especificado é de 100 m. Imagine que seja necessário um lançamento de 140 m; desta forma pode-se lançar 90 m de cabos, usar um repetidor e continuar o lançamento por mais 50 m.

Repetidores não fazem análise dos pacotes de rede que recebem, apenas repetem a informação recebida. Desta forma, se a rede possuir ruídos ou interferências, estas serão também amplificadas. Atualmente, repetidores são usados embutidos dentro de outros equipamentos, especialmente os switches, sendo raro encontrar seu uso na forma de equipamento independente.

5.3. Hub



Hubs são usados comumente como dispositivos concentradores em topologias estrela, responsáveis por centralizar a distribuição de pacotes na rede. Porém é um equipamento com funcionamento lógico do tipo barramento, isto é, qualquer sinal transmitido é replicado em todas as portas do dispositivo. Isso o torna extremamente desvantajoso em relação aos demais concentradores, justificando seu crescente desuso. Podemos interconectar dois ou mais hubs entre si, através de uma técnica conhecida como "cascateamento". A maioria dos hubs possui uma porta chamada Up-Link, destinada ao cascateamento, bastando conectar um cabo comum nesta porta, juntamente com uma porta comum de outro hub. É uma técnica recomendada somente para redes pequenas e em caso de extrema necessidade, pois com o cascateamento, mais replicações de sinal acontecerão, gerando tráfego excessivo à rede e causando lentidão.

5.4. Bridge

A bridge é um equipamento destinado a segmentar uma rede, interligando dois ou mais trechos, inclusive sendo eles de diferentes topologias (ex: estrela interligada com anel). Tem uma análise inteligente do tráfego, verificando os pacotes recebidos e transmitindo-os direto ao seu destino, sem replicar os dados para todos os trechos, diminuído colisões de pacotes. Para tal controle, as bridges fazem leitura do endereço MAC de destino de cada pacote, determinando em qual trecho ele irá trafegar.

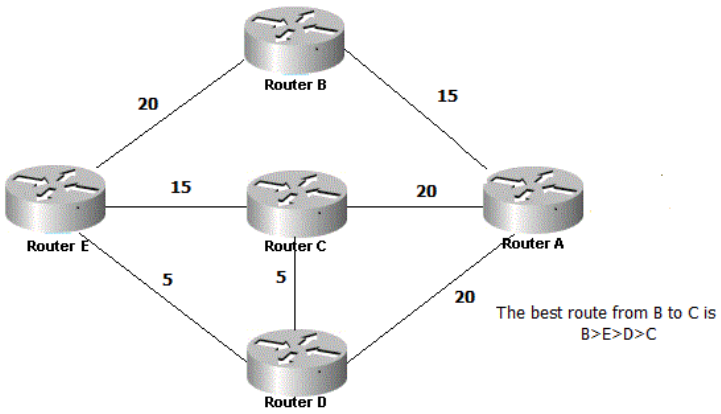
Além disso, as bridges também exercem papel importante no controle do fluxo da rede, filtrando mensagens que passam por ela, de modo que pacotes com erro não sejam retransmitidos. Possuem também uma área de memória interna, onde os dados são armazenados quando o tráfego é intenso. Diferem-se de repetidores comuns por manipular

pacotes e não sinais elétricos, o que permite analisar informações e não retransmitir ruídos ou erros na rede.

5.5. Roteador

Equipamento destinado a interligar redes locais entre si e redes remotas em tempo integral. É mais comumente utilizado para gerenciar pacotes que trafegam de uma LAN para uma WAN (a Internet, por exemplo). Sua principal função é escolher rotas ('rotear') para um pacote trafegar até seu destino, baseando-se em endereços IP (ao invés de MAC) e protocolos de roteamento. Existem diversos modelos de roteadores com diferentes interfaces, por exemplo, modelos com entradas de par trançado, fibra ótica, conectores AUI, sendo capazes de interconectar redes com interfaces distintas. É importante notar que os roteadores podem interconectar redes diferentes (redes independentes), ao passo que repetidores, hubs, bridges e switches atuam num mesmo segmento de rede. As etapas de um roteamento podem ser descritas a seguir:

- O roteador recebe dados de uma de suas redes conectadas;
- Os dados são repassados para a área onde o roteador acessa as informações do pacote;
- O roteador lê o endereço IP de destino do pacote;
- O roteador consulta uma tabela de roteamento para determinar o destino do pacote.



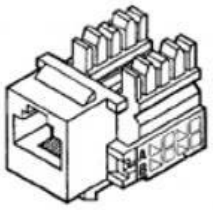
Após consultar o destino, o roteador faz a escolha do melhor caminho para trafegar o pacote baseando-se em "custos" da rede, considerando tráfego, tempo de envio, tamanho do pacote, etc. O cálculo do menor custo é feito com algoritmos. Os mais comuns são o *Distance-Vector* e o *Link-State.* No *Distance*-Vector, cada nó da rede recebe informações de custo dos vizinhos diretamente conectados a ele, de modo distribuído e iterativo, isto é, o custo é recalculado a cada ciclo do pacote, até o seu destino. Já no *Link-State*, o custo é calculado baseando-se em um conhecimento total e global da rede, isto é, cada nó tem informações completas sobre os custos de todas as rotas.

5.6. Switch

Um switch é um equipamento inteligente que tem a função de filtrar dados circulantes numa rede local, analisando pacotes e endereçando-os diretamente ao seu destino, além de, na maioria dos modelos, amplificar o sinal recebido através de um repetidor interno. Diferencia-se

do roteador, pois não faz a escolha do melhor caminho. O uso de switches é ideal em áreas de grande tráfego, especialmente em segmentos próximos a servidores, pois ele trabalha com *store-and-foward*, isto é, coleta os dados armazenando-os e analisando-os, para depois retransmiti-los ao seu destino. Alguns switches encaminham o pacote ao seu destino, analisando endereços IP, sendo mais comum encontrar modelos que fazem essa função trabalhando com endereços MAC.

5.7. Keystone

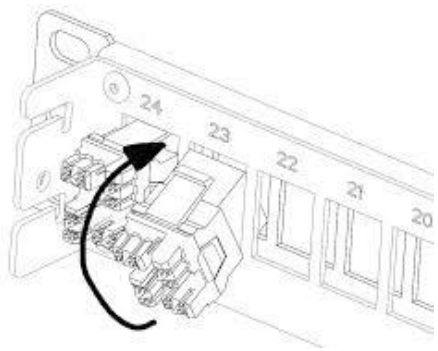


Também chamados de *Jack,* RJ-45 Fêmea ou simplesmente, tomada de rede, trata-se de um dispositivo encaixado na ponta de cabos par trançados, de forma a receber cabos crimpados com o conector RJ-45, completando o fluxo de conexão. É comum estar localizado em paredes, protegidos por um *Faceplate*.

5.8. Faceplate

Espelho de tomada próprio para RJ-45 ou RJ-11. Pode ser encontrado em vários modelos com diferentes quantidade de conexões e nos mais diversos materiais e cores. Protege e oculta fios aparentes, encaixados no *Keystone*.

5.9. Patch Panel



Um *Patch Panel* funciona como um painel de conexões ou painel de tomadas, geralmente numeradas, destinadas a 'organizar' os cabos que vão para as áreas de trabalho do usuário, facilitando a ativação/desativação de uma estação de trabalho. Na parte traseira do *Patch Panel* são encaixados os cabos com *Keystones* na ponta e na parte dianteira vão os cabos com conector RJ-45. Há também modelos de *Patch Panel* próprios para fibra ótica.

5.10. Rack

Equipamento de suporte e proteção aos ativos da rede. Há modelos abertos, que se assemelham a pedestais onde *switches, patches panel*, entre outros são encaixados com parafusos. Os modelos fechados são em formato de caixa, possuindo chaves e cadeados. Podem ficar no chão, como também fixados na parede, à certa altura.

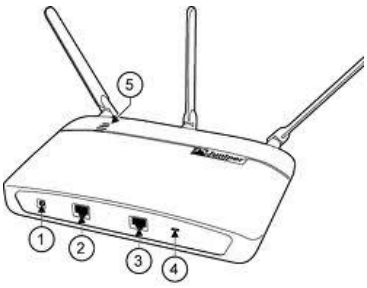
5.11. Modem

O *modem* é um dispositivo que permite a conversão de sinais. Era largamente usado para interconectar dois computadores utilizando o sistema de telefonia analógico para transmissão dos dados. Como o computador apenas aceita sinais digitais, era necessário um *modem* para modular/demodular o sinal analógico para digital e vice-versa. Os padrões de velocidade e conexão foram sendo estabelecidos pelos próprios fabricantes. Alguns exemplos são os padrões *V.fast*, atualmente *V.3*, para modems de 33,6 *Kilobits* por segundo e o padrão da Motorola e AT&T para modems com 28,8 Kbps. Alguns padrões alcançavam 56 kbps, porém em condições de energia favoráveis e por pouco tempo, devido à má qualidade do meio de transmissão.

Outro modelo é o ADSL (*Asymmetric Digital Subscriber Line*), chamado de *modem* digital, o qual podia-se alcançar taxas mais rápidas de até 52 *Megabits* por segundo*,* utilizando linhas telefônicas convencionais. E por último temos os *modems mobile*, que recebem sinal de rede da operadora de telefonia móvel e o converte para uso em microcomputadores ou *notebook*.

5.12. Access Point

Pontos de acesso são dispositivos conectados à uma rede cabeada, de forma a retransmitir sinal sem fio. Pode perder sinal com obstáculos durante o caminho, como água, paredes, árvores, vidro, etc.



5.13. Transceiver

Um *transceiver* (*transmitter* + *receiver*) é um dispositivo de hardware permite conexões interfaceadas, isto é, conectar diferentes interfaces numa mesma rede. Existem diversos modelos, sendo bastante comum, ligações RJ-45 (cabeamento metálico convencional) em fibra ótica.

VADE MECUM

- Quais os equipamentos mais comuns em uma rede?
- Por que o roteador é tão importante?
- Devo usar hubs em minha rede?
- Existem roteadores, switches e outros equipamentos para Fibra Ótica ou somente servem para par trançado?

