



Redes de Computadores e Segurança



AUTORIA
Auro Lima Carvalho



Bem vindo(a)!

Seja muito bem vindo(a)!

Prezado(a) aluno(a), você que está matriculado nessa disciplina, já está trilhando um passo a um futuro promissor na área da tecnologia, onde vamos estar juntos nessa jornada de conhecimento. Nossa proposta é juntos conhecermos os conceitos de Redes de computadores e segurança de dados, os principais componentes de Redes e equipamento que compõe as principais topologias.

Na Unidade I, iniciaremos nossos trabalhos com os conceitos e histórico sobre as redes de computadores, os principais tipos de redes, sua topologia, redes locais, metropolitanas e geograficamente distribuídas, também sobre os meios de transmissão guiados, que são uma abordagem sobre cabeamento estruturado e os meios de transmissão não guiados, conhecidamente como wireless, dentre outras tecnologias.

Já na unidade II, daremos continuidade aos nossos trabalhos ampliando nossos estudos sobre satélites de comunicação, satélites terrestre de baixa órbita, suas tecnologias empregadas e órbitas de operação. Faremos abordagem sobre os equipamentos de redes, onde operam e a importância desses equipamentos nas topologias de redes, e divulgação dos pacotes dados.

Nossa abordagem na unidade III tratará da arquitetura dos sistemas distribuídos, onde os fabricantes de computadores focaram em uma pesquisa com a finalidade de ampliar o potencial computacional, como a velocidade de dados, minimizando o tamanho das máquinas e aumentando o poder de processamento e agilidade de informação. Apresentaremos ainda os aspectos de projetos e implementação de redes, a importância da atuação dos projetistas de redes nas organizações.

Finalizaremos nosso estudo na unidade IV conhecendo sobre os principais sistemas de arquivos distribuídos, conjunto de software e hardware localizados em distintos computadores interligados em rede. Abordaremos ainda nessa unidade sobre requisitos de segurança em sistemas de informação, arquivamento em nuvens, vantagens e desvantagens sobre esse sistema de armazenamento.

Reforçando o convite a você aluno(a), para juntos emergirmos nessa jornada de aprimoramento do conhecimento aos mais diversos assuntos abordados nesse material. Esperamos contribuir para o seu conhecimento pessoal e profissional.

Muito obrigado e sucesso nos estudos!

Sumário

Essa disciplina é composta por **4 unidades**, antes de prosseguir é necessário que você leia a apresentação e assista ao vídeo de boas vindas. Ao término da quarta da unidade, assista ao vídeo de considerações finais.



Unidade 1

Redes e meio de transmissão



Unidade 2

Satélites e Equipamentos de Rede



Unidade 3

Arquitetura de sistemas

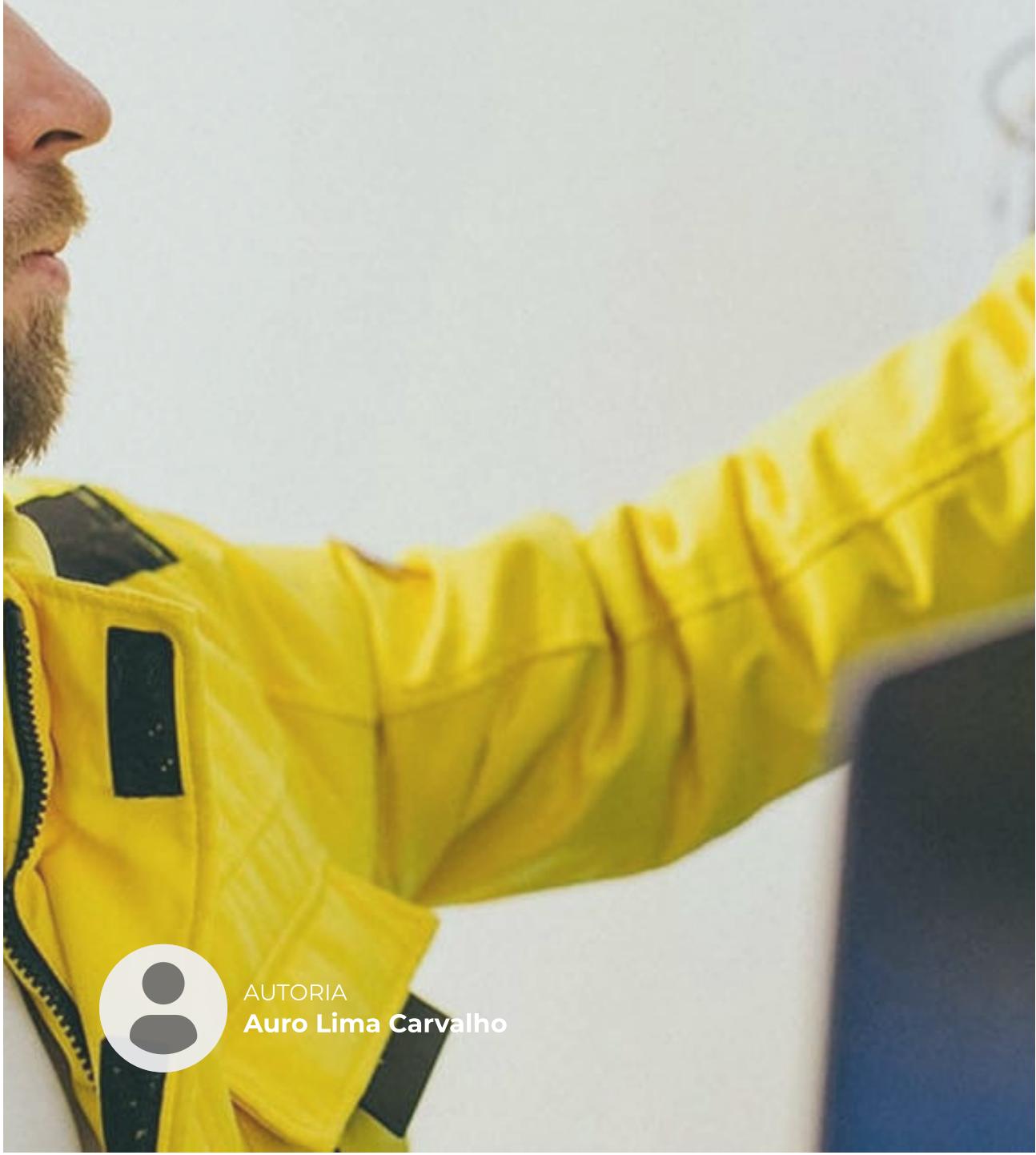


Unidade 4

Sistemas e segurança



Redes de Computadores e Segurança



AUTORIA
Auro Lima Carvalho

Bem vindo(a)!

Seja muito bem vindo(a)!

Prezado(a) aluno(a), você que está matriculado nessa disciplina, já está trilhando um passo a um futuro promissor na área da tecnologia, onde vamos estar juntos nessa jornada de conhecimento. Nossa proposta é juntos conhecermos os conceitos de Redes de computadores e segurança de dados, os principais componentes de Redes e equipamento que compõe as principais topologias.

Na Unidade I, iniciaremos nossos trabalhos com os conceitos e histórico sobre as redes de computadores, os principais tipos de redes, sua topologia, redes locais, metropolitanas e geograficamente distribuídas, também sobre os meios de transmissão guiados, que são uma abordagem sobre cabeamento estruturado e os meios de transmissão não guiados, conhecidamente como wireless, dentre outras tecnologias.

Já na unidade II, daremos continuidade aos nossos trabalhos ampliando nossos estudos sobre satélites de comunicação, satélites terrestre de baixa órbita, suas tecnologias empregadas e órbitas de operação. Faremos abordagem sobre os equipamentos de redes, onde operam e a importância desses equipamentos nas topologias de redes, e divulgação dos pacotes dados.