ALÉM DISSO...

Modems 'reinaram' por anos na famosa 'internet discada'. Embora a velocidade seja 56 Kbps, jamais isso era atingido. Qual era a velocidade da sua internet? E agora?

6. CABEAMENTO ESTRUTURADO

Redes requerem manutenção constante e monitoramento ininterrupto, pois com o uso cotidiano, diversos problemas surgem em função de necessidades dos usuários. Para reduzir o trabalho de analistas e administradores de redes, é fundamental um planejamento prévio na implantação da estrutura de telecomunicação, englobando documentos com descrição detalhada de cada parte da rede e especificação técnica de equipamentos, mapas, grafos, normas, relatórios, etc. Surgiu então o estudo de cabeamento estruturado, uma série de técnicas e convenções que ajudam a organizar melhor toda a composição de uma rede cabeada.

Podemos destacar como principais vantagens do cabeamento estruturado:

- Redução de erros ocasionados por má implantação da rede;
- Otimização de desempenho em geral;
- Manutenção facilitada com documentação da estrutura;
- Garante possível certificação da rede;
- Suporte a aplicações diversas (voz, dados, vídeos, multimídia);
- Facilidade e rapidez em mudança de *layout* do ambiente;
- Ajuda na escalabilidade da rede

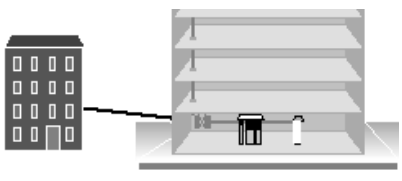
Estatísticas apontam que o cabeamento é responsável por 2% até 5% do custo de uma rede, ao passo que são motivos de 50% a 70% dos problemas em redes. Analisando o impacto, uma disposição organizada e flexível das estruturas de conexão de uma rede é um ponto essencial para o funcionamento bem sucedido, com custo irrelevante.

6.1. Subsistemas de Cabeamento Estruturado

Podemos subdividir a infraestrutura de cabeamento em etapas, para que seja analisadas e estudadas separadamente. Cada subsistema contém normas e convenções específicas que devem ser observadas e aplicadas.

- **SET (Sala de Entrada de Telecomunicações – *Entrance Facility*)**

É representada pelo local de entrada do cabo da empresa provedora de serviços. O cabo tem origem da fiação urbana e adentra na empresa por algum cômodo. Neste ponto, há o encontro com a infraestrutura do edifício, iniciando então a comunicação interna da organização. Pode também representar a ligação de um edifício com outros edifícios, dentro de um complexo. A SET recebe desde *links* de internet até cabos telefônicos.



- **SEQ (Sala de Equipamentos – *Equipament Room*)**

Sala central de toda a comunicação interna, com prumo vertical. Possui os equipamentos de telecomunicações de grandes capacidades como *switches* centrais, roteadores, centrais telefônicas, central de CFTV, etc. As recomendações abrangem temperatura (18º a 24º), umidade relativa (30 a 55%), iluminação (540 lux), área (mínimo de 14 m²) e presença de piso anti-estático. É comum estar no mesmo local da sala de entrada de telecomunicações. Em um cenário ideal, a sala de equipamentos deve ter acesso físico controlado, se possível, proibido, salvo extrema necessidade.

- **AT (Armário de Telecomunicações – *Telecommunication Room*)**

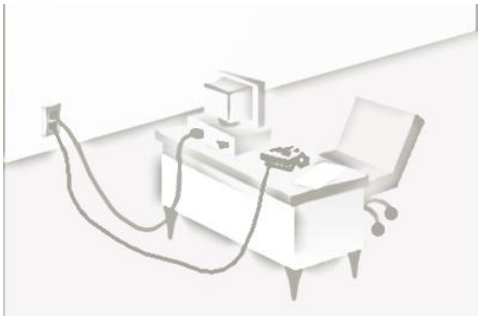
É inviável lançar cabos a partir da SEQ para os pontos de redes do edifício. Por isso, é criado um segundo nível hierárquico representado pelos armários de telecomunicações. Eles ficam espalhados pelos andares, geralmente na forma de Racks alojando equipamentos ativos básicos, com a função de distribuir o fluxo de cabos vindo da SEQ. Recomenda-se as mesmas condições de ambiente da SEQ, sendo 1 AT para 1000 m² de área útil.

- **CP (Cabeamento Primário – *Backbone Cabling*)**

Cabo fundamental na estrutura de rede, interligando salas de equipamentos, armários de telecomunicações. Referenciado também como Cabo Vertical em uma visão térrea da SEQ, contém limites de lançamentos definidos em 90 m para dados e 800 m para voz (cabos UTP). Para fibras óticas, a distância varia de 2 a 3 km.

- **ATR (Área de Trabalho – *Work Area*)**

Destino final da estrutura de cabeamento estruturado, compreendendo o espaço destinado ao trabalho do usuário, onde o mesmo faz uso de seus dispositivos de telecomunicações como computadores, telefones, impressoras de rede, aparelhos de fax cabos de adaptação, etc. Em termos gerais, compreende 10 m².



- **CS (Cabeamento Secundário – *Horizontal Cabling*)**

É o cabeamento que estende dos armários de telecomunicações terminando em uma tomada na área de trabalho do usuário. Deve ter lance máximo de 90 m, abrangendo cabos UTP, FTP, Fibras óticas, e cabos coaxiais.

- **PT (Ponto de Telecomunicações – *Telecommunication Point*)**

Terminação que recebe o cabeamento secundário vindo do armário de telecomunicações. A recomendação das áreas de trabalho é conter um mínimo de 2 pontos de telecomunicações, que pode ser associada para tráfego de voz e dados separadamente.

6.2. Normas de Cabeamento Estruturado

Para uma melhor organização sobre a atividade de implantação da rede, foram elaboradas ao longo do tempo inúmeras normas e convenções específicas de cada aplicação, sob responsabilidade de órgãos internacionais ou locais, dos quais podemos destacar:

- ABNT (Associação Brasileira de Normas Técnicas)
- ANSI (*American National Standards Institute*)
- ISO (*International Organization for Standardization*)
- IEC (*International Electrotechnical Commission*)
- ITU (*International Telecommunications Union*)
- EIA (*Eletronic Industries Alliance*)
- TIA (*Telecommunications Industries Association*)
- IEEE (*Institute of Electrical and Electronics Engineers*)
- IETF (*Internet Engineering Task Force*)
- BICSI (*Building Industry Consulting Service International*)

No Brasil, na maioria dos casos, são praticadas as normas americanas ANSI, as quais serviram de base para elaboração de normas ABNT. Em nível internacional, são praticadas as normas ISO e IEC, também representadas legalmente no Brasil pela ABNT.

- **ABNT NBR 14565**

Norma brasileira surgida em 1994 e publicada em 2000, baseada em normas americanas de administração de redes e estruturação do cabeamento. Aplica-se a prédios comerciais, situados no mesmo terreno, envolvendo salas de equipamento, armário de telecomunicações, entre outros. Abrange também uma documentação extensa para uma rede, incluindo etiquetas, placas de identificação, planta dos pavimentos, etc.

- **ANSI EIA/TIA 568 B**

Foi a primeira norma elaborada para cabeamento estruturado, em 1991. É uma norma aberta, não contendo marcas de nenhum fabricante particular. Especifica um cabeamento genérico para telecomunicações em edifícios comerciais, com definições do meio físico utilizado, pontos de trabalho e localização. Foi revisada em 1995, incluindo em seus itens normas para tomadas

internas, conexão entre prédios e cabeamento em *campus*. A revisão abrangeu também 3 TSB (*Telecommunications Systems Bulletin*), espécies de boletins anteriores de atualização, contendo informações adicionais sobre cabos UTP e STP.

- **ANSI EIA/TIA 569**

Norma de 1998, bastante conhecida entre profissionais, pois especifica edificação dos caminhos que a rede deve percorrer e espaços de telecomunicações em edifícios comerciais, o que definiu a sala de equipamentos. Contém informações sobre a área ocupada pelos elementos do cabeamento estruturado, as dimensões e taxa de ocupação dos encaminhamentos e demais informações construtivas.

- **ANSI EIA/TIA 606**

Norma de 2002, específica para administração de infraestrutura de telecomunicações em edifícios comerciais. Contém instruções de gerenciamento de redes, riscos, eventos, recursos, etc. Tem grande foco na documentação da rede, para esclarecimento da estrutura e identificação dos componentes.

- **ANSI EIA/TIA 607**

Norma de 2002 que trata sobre instalação de sistema de aterramento elétrico de telecomunicações contra descargas atmosféricas sobre o cabeamento metálico.

- **ANSI EIA/TIA 570 A**

Semelhante à norma ANSI EIA/TIA 569, porém voltado para edifícios residenciais, bem como casas individuais.

- **EIA/TIA TSB 72**

Boletim de 1995 que trata especificamente de gerenciamento, componente e performances de transmissão em cabos ópticos.

- **TIA 942**

Norma para projetos de *datacenter*, incluindo topologias, infraestrutura e elementos componentes. É bastante abrangente, com referências para proteção contra incêndios, segurança, construção civil, controle ambiental e qualidade de energia

- **ISO/IEC 11801**

Norma europeia para cabeamento estruturado, equivalente a norma ANSI EIA/TIA 568 B.

- **TIA 1179**

Contém especificações de cabeamento, topologias, distâncias, trechos, áreas de trabalho e outros requisitos complementares para implantação da infraestrutura em instalações sanitárias. Foi criada baseando-se na complexidade do ambiente sanitário em relação a edifícios comerciais padrão.

- **ANSI/BICSI 005-2013**

Abrange toda a infraestrutura de cabeamento no que se refere a segurança eletrônica e espaços correspondentes. A norma traz orientações importantes como práticas de instalação, alturas de montagem dos dispositivos de segurança, sistemas de vigilância eletrônica, alarme e detecção de incêndio, integração de sistemas e análise e gerenciamento de riscos.

RESUMÃO

- Cabeamento estruturado é um estudo para organizar e padronizar a rede da melhor forma possível.
- As normas foram criadas para evitar que cada um monte uma rede corporativa do seu jeito.
- No Brasil são adotadas as normas americanas. No resto do mundo, são adotadas normas americanas e dos órgãos ISO e IEC.
- Cada norma é específica, abrangendo redes comerciais, residências, redes ópticas, etc.

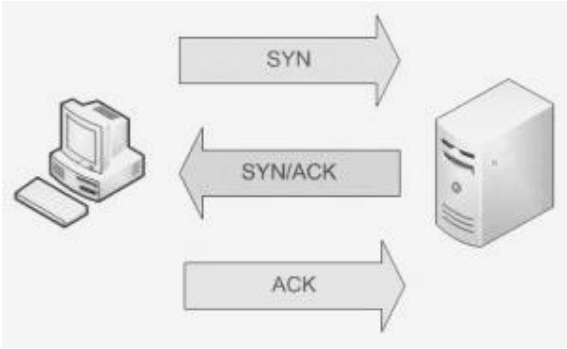
ALÉM DISSO...

Já ouviu falar em RFC (*Request for Comments*)? Embora não seja propriamente uma norma, é um documento numerado que especifica uma tecnologia (por exemplo, redes sem fio). As RFC's foram reunidas pelo IETF, num grande glossário, formando manuais para padrões de comunicação e protocolos diversos, os quais veremos alguns no próximo capítulo. Para saber mais, visite http://www.ietf.org/rfc.html.

7. PROTOCOLOS DE REDE

Os protocolos são um conjunto de regras e procedimentos padronizados que os componentes de rede utilizam para se comunicarem. Por exemplo, para receber ou enviar uma mensagem de correio eletrônico há etapas pré-definidas e ações já determinadas que servidores de e-mail adotam baseados em protocolos. Podemos fazer uma analogia com seres humanos, que para se comunicarem utilizam certo padrão (Língua Portuguesa), onde transmissor e receptor conhecem e aceitam a mesma linguagem de comunicação. Da mesma forma, os componentes de rede precisam trabalhar com protocolos idênticos para haver comunicação entre eles.

- **TCP (*Transmission Control Protocol*)**



Protocolo usado na transmissão de pacotes na rede, definido pela RFC 793. É um protocolo orientado à conexão, ou seja, é necessário haver uma conexão estabelecida para a transmissão dos dados, do contrário, o envio de pacotes é interrompido. Dessa forma, o TCP garante a entrega de todos os pacotes ao seu destino, inclusive retransmitindo os pacotes que não chegarem por algum motivo. Alguns exemplos de aplicações que utilizam TCP são o correio eletrônico e a transferência de arquivos. Para estabelecer conexão, as máquinas realizam um procedimento conhecido como *three-way handshake* (algo como "cumprimento de 3 vias"), representado na figura acima. O cliente envia um pacote numerado pedindo sincronização (*SYNcronization*) com o servidor. O servidor responde com outro pacote reconhecendo (*ACKnowledgement)* o pedido, informando seu número para sincronização. O cliente responde com outro pacote de reconhecimento. Cliente e servidor contêm numerações diferentes, por isso a necessidade de sincronização em ambos os lados. Fazendo uma analogia com uma conversa humana, teríamos:

Cliente	*Servidor, estou enviando a mensagem 100 (Número de sequência do cliente). Dá pra sincronizar (SYN)?*
Servidor	*Claro, sincroniza a mensagem 200 (Número de sequência do servidor) que estou enviando (SYN). Prossiga com a mensagem 101 (ACK).*
Cliente	*Ok, estou enviando a mensagem 101. Prossiga com a mensagem 201 (ACK).*

- **UDP (*User Datagram Protocol*)**

Descrito na RFC 768, é um protocolo usado na transmissão de pacotes, assim como o TCP. Diferencia-se por não ser orientado à conexão, não necessitando de "cumprimentos" entre os

componentes para envio de pacotes. Também não faz verificação de entrega dos pacotes, não os retransmitindo quando estes não chegam ao destino. Por estes motivos, o protocolo UDP é bastante utilizado em aplicações de alta velocidade como *streaming* de vídeos ou músicas, conversas por VOIP, etc.

- **HTTP (*Hyper Text Transfer Protocol*)**

Protocolo usado para aplicações relacionadas ao servidor *web*, como navegação de páginas. Sua implementação derivou o WWW (*World Wide Web*), serviço da Internet que interliga milhões de dispositivos pelo mundo, trocando hipermídias, de modo colaborativo, permitindo que figuras ou vídeos sejam visualizados num *browser* próprio para leitura das informações. A primeira versão do protocolo foi especificada na RFC 2616. Os pacotes HTTP são transportados por um protocolo de transporte (TCP ou UDP).

- **HTTPS (*Hyper Text Transfer Protocol Secure*)**

Implementa uma camada de segurança, a SSL (*Secure Sockets Layer*), para navegação entre páginas de modo criptografado, especificada na RFC 2960. Cliente e servidor compartilham uma chave de segurança para transportar informações por via seguras. É amplamente utilizado em sistemas de identificação de usuário, páginas de instituições financeiras, comércio eletrônico, etc.

- **SMTP (*Simple Mail Transfer Protocol*)**

Protocolo especificado na RFC 2821, usado para envio de correio eletrônico. Seu funcionamento é simples, concebido para textos simples, onde um ou vários destinatários são referenciados e validados e, posteriormente, a mensagem enviada. Utiliza TCP para transporte dos dados, pois necessita garantir a entrega de todos os pacotes.

- **POP (*Post Office Protocol*)**

Definido na RFC 1939, é o protocolo que permite o acesso remoto a um servidor de correio eletrônico, para leitura das mensagens. O POP permite também a transferência das mensagens do servidor para um software leitor instalado localmente na máquina do usuário (chamado de *User Agent*). Ao optar por ler as mensagens de modo local, o protocolo POP traz as mensagens remotas, sem conservar uma cópia delas no servidor.

- **IMAP (*Internet Message Access Protocol*)**

O protocolo IMAP, definido na RFC 1730, trabalha de modo semelhante ao POP, porém ao trazer as mensagens remotas, ele conserva uma cópia delas no servidor. Além disso, o IMAP oferece mais possibilidades como permitir vários acessos simultâneos ao servidor ou gerir várias caixas de correio eletrônico. Conhecendo então os protocolos de envio e recebimento de correio

eletrônico (SMTP, POP e IMAP) e o protocolo de transporte TCP, podemos formular o seguinte exemplo para ilustrar o funcionamento do serviço de entrega de mensagens da Internet:

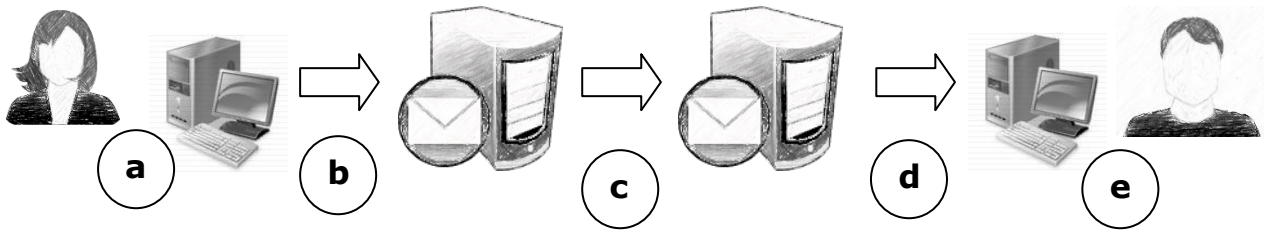
a) Maria usa o *User Agent* para compor uma mensagem "para" ***joao@tableau.com.br***.

b) O *User Agent* de Maria envia a mensagem para o seu servidor de correio; a mensagem é colocada na fila de mensagens.

c) O servidor SMTP de Maria abre uma conexão TCP (*three-way handshake*) com o servidor POP ou IMAP de João; a mensagem é enviada.

d) O servidor POP ou IMAP de João coloca a mensagem na sua caixa de entrada.

f) João chama o seu *User Agent* para ler a mensagem.



- **FTP (*File Transfer Protocol*)**

Especificada na RFC 959, é protocolo padrão para a transferência de arquivos entre computadores, utilizando TCP. Só permite a transferência de arquivos completos, sendo assim, qualquer falha que ocorra na transmissão, os pacotes que já haviam chegado ao destino são destruídos.

- **TelNet**

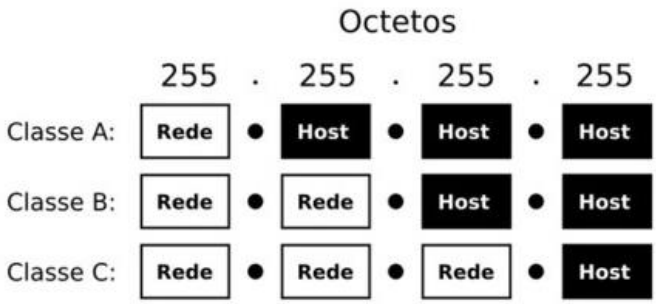
Está definido na RFC 854, porém contém várias outras RFCs especificando outras opções do TelNet. Trata-se de um protocolo para conexão remota entre estações. Baseia-se em TCP para enviar dados em formato ASCII (um código numérico para representar caracteres). De posse do controle remoto da máquina, era possível utilizar uma aplicação lá alojada ou transferir arquivos por exemplo.

- **NTP (*Network Time Protocol*)**

Protocolo utilizado para sincronização dos relógios de computadores, utilizando protocolo UDP. Baseia-se em uma fonte de hora confiável, trocando mensagens entre várias máquinas sincronizando-as.