Nossa abordagem na unidade III tratará da arquitetura dos sistemas distribuídos, onde os fabricantes de computadores focaram em uma pesquisa com a finalidade de ampliar o potencial computacional, como a velocidade de dados, minimizando o tamanho das máquinas e aumentando o poder de processamento e agilidade de informação. Apresentaremos ainda os aspectos de projetos e implementação de redes, a importância da atuação dos projetistas de redes nas organizações.

Finalizaremos nosso estudo na unidade IV conhecendo sobre os principais sistemas de arquivos distribuídos, conjunto de software e hardware localizados em distintos computadores interligados em rede. Abordaremos ainda nessa unidade sobre requisitos de segurança em sistemas de informação, arquivamento em nuvens, vantagens e desvantagens sobre esse sistema de armazenamento.

Reforçando o convite a você aluno(a), para juntos emergirmos nessa jornada de aprimoramento do conhecimento aos mais diversos assuntos abordados nesse material. Esperamos contribuir para o seu conhecimento pessoal e profissional.

Muito obrigado e sucesso nos estudos!

Sumário

Essa disciplina é composta por **4 unidades**, antes de prosseguir é necessário que você leia a apresentação e assista ao vídeo de boas vindas. Ao término da quarta da unidade, assista ao vídeo de considerações finais.



Unidade 1

Redes e meio de transmissão



Unidade 2

Satélites e Equipamentos de Rede



Unidade 3

Arquitetura de sistemas



Unidade 4

Sistemas e segurança



História das redes



AUTORIA
Auro Lima Carvalho

A primeira conexão experimental de computadores em rede ocorreu em 1965, nos EUA, pelos cientistas Lawrence Roberts e Thomas Merril. A experiência realizou-se por uma linha telefônica discada de baixa velocidade, conectando dois centros de pesquisa, um em Massachusetts e o outro na Califórnia. Nasceu ali a semente para o que hoje é a Internet – mãe de todas as redes.

A criação das redes de computadores estava ligada à corrida espacial. Grande parte dos elementos e aplicações elementares para a comunicação entre computadores, como o protocolo TCP/IP, a tecnologia de comutação de pacotes de dados e o correio eletrônico, estão relacionados ao desenvolvimento da Arpanet, propulsora da internet. A Arpanet foi criada por um programa desenvolvido pela Advanced Research Projects Agency (ARPA) mais tarde rebatizada como DARPA.

A agência nasceu do departamento de defesa dos Estados Unidos, onde tinham a preocupação de não perder terreno na corrida tecnológica para os russos com o lançamento do satélite Sputnik, em 1957. Roberts, acadêmico do MIT (Instituto de Tecnologia de Massachusetts), um dos integrantes da DARPA e um dos pais da Arpanet, que começou em 1969 conectando as universidades: UCLA – Universidade da Califórnia em Los Angeles, Stanford, Santa Bárbara e Utah. Em 1983 foi feita a separação dos militares da Arpanet, com a criação da Milnet.

A evolução das redes locais de computadores começou nos anos 70. Antes disso os computadores eram grandes que processavam informações por leitura de fitas e cartões magnéticos. Não existia a interação entre os usuários e as máquinas.

Com o desenvolvimento dos minicomputadores de 32 bits, nos anos 70, que os grandes fabricantes, como IBM, HP e Digital, começaram a criar soluções com o objetivo de distribuir o poder de processamento dos mainframes e procurar facilitar o acesso às informações. O lançamento do VAX pela Digital, em 1977, estava baseado numa estratégia de criar uma arquitetura de rede de computadores. Com isso, a empresa esperava superar a rival Big Blue.

Quando um Vax era ligado, já dava início a procura por outras máquinas para começar a comunicação, um procedimento inovador em uma época que poucos usuários tinham noção do que era uma rede. A estratégia teve sucesso e o VAX alcançou grande popularidade, principalmente em aplicações científicas e de engenharia. Anos depois, a Digital foi comprada pela Compaq e incorporada à HP. As inovações surgidas com o VAX e seu sistema operacional, o VMS, influenciaram os computadores que viriam depois.

O sistema operacional Unix nasceu em 1969 nos laboratórios Bell, apresentando inovações que logo o tornou popular nas universidades e nos centros de pesquisa a partir de 1974. Era um sistema portável e modular, capaz de rodar em vários computadores e evoluir junto com o hardware. Os sistemas operacionais da época eram escritos em assembly, linguagem específica para a plataforma de hardware.

O Unix foi escrito em linguagem C, considerada uma linguagem de alto nível, deu a ele uma inédita flexibilidade. No início ferramentas importantes foram criadas para o Unix, como o e-mail, o Telnet, que permitia o uso de terminais remotos, e o FTP, que se transformou no padrão de transferência de arquivos entre computadores em rede. Através dessa plataforma que surgiram a maioria das tecnologias que hoje se tornaram a Internet.

A Ethernet

O desenvolvimento da tecnologia ethernet foi um marco tecnológico que permitiu a popularização das redes. O avanço que essa invenção representou para a época onde os computadores não compartilhavam cabos comum de conexão. Cada máquina era conectada a outra a uma distância não superior a 2 metros. O grande criador da Ethernet é Robert Metcalfe, um dos gênios produzidos pelo MIT e por Harvard e fundador da 3Com.

Metcalfe era pesquisador do laboratório Parc, que a Xerox mantém até os dias atuais, na Califórnia. Em 1972, ele teve a missão de organizar um sistema que fizesse a conexão das estações Xerox Alto entre si e com os servidores. A intenção era que os pesquisadores do Parc pudessem compartilhar as recém desenvolvidas impressoras a laser.

Uma das teorias sobre a criação da Ethernet é que Metcalfe e equipe tomaram por base um sistema desenvolvido por um casal de estudantes da universidade de Aloha, no Havaí. Com o uso de um cabo coaxial, conseguiram interligar computadores em duas ilhas para poder se comunicar. Antes de ter o nome de Ethernet, a partir de 1973, o sistema de Metcalfe tinha o nome de Alto Aloha Network. Ele mudou a denominação, primeiramente para deixar claro que a Ethernet funcionaria em qualquer computador e não apenas nas estações Xerox. E também para comprovar a diferença em relação ao método de acesso CSMA (*Carrier Sense Multiple Access*) do sistema Aloha. A palavra ether foi uma referência à propagação de ondas pelo espaço.

As letras CD (de Collision Detection) foi acrescentada à sigla CSMA. Um detalhe importante para a detecção de colisão que impede que dois dispositivos acessem o mesmo nó ao mesmo tempo. Assim, o sistema Ethernet monitora se a rede está livre para enviar a mensagem. Caso não esteja a mensagem fica numa fila de espera para ser transmitida. A ethernet iniciou seus trabalhos com uma banda de 2Mbps que permitia conectar 100 estações em até 1 km de cabo.

Usava-se o cabo coaxial no início, chamado yellow cable, de diâmetro maior que os atuais. A topologia era um projeto de barramento. O conector desse sistema foi batizado de vampiro, pois “mordia” o cabo em determinados pontos. Dali saia um cabo serial que se ligava à placa de rede. O yellow cable podia ser instalado no teto ou no chão, conectado ao cabo menor.

O que são Redes de computadores?

Redes de computadores são computadores conectados, com o objetivo de compartilhar dados informativos, arquivos, recursos, programas, impressoras, correio eletrônico, dispositivos, etc., trazendo benefícios aos usuários e empresas que irão utilizá-la.



REFLITA

Existem redes Livres e redes Não Livres. As redes livres são formadas no geral por entusiastas de softwares livres que conectam diferentes nós entre si mediante tecnologia WiFi que compartilham arquivos armazenados em disco e transmitem dados a elevadas velocidades. Por exemplo, hoje uma rede livre pode funcionar a 54 MB/ps, enquanto que em 2008 as redes não livres, como por exemplo a Internet, brindavam aos usuários domiciliares 3 MB/ps tipicamente como um estandarte na Europa, sendo menor ainda a banda larga na América do Sul. As redes livres são administradas de forma cooperativa e no geral o acesso é gratuito. O movimento do software livre, ao menos por parte da Free Software Foundation, se propõe criar uma rede de redes livres de alcance mundial, paralela à Internet.

[ACESSAR](#)

Uso das Redes de computadores

- A utilização das redes traz vantagens, entre elas: As redes permitem um gerenciamento de recursos mais eficientes: A utilização de uma única impressora de excelente qualidade por múltiplos usuários, em vez de várias impressoras de baixa qualidade, conectada a cada máquina.
- As redes ajudam a manter as informações confiáveis e atualizadas: O compartilhamento de arquivos pode ajudar a assegurar que exista somente uma versão de um arquivo em circulação e que qualquer um que use o arquivo esteja sempre trabalhando com a versão mais recente da informação.
- As redes ajudam a acelerar o compartilhamento de dados: A transferência de dados através da rede é sempre mais rápida que qualquer outro meio de

compartilhamento, como cd's, pendrives, etc.

As redes permitem que grupos de trabalhos atuem com mais eficiência: O correio eletrônico e as agendas de grupos permitem que correspondentes de uma equipe de trabalho troquem informações e agendem compromissos de forma prática e eficiente.(TITTEL, 2003, p 36).



Tipos de Redes



AUTORIA
Auro Lima Carvalho

Existem inúmeros tipos de redes privadas ou não, de acordo com suas dimensões e de número de máquinas conectadas, sua velocidade de transferência de dados e extensão. Redes privadas são redes que pertencem a uma mesma organização, considerando-se geralmente três categorias de redes:

- rede LAN (local area network);
- rede MAN (metropolitan area network);
- rede WAN (wide area network).

Rede LAN

LAN significa Local Area Network (em português, Rede Local) e se refere a um grupo de computadores que pertencem a uma mesma organização e que estão conectados entre eles, numa pequena área geográfica, por meio de uma rede, frequentemente através de uma mesma tecnologia (a mais usada é a Ethernet).

Uma LAN representa uma rede em sua forma mais simples. A velocidade de transferência de dados de uma rede local varia de 10 Mbps (para uma rede ethernet, por exemplo) a 1 Gbps (em FDDI ou Gigabit Ethernet, por exemplo). A dimensão de uma rede local pode atingir até 100 ou mesmo 1.000 usuários.

Os serviços oferecidos pela rede local, existem dois modos de funcionamento, em um ambiente de **igual para igual** (em inglês peer to peer e, em português, ponto a ponto), no qual não há um computador central e cada computador tem um papel similar e em um ambiente **cliente/servidor**, no qual um computador central fornece serviços de rede aos usuários.

Rede MAN

As **MAN** (*Metropolitan Area Network* ou Redes Metropolitanas) onde conectam várias LAN geograficamente próximas (no máximo, há algumas dezenas de quilômetros). Logo, uma MAN permite comunicar dois pontos como se ambos fizessem parte de uma mesma rede local. Uma MAN é formada por roteadores ou switches interligados em geral por fibras ópticas.

Rede WAN

Uma **WAN** (*Wide Area Network* ou rede vasta) conecta inúmeras LANs, atravessando grandes áreas geográficas. O custo das conexões aumentam显著mente com as distâncias e podem ter perda de sinal quanto maior forem as distâncias. O funcionamento das WANs ocorrem graças aos roteadores que têm o poder de escolher o trajeto mais adequado para chegar até um ponto (nó) da rede. A rede mais famosa dos WANs é a **Internet**. As redes WAN's passam por uma evolução atualmente com a aplicação e ampliação de novas tecnologias de telecomunicações e com a utilização de fibra ótica.

Novos padrões estão surgindo para fibra ótica, que disponibiliza a transmissão de dados (texto, binário), dados de aplicação em tempo real como som e imagem em uma única linha e em altíssima velocidade (300 Mbps ou superior). A velocidade passa a ser configurada por equipamentos que processam as informações (cliente/servidores) e não do meio físico. A conexão entre os equipamentos geralmente é feita através de Modem's e linhas de 64 Kbps, enlaces E1 (2048 Mbps). Estes serviços são oferecidos pelas empresas de telecomunicações.



SAIBA MAIS

Mercado de trabalho para quem faz o curso de Redes de Computadores

De um escritório de advogados até um hospital ou prefeitura, cada vez mais as empresas precisam ter uma rede de computadores confiável e segura, com boa conectividade e comunicação fluida entre os diferentes programas utilizados. E o trabalho do tecnólogo em Redes de Computadores é fundamental para fazer isso acontecer. O mercado de trabalho para quem faz este curso é vasto e está aquecido. O profissional formado encontra oportunidades de emprego em empresas públicas e privadas de praticamente todos os setores da economia, associações, e ONGs. Empresas ligadas à tecnologia, como desenvolvedores de software, indústria de hardware, operadoras de telefonia celular e de internet também são grandes empregadores destes profissionais, que podem ser contratados como funcionários, trabalhar de forma terceirizada ou até mesmo autônoma, como consultores. Profissionais de TI em geral estão em falta no mercado e quem se qualifica, principalmente em nível superior, tem alta empregabilidade. Uma pesquisa da FGV revelou que a taxa de **empregabilidade de tecnólogos é de mais de 90%** e a chance de conseguir um emprego na mesma área do curso em que se formou é de quase 80%.

[ACESSAR](#)

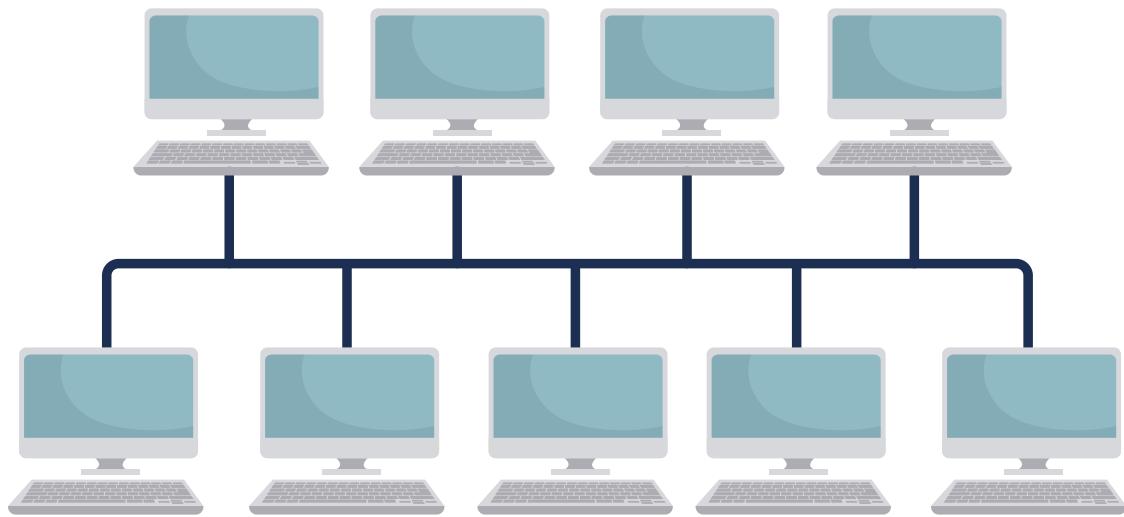
Topologia de Redes

Topologia de redes são arranjos físicos que uma rede está disposta, uma rede informática é formada por computadores conectados entre si, graças a cabos de redes para comunicação e elementos de hardware (placas de rede ou outros equipamentos que garantem a boa propagação dos dados). A configuração de espaço da rede é chamada **topologia física**. As topologias se geralmente se dividem em:

- redes em barramento;
- redes em estrela;
- redes em anel;
- redes em árvore;
- redes de malha.

A **topologia lógica**, contrária à topologia física, são como os dados transitam nas linhas de comunicação. As topologias lógicas mais usuais são a Ethernet, o Token Ring e o FDDI.