- **IP (*Internet Protocol*)**

Protocolo vital para o funcionamento da rede, definido na RFC 791, responsável pelo endereçamento de pacotes. Ao enviarmos dados, os pacotes são numerados com informações



importantes para os componentes, entre elas, o endereço IP de origem e destino, o que permite seu direcionamento e controle de tráfego. Um endereço IP é composto por 4 octetos (4 grupos de 8 bits) representados por decimais e separados por pontos na forma X.Y.Z.W, com a função de identificar a rede (Net ID) a qual o equipamento pertence e o próprio equipamento (Host ID). O menor endereço possível é 0.0.0.0 e o maior é 255.255.255.255. A identificação da rede é concedida no Brasil pela FAPESP (Fundação de Amparo a Pesquisa do Estado de São Paulo) e, a nível internacional, pela ARIN (*American Registry for Internet Numbers*), já a identificação do equipamento é definida pelo administrador de redes local. A combinação é exclusiva, isto é, um endereço IP não se repete em uma mesma rede.

Existem 5 classificações para endereços IP, definidas na RFC 1365: Classe A, B, C, D e E. Usualmente, aplicamos as classes A, B e C. O que as diferencia é a quantidade de números para identificar rede e equipamento.

A classe A possui capacidade para endereçar 128 redes com até 16.777.216 estações cada uma. A classe B possui endereços para 16.284 redes com até 65.536 estações cada. Já a classe C tem capacidade para 2.097.152 com até 256 estações cada. Na tabela abaixo está a relação de endereços de cada classe.

Classe	Início	Fim	Endereços inválidos
A	1.0.0.1	126.255.255.254	10.0.0.0 – 10.255.255.255
B	128.0.0.1	191.255.255.254	172.16.0.0 – 172.31.255.255
C	192.0.0.1	223.255.255.254	192.168.0.0 – 192.168.255.255
D	224.0.0.0	239.255.255.255	*Multicast*
E	240.0.0.0	255.255.255.255	Para uso futuro. Atualmente usado para testes.

Nota-se que o primeiro endereço (final zero) e o último (final 255) não são utilizados por se tratarem de endereços reservados como endereço de rede e endereço de *broadcast* (sinal enviado para todas as máquinas), respectivamente, não podendo, portanto, ser atribuída a nenhuma interface. A classe D é reservada para *multicast* (sinal enviado para várias máquinas) e a classe E é usada para testes do IETF, reservado para o futuro. Há uma faixa de endereços especial que vai de 127.0.0.1 a 127.0.0.254, reservados para *loopback*, um tipo de sinal especial que é enviado e recebido pelo mesmo dispositivo. Na maioria dos sistemas, adota-se o endereço 127.0.0.1. Em sistemas Linux, a interface *loopback* é chamada *lo* ou *lo0*, em outros

casos, atribui-se, embora tecnicamente errado, o nome de *localhost*. Por fim temos os endereços inválidos ou privados que são usados em redes domésticas ou corporativas de modo interno e particular, sem contato com a rede pública. Mais detalhes sobre endereços IP especiais estão descritos na RFC 3330.

- **IPX/SPX (*Internetwork Packet Exchange/Sequenced Packet Exchange*)**

Protocolos proprietário da Novell, empresa de software americana na área de redes, também proprietária do Sistema Linux Suse e do Sistema Operacional de Rede Netware, famoso na década de 80. Muito usado inicialmente, hoje está obsoleto, porém ainda em uso, pois há dispositivos antigos que só conseguem se comunicar através dele. O IPX atua como o IP, fornecendo endereçamento na rede, composto por 32 bits, representados em hexadecimal (ex: AAAAAAAA 00001B1EA1A1 0451) Já o SPX, atua como o TCP, transportando dados pela rede e sendo orientado à conexão.

- **IRC (*Internet Relay Chat*)**

Protocolo de comunicação definido na RFC 1459, bastante utilizado para bate-papo e troca de arquivos, permitindo a conversa em grupo ou privada. Foi muito popular no final dos anos 90 e início de 2000 com o software mIRC, perdendo espaço posteriormente para mensageiros instantâneos com mais possibilidades (conversa com webcam e voz, integração com correio eletrônico, jogos, etc).

- **SNMP (*Simple Network Management Protocol*)**

Protocolo de gerenciamento de redes, extremamente útil para administradores, pois facilita a troca de informações entre os componentes de rede. Com ele, o administrador de rede pode mensurar desempenho, encontrar problemas, gerenciar eventos, visualizar gráficos, etc.

- **DNS (*Domain Name System*)**

Protocolo definido nas RFCs 882 e 883 (atualizado nas RFCs 1034 e 1035), exerce um papel importante. Cada componente na rede possui um endereço IP de localização, assim como as páginas da Web. Quando desejamos acessar uma determinada página, normalmente digitamos o nome desta página. O protocolo DNS, juntamente com o servidor DNS, tem o trabalho de resolver o nome, procurando seu IP correspondente, consultando suas bases e também outros servidores pela rede. Sem o DNS, só conseguiríamos acessar páginas e dispositivos pelo IP. (Experimente abrir o navegador, digitar 74.125.196.94 e pressionar ENTER).

- **ICMP (*Internet Control Message Protocol*)**

Definido na RFC 792, é um protocolo para transmitir relatórios de erros pela rede, causados pelo protocolo IP. É bastante conhecido entre *hackers* e *crackers* sendo usado em ataques de

negação de serviço (DoS). Também é bastante útil para comandos *ping* (usado basicamente para verificação estados de dispositivos) e *tracert* (traça rotas dos pacotes até seu destino).

- **DHCP (*Dynamic Host Configuration Protocol*)**

Tem a função de controlar e disponibilizar endereços IP para os dispositivos que os requisitam. O administrador de redes local define uma faixa de endereços e o servidor DHCP oferece endereços IP dentro dessa faixa, sempre que algum dispositivo solicita. A maior vantagem está na comodidade do administrador em não ter que definir IP fixo para cada componente, sendo este atribuído de modo dinâmico e automático. Como desvantagem, atribui-se a perda de controle sobre a identidade de quem se conecta na rede. Está definido na RFC 2131

- **ARP (*Address Resolution Protocol*)**

Todo pacote enviado pela rede, deve ser endereçado com os números IP e MAC de destino. Quando somente o IP é conhecido, o protocolo ARP envia um broadcast na rede, solicitando o endereço MAC. A operação contrária (solicitar o IP a partir do endereço MAC) é feita pelo protocolo RARP (*Reverse Address Resolution Protocol*).

- **SSH (*Secure Shell*)**

Mesmo funcionamento do protocolo TelNet, possibilitando conexão remota com outra máquina. A diferente está no modo de conexão do SSH que é criptografado. A mais conhecida aplicação de SSH é a VPN (*Virtual Private Network*) que, com o recurso de *tunelling* (tunelamento), permite transportar dados por vias extremamente seguras. Para sistemas Windows, há o cliente PuTTY, permitindo facilmente abrir conexões TelNet e SSH.

7.1. Portas de protocolos

As portas lógicas permitem que vários programas estejam em funcionamento ao mesmo tempo, na mesma máquina, trocando informações com serviços. Cada é porta é identificada com um número, existindo um total de 65535 portas; os protocolos são associados a uma porta específica. As portas de 1 a 1023 são reservadas a protocolos bem conhecidos e bastante utilizados. As portas mais altas (>1023) são destinadas para estabelecimento de conexões de serviços nos clientes. Por definição, nenhum protocolo ou serviço é associado às portas 49152 até 65535. Uma curiosidade é que o Brasil alterou no início de 2013 a porta SMTP para reduzir o número de *spams* (mensagens de correio eletrônico indesejadas ou maliciosas), fechando a porta 25 e abrindo a porta 587, por considerar esta mais segura. Com a medida, leitores de mensagens como o *Outlook* da Microsoft tiveram que alterar suas configurações. *Webmails* como o Gmail da Google ou o Hotmail da Microsoft não foram afetados.

Porta	Protocolo	Porta	Protocolo	Porta	Protocolo
20/21	FTP	80/81	HTTP	194	IRC
23	TelNet	109/110	POP / POP3	213	IPX
22	SSH	123	NTP	443	HTTPS
25	SMTP	143	IMAP	546/547	DHCP
53	DNS	161	SNMP		

RESUMÃO

- Protocolos são "idiomas" que os computadores e dispositivos de rede utilizam para conversarem, se entenderem e conseguir realizar as tarefas.
- O mais importante talvez seja o IP, responsável por endereçar a informação para destino correto.

ALÉM DISSO...

Os endereços IP versão 4 estavam ficando escassos devido quantidade de novos dispositivos e redes que surgiam constantemente. Pensando nisso, foi lançado em 2012 o IPv6, 6ª versão do protocolo IP que veio para solucionar a falta de endereços na Internet, pois os cerca de 4,3 bilhões de endereços IPv4 estavam acabando. Em uma analogia, o IPv4 seria um copo de água de 200ml, enquanto o IPv6 seria o Oceano Pacífico, o maior da Terra. É muito IP!

VADE MECUM

- Por que existem tantos protocolos?
- O que consigo fazer através dos protocolos?

8. MODELOS DE REFERÊNCIA EM ARQUITETURA DE REDES

Conceitualmente o modelo de comunicação em redes se dá através de camadas, sendo cada camada vista como uma etapa, onde acontece determinada ação que integra todo o processo de comunicação. O modelo de camadas ou modelo de referência são pilhas de protocolos, que são propostos para estabelecer regras de tratamento de dados por etapas, onde pode haver variações de tempo, tamanho dos pacotes, etc. A divisão em camadas facilita a compreensão de todo o problema detalhando partes do mesmo.

8.1. Modelo OSI (*Open Systems Interconnection*)

Define um modelo genérico composto por 7 camadas. Foi proposto na década de 70/80 quando não havia padrões de comunicação entre hardwares de diferentes fabricantes. Na prática, é utilizado para fins didáticos apenas, sendo inadequado para implementação, pois não especifica com exatidão os serviços e protocolos que devem ser utilizados em cada camada, simplesmente declara o que cada elemento faz e não como faz. Para entender o conceito de camadas podemos fazer uma analogia com o sistema postal, na tabela abaixo.