Figura 1: Barramento



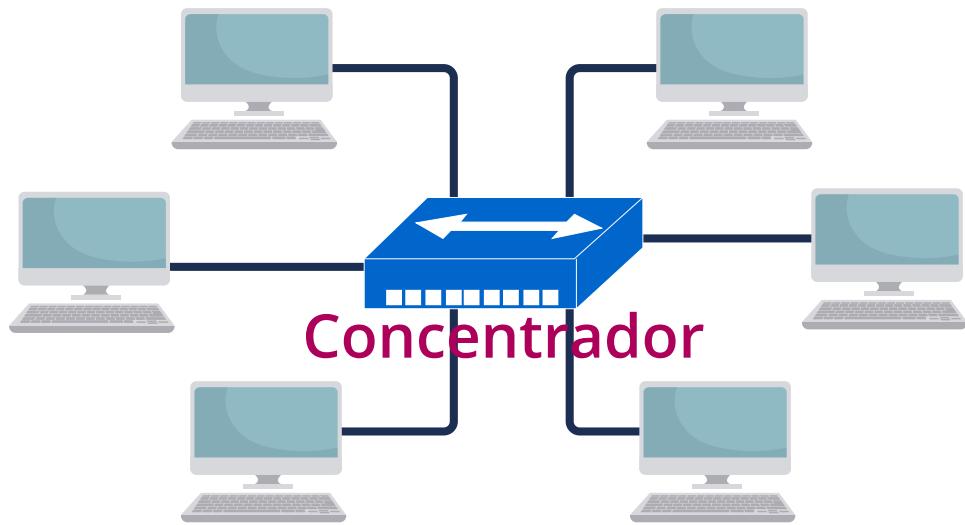
Fonte: acesse o link [Disponível aqui](#)

Na topologia de barramento, os nós ficam conectados a uma única linha de transmissão e todos compartilham o mesmo meio de transmissão para receber como para enviar mensagens. Esse tipo de topologia é utilizado nas redes que implementam *broadcasting*.

Devido a maneira que os nós estão conectados a linha, caso haja algum problema com o meio de transmissão, por exemplo, um rompimento de um cabo, todos os nós da rede ficarão incomunicáveis.

Pode parecer tanto quanto arriscada a implementação deste tipo de topologia, mas a verdade, a maioria das redes já foi assim, como por exemplo a Ethernet.

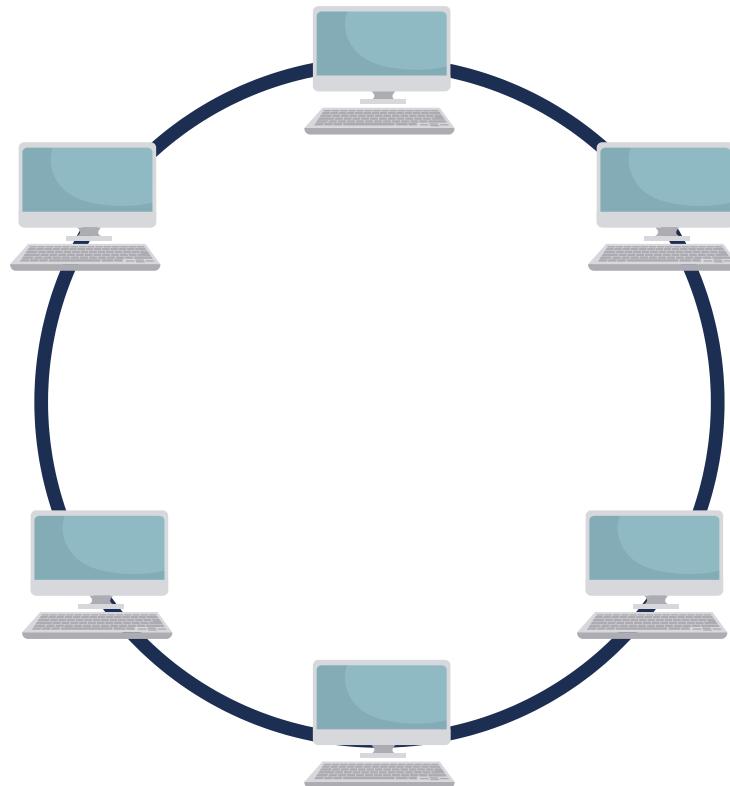
Figura 2: Estrela



Fonte: acesse o link [Disponível aqui](#)

Na topologia em estrela todos os nós estão ligados ponto-a-ponto a um nó central chamado concentrador (*hub* em inglês), trata-se de uma caixa com diversas junções às quais se podem conectar os cabos provenientes dos computadores. Seu papel é garantir a comunicação entre os diferentes nós. Quando um nó quer se comunicar com um outro nó qualquer diferente do *hub*, o nó origem envia a mensagem primeiro para o hub e, posteriormente, o *hub* envia a mensagem para o nó destino.

A grande vantagem desta topologia é sua simplicidade de implementação e baixo custo. Sua desvantagem, no entanto, praticamente a desqualifica, pois se o *hub* sofrer qualquer problema, todos os outros nós não poderão se comunicar. Uma solução comum para este problema é adotar a redundância de equipamentos críticos que, em caso de falha no equipamento, poderão assumir as funções do equipamento inoperante. Por outro lado, uma rede em estrela é mais cara do que uma rede em barramento, já que ela requer um hardware suplementar (o *hub*).

Figura 3: Anel

Fonte: acesse o link [Disponível aqui](#)

A topologia em anel (ring ou loop) se assemelha muito com a topologia de barramento. Primeiramente, os nós compartilham o mesmo meio de transmissão, se comunicando através do conceito de broadcasting. Em primeiro lugar, caso haja um problema com a linha, toda a rede ficará indisponível.

Alguns fabricantes utilizam essa topologia em suas redes locais, sendo a tecnologia de fibra ótica baseada nessa concepção. As duas principais topologias lógicas que utilizam esta topologia física são o Token ring (anel com ficha) e o FDDI (Fiber Distributed Data Interface e, em português, Interface de dados distribuída por fibra).



Meios de Transmissão Guiados



AUTORIA
Auro Lima Carvalho

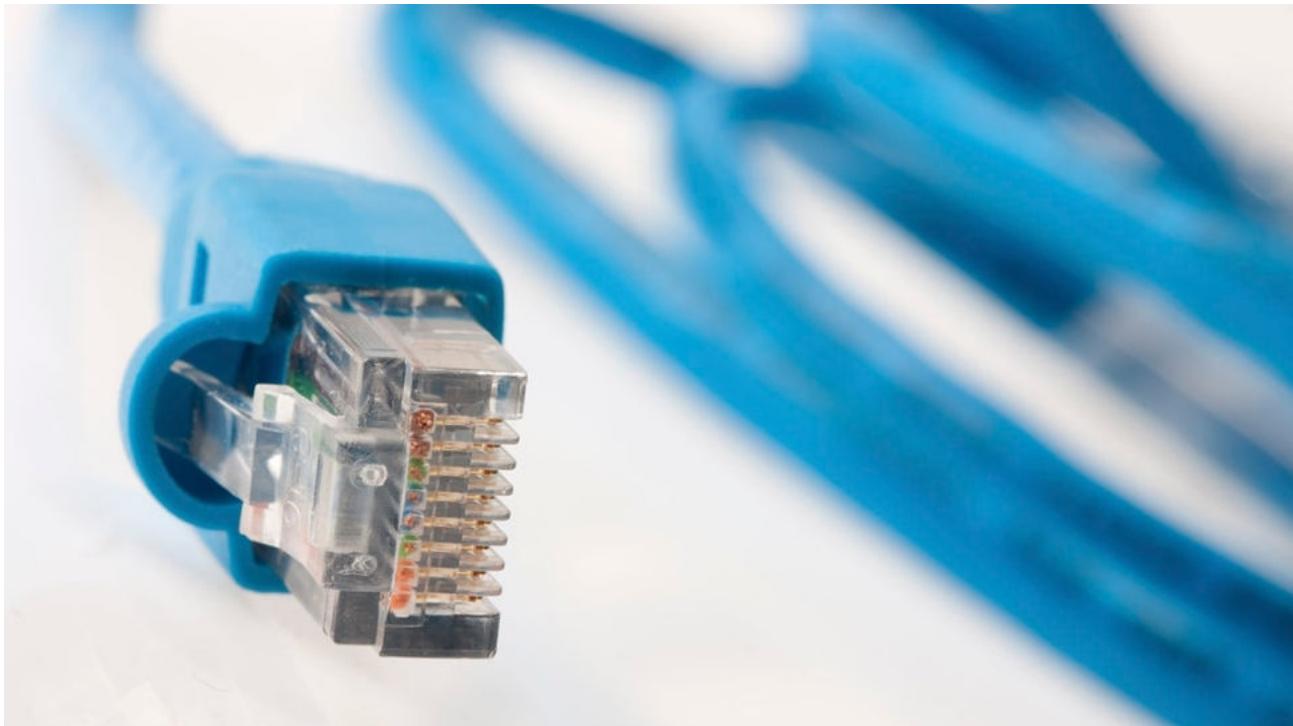
Transmitir fluxo de bits entre computadores são a principal função dos meios de transmissão. Diversos meios físicos são usados para realizar a transmissão, cada um tem sua própria característica em termos de largura de banda, retardo, custo e facilidade de instalação e manutenção. Os meios físicos são agrupados em meios guiados, como os fios de cobre e fibras ópticas, e em meios não-guiados, como as ondas de rádio e os raios laser transmitidos pelo ar.

Cabos

Os projetos de cabeamento de uma rede fazem parte do meio físico usado para conectar computadores. É um fator muito importante para o bom funcionamento da rede e esse projeto envolve aspectos sobre a taxa de transmissão, largura de banda, facilidade de instalação, imunidade a ruídos, confiabilidade, custos de interface, exigências geográficas, conformidade com padrões internacionais e disponibilidades de componentes, entre outros.

O sistema a ser usado no cabeamento determina a estabilidade de uma rede. Pesquisas apontam que cerca de 80% dos problemas físicos em uma rede tem origem no cabeamento, prejudicando de maneira considerável a confiabilidade da operação da rede. A implantação do cabeamento corresponde a aproximadamente 6% do custo total da rede e 70% da manutenção de uma rede é causado pelos problemas oriundos do cabeamento.

Figura 4: Cabo par trançado



Fonte: @nomadsoul1 em Freepik.

Figura 5: Cabo coaxial



Fonte: @volodymyr-vorona em Freepik.

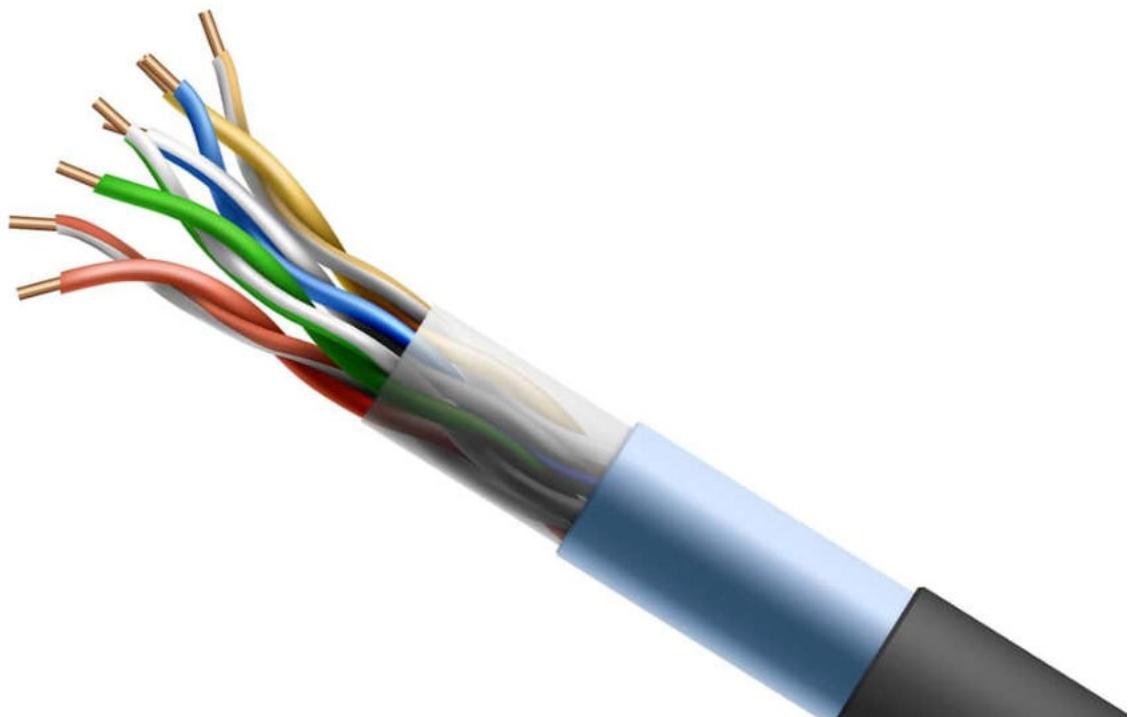
Em matéria de cabos, os mais utilizados são os cabos de par trançado, os cabos coaxiais e cabos de fibra óptica. Cada categoria tem suas próprias vantagens e limitações, sendo mais adequado para um tipo específico de rede.

- **Os cabos de par trançado** - são os mais utilizados por ter um melhor custo benefício, fácil de ser encontrado pronto em lojas de informática, ou confeccionado sob medida, e ainda são 10 vezes mais rápidos que os cabos coaxiais.
- **Os cabos coaxiais** – se destacam pelo fato dos dados serem transmitidos através de uma distância maior que a permitida pelos cabos de par trançado sem blindagem (UTP), em contra partida não são flexíveis para manusear custam mais caros que o par trançado.
- **Os cabos de fibra óptica** – proporcionam transmissões de dados a velocidades bem maiores e são imunes a todo e qualquer tipo de interferência eletromagnética, porém, seu custo é muito alto e difícil de instalar, demandando equipamentos e mão de obra especializada. Mesmo tendo uma alta velocidade de transferência, as redes de fibras ainda não são uma boa opção para pequenas redes devido ao custo.

Cabo Par Trançado

O cabo par trançado surgiu por ser o mais flexível dos cabos, e com maior velocidade de transmissão, ele substitui os cabos coaxiais desde o início da década de 90. É muito raro atualmente o uso de cabos coaxiais em instalações de rede, apesar do custo adicional decorrente da utilização de hubs e outros concentradores. O custo do cabo é mais baixo, e a instalação é mais simples. O nome “par trançado” é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de fios entrelaçados. Os cabos coaxiais usam uma malha de metal que o protege contra interferências externas; já os cabos de par trançado utilizam um tipo de proteção mais simples, o entrelaçamento dos cabos forma um campo eletromagnético que bloqueia interferências externas.

Figura 6: Cabo par trançado, com seus pares entrelaçados



Fonte: @vectorpocket em Freepik.

Existem basicamente dois tipos de cabo par trançado:

- Cabos sem blindagem chamados de UTP (*Unshielded Twisted Pair*);
- Cabos blindados conhecidos como STP (*Shielded Twisted Pair*).

O que os diferencia é que os cabos blindados além de contarem com a proteção do entrelaçamento dos fios, possuem uma blindagem externa (assim como os cabos coaxiais), sendo mais apropriados a ambientes com grandes interferências. Outras fontes menores de interferências são as lâmpadas fluorescentes (principalmente lâmpadas cansadas que ficam piscando), cabos elétricos quando colocados lado a lado com os cabos de rede e mesmo telefones celulares próximos aos cabos.

Figura 7: Cabo par trançado



Fonte: @user2649817 em Freepik.

Figura 8: Placa de rede para cabo par trançado



Fonte: adaptada de @CEphoto em Wikimedia Commons.

Quanto mais interferência na rede, menor será o desempenho dela e menor será a distância que poderá ser usada entre os micros, e mais vantajosa será a instalação de cabos blindados. Em ambientes normais os cabos sem blindagem costumam funcionar muito bem sem problemas de interferência.