Usuário envia a carta	⟷	Usuário recebe a carta
Carteiro coleta	⟷	Carteiro entrega
Triagem (encaminhamento)	⟷	Triagem (recebimento)
Serviço de malote	⟷	Serviço de malote

Cada camada do modelo OSI presta serviços à camada superior. Na transmissão de informações uma camada recebe dados repassados pela sua camada superior, faz um tratamento desses dados e repassa para a camada de baixo. As camadas da pilha de transmissão se comunicam apenas com as mesmas camadas de recepção da mensagem. Cada camada possui protocolos próprios, destinados aos serviços daquela etapa

- **Camada de Aplicação**

Camada mais alta, responsável por reconhecer e manipular o protocolo de aplicação que está sendo utilizado, bem como estabelecer regras para a troca de mensagens entre as aplicações. Funciona como uma grande janela para executar as aplicações finais (geralmente executada por usuários) que tem como suporte o acesso à rede e seus serviços. Os protocolos conhecidos atuantes nessa camada são o HTTP, FTP, SMTP, POP, entre outros.

- **Camada de Apresentação**

Na transmissão, esta camada tem a função de capturar os dados da aplicação e formata-los de maneira que possa ser repassada para a camada de baixo já tratados para o envio. Na recepção da mensagem, essa camada recebe dados da camada inferior e trata-os para que sejam exibidos ao usuário corretamente e num formato inteligível. E também conhecida como camada de tradução por tratar a semântica e sintaxe das informações (acentos, caracteres especiais, etc) e não apenas bits de rede.

- **Camada de Sessão**

Responsável por estabelecer, gerenciar e encerrar conexões entre aplicações de diferentes máquinas, fazendo sincronização entre os dispositivos, além de realizar controle de tráfego. Em casos de autenticação, a camada de sessão faz o controle de quais usuários podem realizar conexões ou não. Em transferências de arquivos grandes, a sessão insere pontos de sincronismo nos arquivos já baixados para, em caso de falha, não ter que transferir tudo novamente.

- **Camada de Transporte**

Após a sessão estabelecida, os dados são entregues a camada de transporte que é responsável por dividir as informações em pedaços menores para trafegá-los. Também faz o controle de fluxo para evitar que uma máquina rápida sobrecarregue outra mais lenta com envios de pacotes em massa. No receptor, a camada de transporte tem a função de receber os pacotes que chegam, colocá-los em ordem, remontá-los e repassar para a camada de sessão. Na camada de transporte estão os protocolos TCP e UDP (ou SPX para redes Novell).

- **Camada de Rede**

Tem importância crucial, endereçando origem e destino dos pacotes entregues pela camada de transporte e realizando controle de congestionamento da rede. Controla as operações da rede de um modo geral, criando rotas e monitorando o percurso dos pacotes pelo seu endereço. É nesta camada que ficam localizados os roteadores da rede, concentradores de alta influência no fluxo geral da rede. Trabalha com os protocolos IP, ARP, RARP e ICMP.

- **Camada de Dados**

Também chamada de Enlace de Dados, esta camada tem a função de conferência, correção de erros contidos nos pacotes recebidos da camada de rede e inserção de novas informações. Os dados aqui são chamados de quadros e recebem endereços de origem e destino, bem como o controle de erros. Diferentemente da camada de rede, não trabalha com IP e sim com endereços MAC, no formato hexadecimal, identificando as placas de rede transmissora e

receptora. A maioria dos *switches* trabalha aqui, embora alguns modelos operem na camada de rede. O controle de fluxo para evitar congestionamento é feita por uma subcamada chamada LLC (*Link Logical Control*).

- **Camada de Rede**

Refere-se diretamente ao meio físico utilizado e outros equipamentos. Aqui os dados são bits brutos (0 e 1), operados entre *hubs*, repetidores, cabos metálicos e fibras óticas. A função básica é transmitir e receber pulsos elétricos ou ópticos que serão convertidos para bits através de moduladores. Seu principal dispositivo é o NIC, sendo assim, diz respeito apenas ao meio usado para transmitir e receber, sem considerar onde os dados trafegam.

8.2. Modelo TCP/IP

Tornou-se um padrão na década de 70 e logo se tornou popular, sendo o modelo atualmente usado na Internet e em redes gerais. Possui arquitetura aberta, não contendo marcas específicas de fabricantes de *hardware*. Baseia-se em 4 camadas, em oposição às 7 camadas do modelo OSI. Algumas camadas TCP/IP realizam implicitamente a função de camadas do modelo OSI, justificando seu número reduzido. Cada camada TCP/IP possui seus protocolos, sendo o protocolo TCP atuante na camada de transporte e o protocolo IP atuante na camada de Internet. Os dois protocolos se completam nas operações, com o IP endereçando os dados e o TCP controlando o tráfego e transportando pacotes. Na figura abaixo, podemos ver uma representação gráfica de um pacote TCP/IP

<table>
<tr><td colspan="5">Porta origem</td><td colspan="3">Porta destino</td></tr>
<tr><td colspan="8">Número de sequência</td></tr>
<tr><td colspan="8">Número de confirmação</td></tr>
<tr><td>Header size</td><td>Reservado</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Tamanho da janela</td></tr>
<tr><td colspan="5">Checksum</td><td colspan="3">Urgent pointer</td></tr>
<tr><td colspan="8">Opções (tamanho variável)</td></tr>
<tr><td colspan="8">Dados (tamanho variável)</td></tr>
</table>

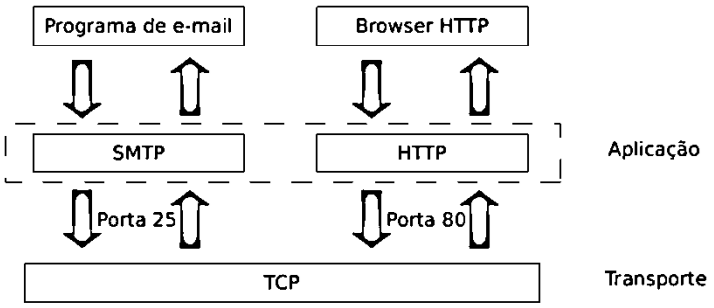
- PORTA ORIGEM: Porta do programa de aplicação que está enviando o pacote;
- PORTA DESTINO: Porta do programa de aplicação de destino;
- NÚMERO DE SEQUÊNCIA: Posição deste segmento no fluxo de dados;
- NÚMERO DE CONFIRMAÇÃO: Especifica o próximo segmento aguardado;

- HEADER SIZE: Tamanho do cabeçalho em números de palavras de 32 *bits*;
- URG: Valor 1 se houve informação no campo Urgent Pointer;
- ACK: Valor 1 indica confirmação de recebimento do segmento;
- PSH: Campo usado para indicar que o segmento deve ser entregue imediatamente;
- RST: Utilizado para reiniciar uma conexão;
- SYN: Usado junto com o ACK para solicitar ou aceitar uma conexão;
- FIN: Usado para encerrar uma conexão;
- TAMANHO DA JANELA: Indica o tamanho disponível do buffer do receptor;
- CHECKSUM: Verificação de erros;
- URGENT POINTER: Usado para indicar onde se encontra algum dado urgente;
- OPÇÕES: Campo para configuração de opções;
- DADOS: Dados das aplicações.

- **Camada de Aplicação**

Equivalente às camadas de aplicação, apresentação e sessão do modelo OSI, operando protocolos HTTP, SMTP, FTP, POP, DNS, entre outros. Tem a mesma função de estabelecer uma interface com a tarefa do usuário, adequando-se às especificações do tipo de aplicação em questão. As aplicações no modelo TCP/IP não possuem padronização comum, sendo atribuído para cada uma, um RFC. O controle é feito através das portas de cada protocolo.

- **Camada de Transporte**



Responsável por receber os dados da aplicação, transformá-los em pacotes e entregá-los para a camada inferior, operando os protocolos TCP e UDP. A escolha de qual serviço de transporte utilizar depende da aplicação, considerando tolerância ou não de perda de dados, requisitos temporais e largura de banda necessária.

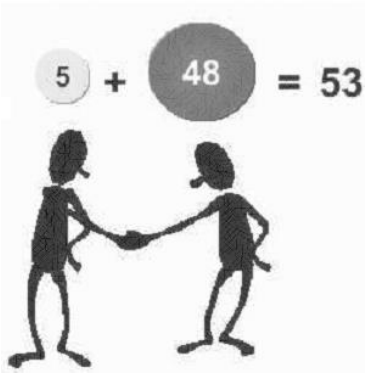
- **Camada de Internet**

Equivalente à camada de rede do modelo OSI, com a função básica de roteamento e endereçamento, operando os protocolos IP, ICMP e ARP. Define as rotas de transporte, gerencia o tráfego de dados, controla e previne o congestionamento e efetua tradução de nomes lógicos (IP) para nomes físicos (MAC). Os dados aqui são chamados de datagramas que são entregues à camada de interface com a rede para serem transmitido pelo meio físico.

- **Camada de Interface com a Rede**

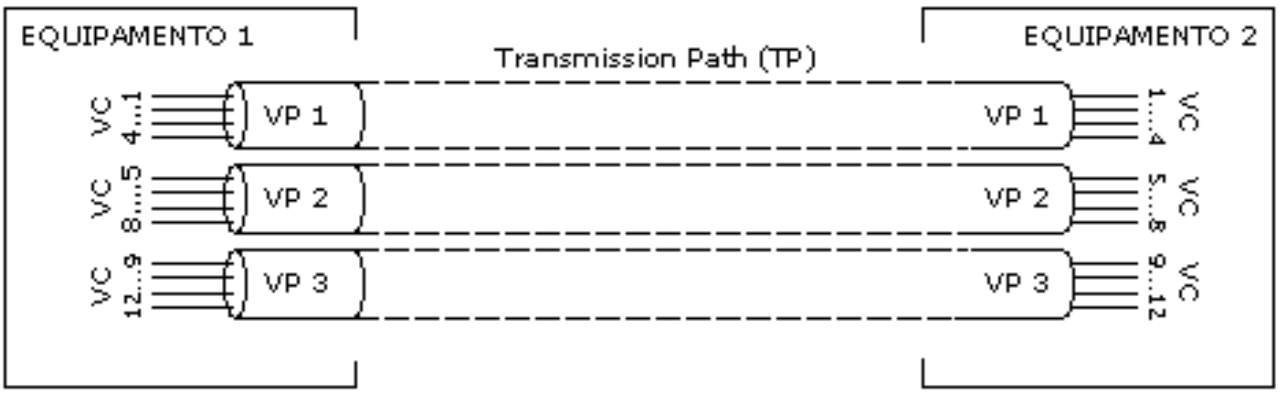
Equivalente às camadas de enlace de dados e físca do modelo OSI, esta camada não é bem especificada, limitando-se ao meio físico utilizado para transmitir. São utilizados aqui, padrões de rede definidos pelo IEEE, sendo alguns exemplos o padrão 802.3 *Ethernet* (redes cabeadas), padrão 805.5 *Token Ring* (redes em anel), padrão 802.11 *Wireless* (redes sem fio), padrão 802.15.1 *Bluetooth* ou 802.15.4 *Zigbee* (redes sem fio de curta distância e baixo consumo de energia) e padrão 802.16 *WiMax* (redes sem fio de altíssima velocidade).