Existem no total, 5 categorias de cabos de par trançado. Em todas as categorias a distância máxima permitida é de 100 metros. O que muda é a taxa máxima de transferência de dados e o nível de imunidade a interferências. Os cabos de categoria 5 que tem a grande vantagem sobre os outros 4 que é a taxa de transferência que pode chegar até 100 mbps, e são praticamente os únicos que ainda podem ser encontrados à venda, mas em caso de dúvida basta checar as inscrições no cabo, entre elas está a categoria do cabo.

A utilização do cabo de par trançado tem suas vantagens e desvantagens, vejamos as principais:

- **Vantagens**

Preço. Mesma com a obrigação da utilização de outros equipamentos na rede, a relação custo benefício se torna positiva.

Flexibilidade. Como ele é bastante flexível, ele pode ser facilmente passado por dentro de conduítes embutidos em paredes.

Facilidade. A facilidade com que se pode adquirir os cabos, pois em qualquer loja de informática existe esse cabo para venda, ou até mesmo para o próprio usuário confeccionar os cabos.

Velocidade. Atualmente esse cabo trabalha com uma taxa de transferência de 100 Mbps.

- **Desvantagens**

Comprimento. Sua principal desvantagem é o limite de comprimento do cabo que é de aproximadamente 100 por trecho.

Interferência. A sua baixa imunidade à interferência eletromagnética, sendo fator preocupante em ambientes industriais.

No cabo de par trançado tradicional existem quatro pares de fio. Dois deles não são utilizados, pois nos outros dois pares, um é utilizado para a transmissão de dados (TD) e outro para a recepção de dados (RD).

(obs.) Um cuidado importante a ser tomado é que sistemas de telefonia utilizam cabos do tipo par trançado, só que este tipo de cabo não serve para redes locais.

Cabo Coaxial

O cabo coaxial foi o primeiro cabo disponível no mercado, e era até a alguns anos atrás o meio de transmissão mais moderno que existia em termos de transporte de dados, existem 4 tipos diferentes de cabos coaxiais, chamados de 10Base5, 10Base2, RG-59/U e RG-62/U. O cabo 10Base5 é o mais antigo, usado geralmente em redes baseadas em mainframes. Outro modelo de cabo coaxial é o RG62/U, usado em

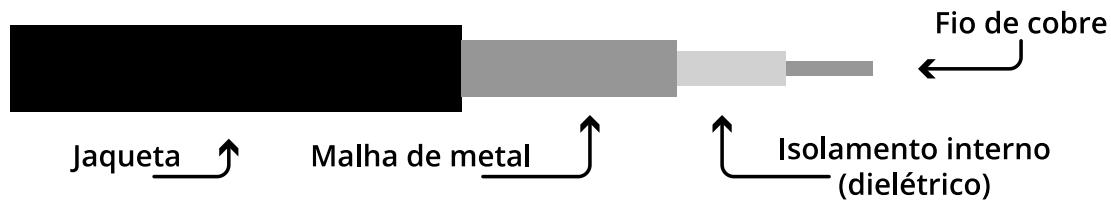
redes Arcnet. Existe também o cabo RG-59/U, aplicados na fiação de antenas de TV. Os cabos 10Base2, também chamados de cabos coaxiais finos, ou cabos Thinnet, são os cabos coaxiais usados em redes Ethernet, são os cabos mais populares nas lojas do ramo. Seu diâmetro é de 0.18 polegadas, aproximadamente de 4.7 milímetros, o que os tornam mais flexíveis e de fácil manuseio e instalação.

Cabos coaxiais são constituídos por 4 camadas:

- condutor interno, o fio de cobre que transmite os dados;
- uma camada isolante de plástico, chamada de dielétrico que envolve o cabo interno;
- uma malha de metal que protege as duas camadas internas;
- uma nova camada de revestimento, chamada de jaqueta.

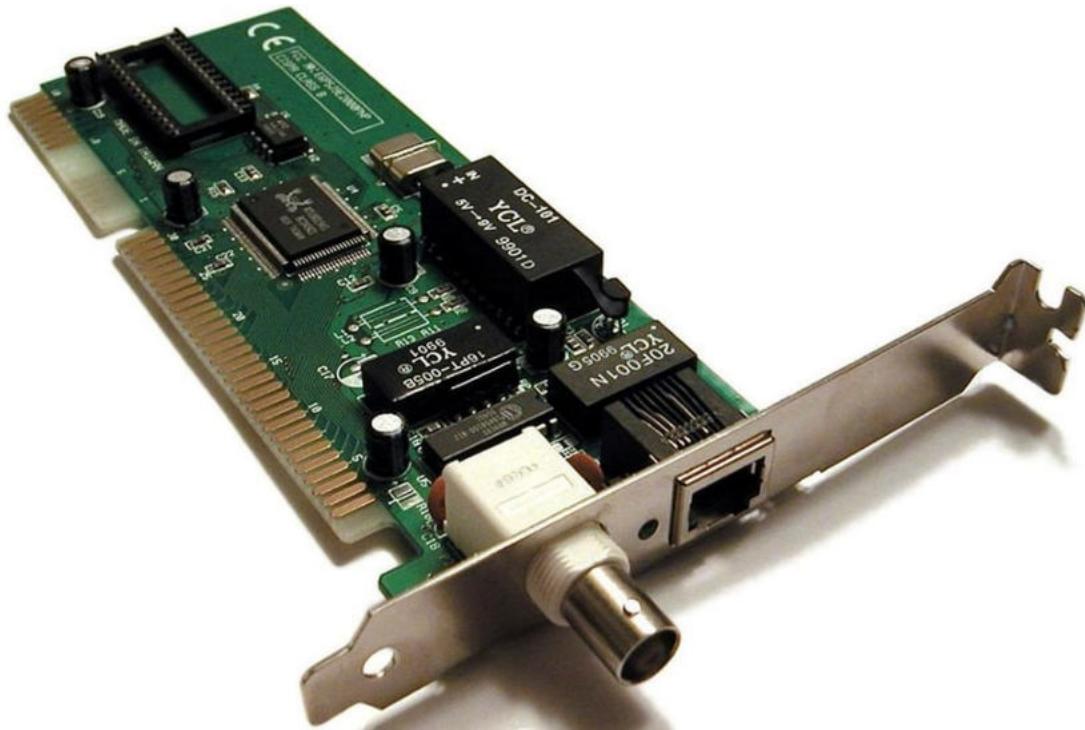
Figura 9: Estrutura do cabo coaxial

Estrutura do Cabo Coaxial



O cabo Thin Ethernet deve formar uma linha que vai da máquina de origem a máquina destino na rede, sem desvios. Não é possível formar configurações nas quais o cabo forma um "Y" no cabeamento. Apenas o primeiro e o último micro do cabo devem utilizar o terminador BNC.

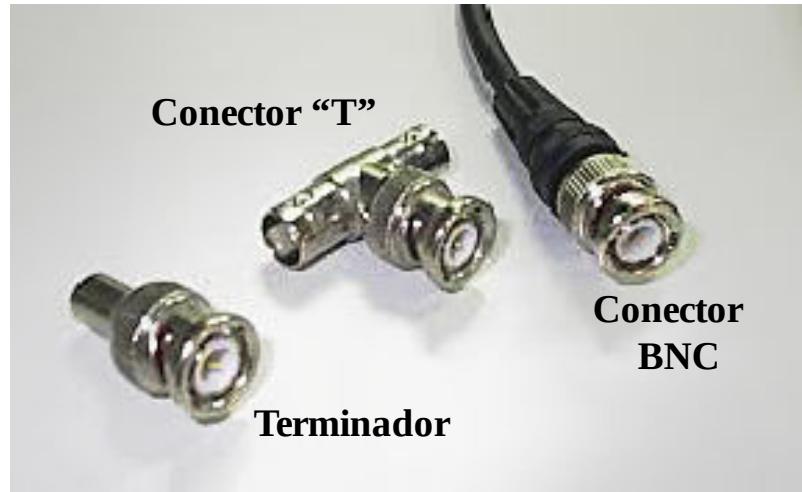
Figura 10: Placa de rede para rede com cabo coaxial



Fonte: Wikimedia Commons

O Cabo 10base2 tem a vantagem de dispensar hubs, pois a ligação entre os micros é feita através do conector “T”, mesmo assim o cabo coaxial caiu em desuso devido às suas desvantagens:

- Custo elevado,
- Instalação mais difícil e mais fragilidade,
- Se o terminador for retirado do cabo, toda a rede sai do ar.

Figura 11: Conectores e Terminador**Conectores e Terminador**

O “10” na sigla 10Base2, quer dizer que os cabos transmitem informações a uma velocidade de até 10 megabits por segundo, “Base” significa “banda base”, é a distância máxima que o sinal pode percorrer através do cabo, no caso o “2” que significa 200 metros, na prática é apenas um arredondamento, pois nos cabos 10Base2 a distância máxima utilizável é de 185 metros.

Figura 12: Cabo de rede coaxial

Fonte: Wikimedia Commons

O Uso de cabos 10Base2 deve ser de no mínimo de 50 cm ligando um cabo a outro, e o comprimento máximo do cabo (do primeiro ao último micro) não pode superar os 185 metros. Pode-se conectar até 30 micros no mesmo cabo, pois além dessa quantidade de máquinas aumenta o número de colisões de pacotes na rede e o desempenho será prejudicado em toda a rede.

Cabos de Fibra Óptica

É graças as fibras ópticas que a Internet e o sistema telefônico que existem hoje funcionam de maneira rápida. Com a transformação das tecnologias de rede para padrões de maiores velocidades como ATM, Gigabit Ethernet e 10 Gigabit Ethernet, a adesão de fibras ópticas vem tomando espaço também nas redes locais. O início de sua fabricação de deu em 1978 e substituiu os cabos coaxiais nos Estados Unidos na segunda metade dos anos 80. Em 1988, os primeiros cabos submarino de fibras ópticas mergulharam no oceano, dando inicio a superestrada da informação. O físico indiano Narinder Singh Kanpani é o inventor da fibra óptica, que passou a ter aplicações práticas na década de 60 com o advento da criação de fontes de luz de estado sólido, como o raio laser e o LED, diodo emissor de luz.

Existem dois tipos de fibras ópticas: As

- fibras multímodo
- fibras monomodo

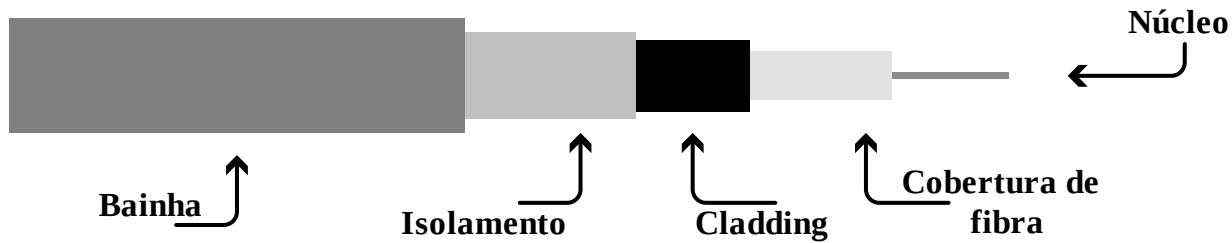
A opção por um desses tipos dependerá da sua aplicação da fibra. As fibras multímodo são utilizadas em aplicações de rede locais (LAN), enquanto as monomodo são mais utilizadas para aplicações de rede de longa distância (WAN), tem custo mais elevado, porém, mais eficientes que as multímodo. No Brasil, o uso da fibra se ampliou na segunda metade dos anos 90, com implementação dos backbones das operadoras de redes metropolitanas.

Indo na contra mão dos cabos coaxiais e de par trançado, que são apenas fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a qualquer tipo de interferência externa eletromagnética. Outra vantagem é que os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

O cabo de fibra óptica é composto por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e protege o núcleo. Logo depois possui uma camada de plástico protetora chamada de *cladding* e uma nova camada de isolamento e finalmente uma capa externa chamada *bainha*.

Figura 13: Estrutura de cabo de fibra óptica

Estrutura do Cabo de Fibra Óptica



A transmissão de dados por fibra óptica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho a uma velocidade de 10 a 15 MHz. As fontes de transmissão de luz podem ser diodos emissores de luz (LED) ou lasers semicondutores. O cabo óptico com transmissão de raio laser é o mais eficiente em potência devido a sua espessura reduzida. Já os cabos com diodos emissores de luz são muito baratos, além de serem mais adaptáveis à temperatura ambiente e de terem um ciclo de vida maior que o do laser.

O cabo de fibra óptica pode ser utilizado tanto em ligações ponto a ponto quanto em ligações multímodo. A fibra óptica permite a transmissão de muitos canais de informação de forma simultânea pelo mesmo cabo. Utiliza, por isso, a técnica conhecida como multiplexação onde cada sinal é transmitido numa frequência ou num intervalo de tempo diferente.

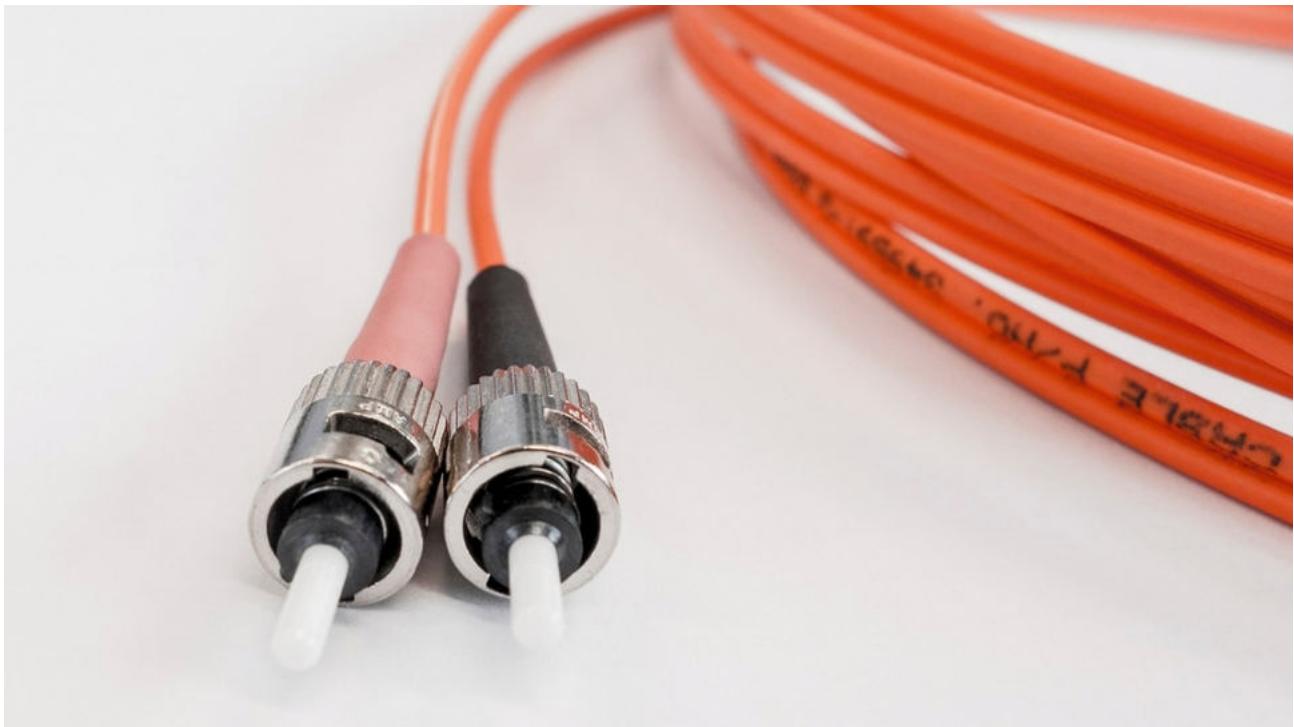
Figura 13: Placa de rede com conector para fibra óptica

Algumas vantagens da fibra óptica sobre os condutores de cobre são:

- Maior alcance;
- Maior velocidade;
- Imunidade a interferências eletromagnéticas;

O custo para aquisição de cabo de fibra óptica não é elevado em comparação com os cabos convencionais, mas seus conectores são bastante caros, assim como a mão de obra usada para a sua montagem. A montagem desses conectores exige cursos de especialização, instrumentos especiais, como microscópios, ferramentas específicas para corte e polimento, medidores e outros aparelhos sofisticados.