8.3. Modelo ATM (*Asynchronous Transfer Mode*)



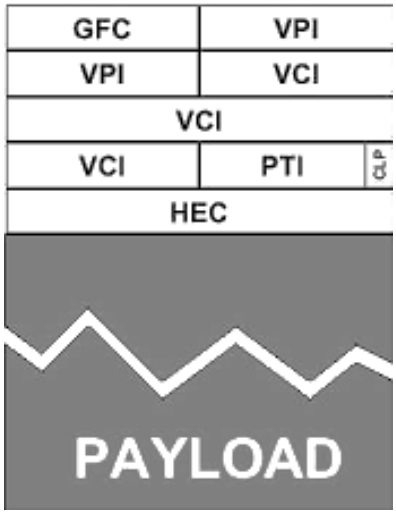
Modelo de redes de alta velocidade composto por 3 camadas, largamente usado em sistemas de telecomunicação de longa distância e operadoras de serviços digitais integrados, transmitindo dados, voz e vídeo em uma única estrutura de rede. Caracteriza-se por não trafegar pacotes e sim estruturas chamadas células com tamanho de 53 bytes. O tamanho das células ATM vem de um acordo entre americanos que desejavam 64 bytes com cabeçalho e europeus com proposta de 32 bytes com cabeçalho, chegando então a 48 (32+64/2) bytes + 5 bytes de cabeçalho. Grande parte de sua estrutura é constituída de fibra ótica, garantindo alto desempenho, baixo atrasos e margem mínima de erros. Atinge velocidade de 25 Mbps a mais de 622 Mbps, embora cogita-se chegar de 2Gbps a 10 Gbps em alguns tipos de fibras.

Redes ATM trabalham com um conceito chamado *Virtual Connections*, onde temos 3 componentes integrados. O *Transmission Path* (TP) é a rota de transmissão física entre equipamentos da rede ATM. O *Virtual Path* (VP) é a rota virtual configurada na infraestrutura TP, que pode conter vários VP's. O *Virtual Channel* (VC) é o canal virtual configurado na infraestrutura VP, que pode conter vários VC's. Fazendo uma analogia automobilística, enquanto o VP seria uma pista de corrida, os VC's seriam as faixas de rolagem. Cada componente contém um identificador único (VPI e VCI) para os dados trafegados, sendo estes utilizados no roteamento de células ATM para determinar endereços de origem e destino.



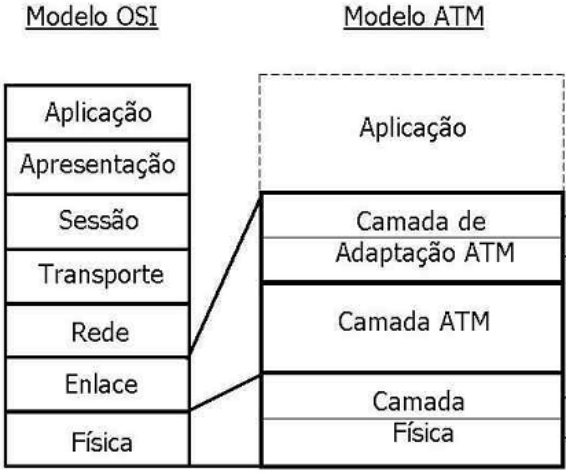
Redes ATM são orientadas à conexões, onde o pedido de conexão é feito através de sinalização onde uma célula é enviada pelo remetente, solicitando o procedimento. Caso seja aceito pelo destinatário, é estabelecido uma *Virtual Channel Connection* (VCC) e uma *Virtual Path Connection* (VPC). As conexões ATM são em sua maioria ponto-a-ponto, embora haja um pequeno uso entre computadores e servidores de alta performance.

A célula ATM é representada na figura abaixo. A área de cabeçalho carrega informações de controle com mecanismos de detecção e correção de erros com 5 bytes (40 bits) de tamanho. O VPI (*Virtual Path Identifier*) com 12 bits e o VCI (*Virtual Channel Identifier*) com 16 bits carregam endereços de origem e destino, necessário para o roteamento das células. GFC (*Generic Flow Control*) com 4 bits identifica o tipo de célula para a rede. O PTI (*Payload Type Identifier*) com 3 bits carrega informações sobre o tipo de dados que a célula contém: de usuário, de sinalização ou de manutenção. A CLP (*Cell Loss Priority*) com 1 bit indica a prioridade da célula na qual células de menor prioridade são descartadas durante congestionamentos. O campo HEC (*Header Error Check*) com 8 bits é usado para detectar e corrigir erros no cabeçalho. O *payload* representa a área útil para tráfego de dados. A informação é mantida intacta ao longo da rede, sem passar por correções ou verificações de erro.



- **Camada AAL (*ATM Adaptation Layer*)**

A camada mais alta do modelo ATM é responsável por segmentar os dados recebdios e montar a célula ATM, preparando-a para uso da aplicação.



- **Camada ATM**

É a camada controladora, representando as camadas de rede e de transporte do modelo OSI. Determina para onde serão encaminhadas as células, além de controlar diversas funções de tráfego como por exemplo, marcação de células de baixa prioridade, indicadores de congestionamento, controles genéricos de fluxos de dados e velocidade de transmissão de dados. Para o roteamento, o modelo ATM não especifica um algoritmo particular.

- **Camada Física**

Como nas outras arquiteturas, representa o meio físico de transmissão, tendo funções como o alinhamento de bits, sinalizações na linha, conversão de sinais elétricos para sinais ópticos e geração do cabeçalho de erros. Diferentemente do modelo TCP/IP, não requer nenhum padrão específico para a camada física.

RESUMÃO

- O modelo OSI é composto por 7 camadas bem explicadas, facilitando o isolamento do problema, porém é inadequado para uso na prática, servindo apenas didaticamente.
- O modelo TCP/IP é composto por 3 camadas, usado largamente na Internet, embora não tenha robustez. Uma solução híbrida é ideal.
- O modelo ATM é usado em redes de alta velocidade, popular na Europa. No brasil é operado em telefonia de longa distância e serviços digitais integrados.

ALÉM DISSO...

Alguns padrões ainda não estão bem difundidos. Um grande exemplo é o PLC (*Power Line Communications*) ou BPL (*Broadband Power Line*) cuja transmissão de dados é feita pela rede elétrica. Isso significa que cada tomada de energia se transforma em um ponto de rede. No Brasil, alguns testes começaram com sucesso em Barreirinhas, município do Maranhão, mas não avançaram. Os últimos estudos procuravam reduzir as interferências dos muitos equipamentos elétricos (televisão, geladeira, etc) conectados junto com a rede. Outras tecnologias não muito bem definidas são o 4G, a transmissão por Infravermelho e, mais recentemente, a transmissão NFC *(Near Field Communication*). Vale a pesquisa!

VADE MECUM

- Por que existem padrões de rede?
- Posso usar ATM em rede doméstica?

9. SEGURANÇA DE REDES

A segurança é fator crucial para o sucesso de uma rede, assim como em qualquer outra área de tecnologia. Muitos são os ataques praticados e poucos são os profissionais capacitados para aplicar técnicas de segurança. Podemos apontar vários problemas como destruição de informações ou recursos, modificação de dados, roubo/perda/remoção de recursos, interrupção de serviços, etc. Uma rede desprotegida pode significar grande prejuízo não só corporativo mas também comunitário. Isso se deve ao fato da importância crescente conquistada por redes públicas e governamentais ao longo dos anos, aumentando também o interesse de atacantes em investidas contra a infraestrutura do local. Até mesmo uma guerra cibernética de grandes proporções foi cogitada após um ataque a Estônia em 2007, um país extremamente conectado e distribuído com sistemas vitais (energia, bancos, etc) funcionando à base de interligações de redes.

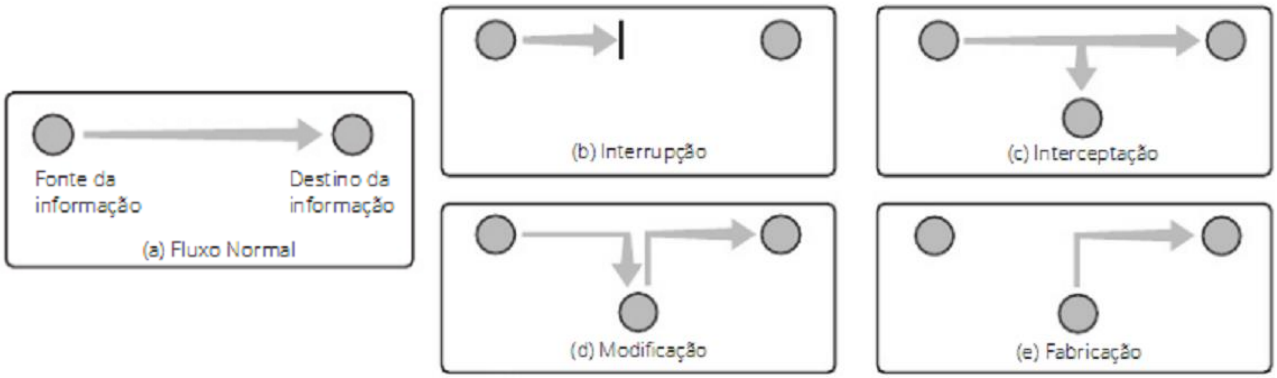
Mas o que é segurança? O que exatamente precisa ser protegido? Como proteger ativos da rede, pessoas e informações? Qual o valor da informação? As perguntas podem ser respondidas pelos próprios objetivos da segurança, seja reduzir a probabilidade de ocorrência de incidente de segurança ou recuperação rápida dos dados em caso de desastres ou incidentes. A segurança apoia-se na presentavação de 3 princípios básicos que justificam sua aplicação em cenários diversos.

- CONFIDENCIALIDADE: a informação não é passada ou revelada à pessoas não autorizadas. O objetivo é manter o sigilo e a privacidade dos dados. A informação certa comunicada às pessoas certas (na hora certa) é de importância vital.
- INTEGRIDADE: a informação não é alterada, removida ou deturpada sem autorização expressa do autor da mesma. A mensagem trafegada é original e correta.
- DISPONIBILIDADE: Os ativos, serviços e recursos estão sempre disponíveis, sem interrupções no fornecimento.

A resistência ou despreocupação em uso de técnicas de segurança em organizações ainda é alta, mesmo sendo fator determinando no rumo dos negócios. Embora historicamente haja opiniões semelhantes, a segurança jamais deve ser vista como barreira para os negócios e sim como suportador para novos empreendimentos. Graças a técnicas de segurança, foi possível implementar negócios digitais e serviços de comodidade (serviços bancários, compras, etc) baseados em *Internet*. É importante salientar que não existem sistemas totalmente seguros ou sem riscos. Ameaças e riscos não podem ser eliminados, apenas gerenciados e controlados. A segurança envolve questões gerenciais, operacionais e tecnológicas, cobrindo toda a organização e não só seus administradores. O cumprimento de normas por parte dos colaboradores é essencial.

9.1. Modelos de Ataques

Um ataque é qualquer ação que comprometa a segurança ou que afete um dos 3 princípios básicos de segurança. A ação de um atacante é tomada sempre pela existência de vulnerabilidades ou falhas que possam ser exploradas. Um exemplo de vunlenrailidade é o desconhecimento técnico de administradores de rede em alguma tecnologia ou softwares desatualizados nos ativos. A motivação para ataques é diversa, culminando em interesses comuns como dinheiro, curiosidade do atacante, razões pessoais contra a vítima, experimentos e desejos de aprender, necessidade psicológica/emocional, vingança, mentalidade maliciosa, espionagem industrial, entre muitos outros. Abaixo podemos ver modelos de ataques específicos.



- **Interrupção**

Quando um ativo é estruído ou torna-se indisponível (ou inutilizável). Alguns exemplos são a destruição de disco rígido, cortes de linhas de comunicação e ataques de negação de serviço.

- **Interceptação**

Quando um elemento não autorizado tem acesso a um ativo, afetando a confidencialidade. Alguns exemplos são escutas de cabos de comunicação, monitoramento de tráfego não autorizado e cópias ilícitas de arquivos ou *softwares*.

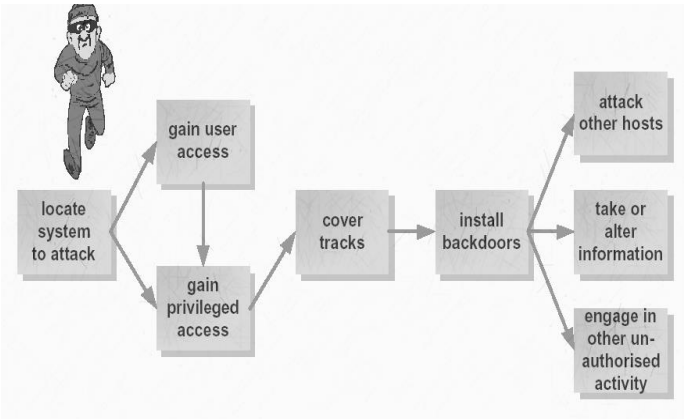
- **Modificação**

Quando um ativo é alterado por parte não autorizada, afetando a integridade. Alguns exemplos são modificações de mensagens na rede, alteração em arquivos e em valores de sistema.

- **Fabricação**

Quando uma parte não autorizada insere objetos falsos em um ativo, comprometendo a autenticidade e o não repúdio. Alguns exemplos são a adição de registros não existentes em um arquivo e construções de páginas *web* falsas.

9.2. Tipos de Ataques



Ataques vêm se sofisticando ao longo do tempo, acompanhando seu crescimento. Atualmente, os níveis estão altíssimos, justificados por uma série de fatores como a popularidade da *Internet* e de comércios eletrônicos, falta de leis específicas, grande quantidade de material orientado a atacantes, desnecessário conhecimento técnico, etc. A maioria dos atacantes seguem passos padronizados para realização de ataques. Primeiro há um procedimento chamado *footprinting* que se refere a descobrir todas as informações relacionadas às tecnologias do alvo. A partir do resultado das descobertas, o ataque pode ser mais bem planejado e executado. Os objetivos comuns do *footprinting* são o levantamento de informações sobre domínios na *Internet* (nomes, responsáveis, etc), identificação do sistema operacional do alvo, descoberta de sub-redes, serviços TCP e UDP disponíveis, topologia de rede utilizada, nomes de usuários e grupos, endereços de e-mail, etc. Vamos conhecer algumas técnicas de *footprinting* e tipos de ataques.

- **Consulta de bases**

Domínios com terminações .com.br podem ser consultados através da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo, representada pelo endereço eletrônico http://registro.br. Lá pode-se obter informações como o servidor do domínio, nome e documento do responsável, datas de registro e expiração, entre outras. Para outras terminações, pode-se consultar a base *WHOIS* pelo endereço http://who.is

- ***Dumpster Diving / Trashing***

É uma técnica utilizada para conseguir informações privilegiadas que potencializam as tentativas de quebra de senha e invasões. Consiste em vasculhar o lixo, à procura de informações da organização como nome de contas e senhas ou informações confidenciais/ pessoais. Vale ressaltar que é um procedimento legal, pois não se trata de roubo de dados. Um equipamento eficiente e pouco utilizado contra *trashing* é o fragmentador de papéis.

- **Engenharia Social**

Poderosa técnica que explora fraquezas humanas e sociais ao invés de explorar tecnologias, ante a fragilidade humana em questões envolvendo segurança. As principais características são uso de falsa identidade, psicologia e técnicas de intimidação e exploração de boa fé das

pessoas. O famoso atacante *Kevin Mitnick* usou durante anos, intensivamente, técnicas de engenharia social para investidas contra organizações. Certa vez, se fazendo passar por um alto executivo, conseguiu acesso a um documento interno, apenas pedindo à secretária que enviasse uma cópia via *fax*. Outros exemplos de técnicas são envolver-se afetivamente com alguém da organização, disfarçar-se de técnico ou entregador, inserir erros de *software* de propósito para ser chamado para dentro da organização para consertar o problema, entre outras.

- ***Packet Sniffing***

Também conhecida como escuta passiva (*passive eavesdropping*) é uma técnica usada originalmente para resolução de problemas onde os *softwares* farejadores capturam pacotes trafegados na rede. Com isso, o atacante pode ter acessos a senhas contidas nas requisições de rede e outras informações como endereços IP de máquinas da rede.

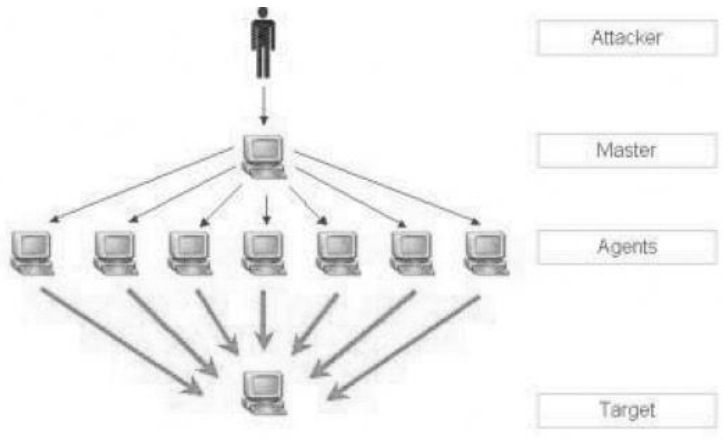
- ***Port Scanning***

São ferramentas utilizadas para levantar quais serviços estão disponíveis por meio de mapeamento de portas TCP e UDP. Além disso, podem-se descobrir faixas de endereços IP, portas abertas com serviços em execução e informações sobre o sistema operacional alvo.

- ***Spoofing***

Técnica utilizada para simular um serviço original, desviando e capturando todos os pacotes que deveriam chegar ao destino verdadeiro. É comum ser utilizada para páginas falsas de bancos ou telas de autenticação.

- ***Denial of Service (DoS)***



Conhecida técnica de ataque que tem que por objetivo a indisponibilidade através de sobrecarga de solicitações de serviço (*flood*) e não a invasão do alvo. Pode gerar grande tráfego de dados, causando paradas temporárias do serviço. Sua detecção é difícil, porém solucionável. Uma variação deste ataque é o DDoS (*Distributed Denial of Service*), no qual a ação é distribuída sobre várias máquinas (chamadas "zumbis") controladas remotamente por um computador central.

- ***SYN Flooding***

Explora os pacotes de pedido de conexão (SYN) em operações TCP através do *three-way handshake*. O atacante envia um grande número de pacotes SYN de modo que o servidor passe a não ser capaz de responder todas elas. Em conexões TCP, o cliente requisita uma conexão enviando um SYN ao servidor. O servidor confirma esta requisição mandando um SYN-ACK de volta ao cliente. O cliente por sua vez responde com um ACK, e a conexão está estabelecida. Um atacante pode não mandar esta última mensagem ACK. O servidor irá esperar por isso por um tempo, já que um simples congestionamento de rede pode ser a causa do ACK faltante. Um ataque de *Syn Flood* é feito com os endereços IP's forjados (*spoof*), para que o atacante não receba os ACK's de suas falsas solicitações.

- ***Buffer Overflow***

O *Buffer* é uma área de armazenamento temporário utilizado pelas aplicações ao executar determinadas tarefas, garantindo rapidez. A técnica de ataque consiste em injeção de código na aplicação de modo a ultrapassar a capacidade da área de *buffer*, causando lentidão e comprometendo a disponibilidade do recurso.

- ***Password Crackers***

Técnica utilizada para conseguir identificar uma senha de acesso. O êxito desta técnica está diretamente ligado à complexidade da senha. Os ataques podem ser por força bruta (onde um *software* vai tentando senhas até acertar) ou por dicionários (onde um *software* utiliza palavras de um dicionário como nomes, substantivos, etc.

Análise Microsoft

A *Microsoft* criou um modelo de análise chamado STRIDE, representando as iniciais de *Spoofing* (falsificação), *Tampering* (violação), *Repudiation* (repúdio), *Information Disclosure* (divulgação não autorizada de informação), *Denial of Service* (negação de serviço) e *Elevation of Privilege* (elevação de privilégio).

Ao cumprir as etapas STRIDE, isto é, reduzir as ameaças de seus componentes, pode-se argumentar que o sistema é seguro.

9.3. Medidas de Segurança

Jamais haverá ambientes totalmente seguros. O objetivo da adoção de medidas de segurança é implementar controles que minimizam vulnerabilidades e previne ameaças. As medidas abrangem procedimentos, configurações, *softwares* e *hardwares*, em comum acordo com todos os envolvidos. Deve-se sempre considerar o custo da medida de segurança em etapas de implantação, manutenção, revisão e atualização. A estimativa é baseada em aceitações de riscos para elaboração do custo benefício entre a proteção e seus custos. A ABNT homologou em 2001 a norma de segurança NBR ISSO/IEC 17779 que inclui, entre outras coisas,

documentação da segurança interna da organização, educação e treinamento aos envolvidos e geração de relatórios de segurança. Vamos conhecer algumas medidas:

- **Políticas de Segurança**

Conjunto de normas e diretrizes internas destinadas a proteção dos ativos da organização. O objetivo é definir a forma de utilização dos seus recursos através de procedimentos para prevenir e responder a incidentes de segurança. A elaboração da politica de segurança deve ter a participação de todas as áreas da organização e deve ser inviolável. O ideal é englobar quais permissões deve haver no sistema, quais *hardwares* e *softwares* serão permitidos, qual procedimento em caso de violação, o que será protegido e vigência. Outras características são ser simples, clara, objetiva, de acordo com as leis, aplicável, consistente e conter justificativas das regras.

- **Criptografia Forte**

A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia, escrita) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem. A cifragem consiste basicamente na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida. Um exemplo é o uso do protocolo HTTPS em páginas *web*. Ao acessar uma página bancária ou um formulário, é possível observar o endereço da página começando com "https... " e não mais com "http..." ou então um símbolo de cadeado fechado em algum ponto da página. Quando há a presença de algum desses elementos, os dados ali presentes estão sendo criptografados.

- **Segurança Física / Controle de Acesso**

É comum em sala de servidores ou em setores de cofres bancários haver profissionais de segurança física guardando seu conteúdo. Isso se deve ao fato de que em certos ambientes, o acesso físico deve ser controlado ou até mesmo proibido. Outros meios são uso de câmeras de circuito interno ou alarmes.

- ***Firewall***

O Firewall é um sistema inteligente de análise de informações responsável por monitorar o tráfego que circula em uma rede, analisando as informações que entram ou sai dos computadores. A fim de entender como um Firewall funciona, considere que a rede seja um edifício onde o acesso deva ser controlado. O edifício tem uma sala de espera como o único ponto de entrada. Nesta sala de espera, as recepcionistas recebem os visitantes, os guardas de

segurança observam os visitantes, as câmeras de vídeo gravam as ações de cada visitante e leitores de sinais autenticam os visitantes que entram no edifício. Estes procedimentos devem funcionar bem para controlar o acesso ao edifício, contudo se uma pessoa não autorizada consegue entrar, não há meio de proteger o edifício contra as ações do intruso. Porém, se os movimentos do intruso são monitorados, é possível detectar qualquer atividade suspeita.

- **Autenticação**

Autenticar é o ato de reconhecer quem está acessando informações restritas. Este reconhecimento pode ser feito de várias formas, sendo as mais comuns por meio de senha, cartão magnético ou biometria (íris, voz, impressão digital, face, etc). O reconhecimento biométrico tem se mostrado bastante avançado no âmbito da segurança e várias empresas utilizam este métodos para com seus funcionários. Mas este apresenta alguns problemas esporádicos como rouquidão (no caso de reconhecimento por voz), gripes, resfriados, lacrimejamento (para reconhecimentos oculares), entre outros. Para senhas, o ideal é implantar em políticas, trocas de senhas regulares e conscientização para o uso de senhas fortes dentro da rede.

- **Antivírus/Antispy**

Existem inúmeros *softwares* antivírus e antispy que podem ser baixados gratuitamente. Eles inibem a ação de programas espiões e avisam quando um deles tentar se instalar no seu computador. Alguns leitores e servidores de e-mails oferecem o filtro antispam onde você pode bloquear mensagens de determinados remetentes.

- **Esteganografia**

É um ramo particular da criptologia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença. Ao contrário da criptografia, que procura esconder o conteúdo da mensagem, a esteganografia procura esconder a existência da mensagem. A esteganografia esconde as mensagens através de artifícios, por exemplo, imagens ou um texto que tenha sentido, mas que sirva apenas de suporte (como o alfabeto biliteral de Francis Bacon ou as famosas cartas de George Sand). A ideia é mesclar a mensagem numa outra e onde apenas determinadas palavras devem ser lidas para descobrir o texto camuflado. Olhe para a imagem acima. É só uma cortina?

APÊNCICE – EXERCÍCIOS

1. O que é uma rede de computadores?
2. Justifique 2 aplicações vantajosas na utilização de redes de computadores
3. O que é colisão de pacotes?
4. Defina concentrador
5. Quantas e quais camadas possui o modelo TCP/IP?
6. Qual a principal função do roteador?
    a) Controlar o acesso de usuários
    b) Realizar filtragem do conteúdo dos pacotes que circulam na rede
    c) Escolher o melhor caminho para um pacote chegar ao seu destino
    d) Interligar dispositivos em uma rede local
7. Explique a função do Armário de Telecomunicações em cabeamento estruturado
8. Qual o nome dado ao cabo principal de uma rede?
9. Qual a função da blindagem nos cabos par trançado?
10. Qual o tipo específico de rede para computadores distantes geograficamente?
11. Se a interferência é o principal desafio, um projetista deve considerar a utilização de:
    a) Cabos coaxiais
    b) Par Trançado
    c) Fibra Ótica
12. Qual o tipo de conector utilizado em cabos coaxiais?
13. Cite 2 desvantagens da fibra ótica.
14. Em que tipo de situação as redes sem fio são recomendadas?
15. Explique a técnica de cascateamento.
16. Correlacione as 2 colunas

(a) Hub	( ) Amplifica o sinal
(b) Switch	( ) Replica a mensagem para todas as estações
(c) Repetidor	( ) Usado para acessar a internet

17. Cite 1 desvantagem de redes híbridas.
18. O que é cabeamento estruturado?
19. Ao se optar por par trançado, deve-se considerar a distância máxima de _____ metros.
20. Considere uma escola com 2 prédios separados por uma área de uma quadra poli esportiva com dimensões aproximadas de 80x60m. Os dois prédios irão possuir laboratórios de informática, sendo um deles um prédio histórico com mais de cem anos e o outro um prédio recém-construído. Qual a solução para o meio de comunicação que deverá ser utilizada para:
    a) Interconectar as máquinas de um mesmo prédio, para cada caso.
    b) interconectar os dois prédios.

21. Para os cabos utilizados na montagem de redes, assinale a afirmativa INCORRETA.
    a) Um cabo UTP contém pares de cabos de cobre isolados torcidos um sobre o outro para reduzir a interferência eletromagnética.
    b) Cabos STP são menos suscetíveis à ruídos do que os UTP e suportam taxas mais altas de transmissão
    c) Cabos de fibra ótica são imunes a interferência eletromagnética.
    d) Conectores RJ-45 são utilizados para conectar cabos coaxiais.
22. O que é criptografia?
23. O que é um protocolo?
24. Cite 1 protocolo de transporte.
25. Para que serve o protocolo POP?
    a) Transportar pacotes.
    b) Enviar correio eletrônico.
    c) Navegar com segurança.
    d) Receber correio eletrônico.
26. Quando devo usar TCP e quando usar UDP?
27. Explique o *three-way handshake*.
28. Indique o modelo de ataque:
    a) Adição de um registro falsificado no BD.
    b) Desabilitar um sistema de arquivos.
    c) Modificação de dados trafegando na rede.
    d) Captura de dados da rede, através de escutas.
    e) Alteração de um software para que execute de forma diferente.
29. Fale sobre redes ATM.
30. Sobre o que trata a norma brasileira ABNT NBR 14565?
31. Considere o IP 192.59.66.0 com uma máscara de sub-rede 255.255.255.240, encontre:
    a) Quantas redes?
    b) Quais os endereços de broadcast?
    c) Quais os endereços IP válidos dentro de cada rede.
32. Quais as principais características de uma rede LAN?
33. Qual a função de um *modem*?
34. O que é uma topologia?
35. O que é um *broadcast*?
36. Qual o papel da camada física nos modelos de referência?
37. Explique esteganografia.
38. O que é Engenharia Social?
39. O que é NIC?
40. Por que *switches* são melhores que *hubs*?

REFERÊNCIAS

TANENBAUM, Andrew S. Redes de Computadores. 6ª ed.

KUROSE, James. Redes de Computadores e a Internet.

MORIMOTO, Carlos. Redes, Guia Prático.

==========

Apostila produzida pelo Prof. Esp. Jonas Willian R. Aureliano para o Curso Técnico de Informática do Colégio Tableau de Guaratinguetá.