Figura 14: Cabo de fibra óptica



Fonte: @blickpixel em Pixabay

Pelo seu custo elevado, cabos de fibras ópticas são viáveis apenas quando precisam atingir grandes distâncias em redes que permitem segmentos de até 1 KM, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 5 KM (distâncias maiores são obtidas usando repetidores).

Mesmo permitindo longas distâncias, os cabos de fibra óptica alcançam taxas de transferências de até 155 mbps, sendo indicadas em ambientes que demandam uma grande transferência de dados. Como não produzem faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões. Outra grande vantagem, o sinal transmitido através dos cabos de fibra é mais difícil ser interceptado, sendo mais seguros para transmissões de dados sigilosos.

Os padrões mais comuns de redes usando fibra ótica são:

- FDDI (Fiber Distributed Data Interface)
- FOIRL (Fiber- Optic InterRepeater Link)
- 10BaseFL
- 100BaseFX
- 1000BaseSX
- 1000BaseLX



Meios de Transmissão não guiados



AUTORIA
Auro Lima Carvalho

Conceitos de redes sem fio (wireless)

A rede sem fio é uma rede de comunicação sem cabo por onde a transmissão de dados é realizada através de ondas. Atualmente, vários tipos de rede pode se enquadrar a esta definição, por exemplo, as redes utilizadas em provedores de internet, serviços de telefonia móvel ou apenas para uso pessoal e doméstico. As redes sem fio fazem parte da tecnologia e contribuem muito com o desenvolvimento da comunicação social. É uma tecnologia que cresce progressivamente, e que podem aumentar significativamente a quantidade de dados a serem transmitidos.

As redes sem fios surgiram para estabelecer uma comunicação entre os diversos dispositivos sem o uso de cabos. Este sistema possui grande importância do ponto de vista financeiro, pois essa economia dispensa o uso e presença de cabos. Por outro lado, o principal problema das redes sem fio é a segurança, o que torna necessário o desenvolvimento de padrões específicos para manter a rede imune qualquer tipo de invasões ou por roubar qualquer informação. No caso da internet, estes sistemas de segurança recebem o nome de WPA, WP2 e WEP.

O wireless é um termo inglês associado à rede WI-FI (Wireless Fidelity). Muitos veem essa abreviatura todos os dias, mas nem todos sabem o que realmente significa. Em português WI-FI significa fidelidade sem fio, ao pé da letra e wireless significa não possuir fios. No surgimento da internet, estar conectado significava literalmente estar conectado a um cabo e isso impossibilitava sua locomoção. O wireless também apresenta regras ou protocolos que estão relacionadas à tecnologia do rádio e da televisão.

O wireless baseia-se de uma frequência que leva os dados do computador para o router e assim se conecta as redes. Assim que os dados se encontram no router, eles são transmitidos do cabo para os provedores da internet e então transmitidos ao mundo virtual. O wireless é uma tecnologia que abrange vários campos, logo todo aparelho que opera sem o uso de fios ou cabos pra transmissão pode ser considerado wireless.

A tecnologia wireless pode sofrer interferências, por isso é muito importante que a distância da conexão esteja apropriada ao link que se deseja estabelecer. Assim o sinal chega ao receptor de forma nítida e conecta-se como se fosse um cabo. O termo WI-FI foi criado por uma empresa comercial, ocorreu quando diversas empresas se uniram e desenvolveram um padrão de comunicação sem fio para uso nos computadores. Assim que padronizada o uso da tecnologia wireless, foi contratada uma empresa de publicidade que criou o termo WI-FI para que os usuários em geral conhecessem que se tratava toda vez que fosse mencionada essa palavra. Associaram ao símbolo do Ying-Yang para tornar o standard wireless mais chamativo e atrativo.

Caso não tivessem contratado essa empresa, a tecnologia wireless seria conhecida na informática como “IEEE 802.11b de sequência direta”, logo esse nome não seria possível fazer publicidade.

Revolução em constante desenvolvimento

As redes sem fio revolucionaram o campo das telecomunicações. Significaram um grande progresso à medida que proporcionam uma melhor conexão para todo lugar habitado que exista algum tipo de cobertura. Essa nova tecnologia tem minimizado os custos significativamente pela questão do não uso de cabos. Espera-se que no futuro próximo tenhamos melhorias na tecnologia das redes sem fio para que aumente sua eficiência e abrangência.



Conclusão - Unidade 1

Chegamos ao final da primeira unidade de estudos sobre redes de computadores, onde abordamos a definição e o contexto histórico das redes de comunicação de dados, mostrando um grande leque de funções e recursos disponíveis na rede.

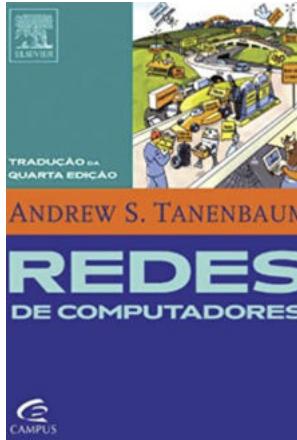
Conhecemos os tipos básicos de redes, suas topologias e modelos que se enquadram melhor em cada organização e a sinalização de circuitos usados para permitir que os computadores troquem dados entre si, os tipos de cabos usados em comunicação para transporte de dados do transmissor ao receptor.

Além dos transportes de dados dos meios guiados, conhecemos também os meios não guiados de informação que são as redes sem fio também chamadas de *wireless*, ou qualquer dispositivo que tenha transmissão sem o uso de cabos, como televisores de controle remoto, brinquedos e drones, onde essa tecnologia veio para ficar e revolucionar os meios de transmissão de dados e informações.

Nossa missão nesse primeiro material foi apresentar a você aluno(a) uma introdução a tecnologia de redes e sistemas de cabeamento estruturado, com a intenção de estimulá-lo(a) a explorar mais essa área que tem um vasto campo de atuação profissional tecnológica.

Até a próxima unidade, bons estudos!!

Material Complementar



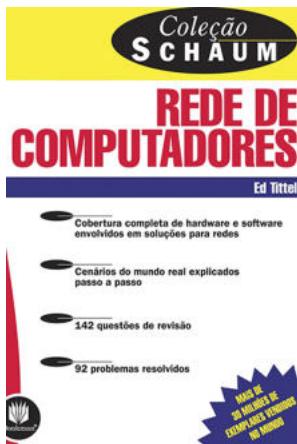
Livro

Redes de Computadores

Autor: Andrew S. Tanenbaum

Editora: Elsevier

Sinopse: As principais conquistas tecnológicas do século XX se deram no campo da aquisição, do processamento e da distribuição de informações. Entre outros desenvolvimentos, vimos a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria da informática e o lançamento dos satélites de comunicação.



Livro

Redes de Computadores

Autor: Ed Tittel

Editora: Bookman

Sinopse: As tecnologias usadas para transferir dados entre computadores envolvem muitas metodologias e componentes diferentes. Uma das principais finalidades da comunicação de dados é permitir que diferentes *hardware*s e sistemas operacionais se comuniquem e se entendam entre si. Para tanto, o meio de transmissão envolvido na comunicação de dados tem que atender a certas especificações de *hardware* e o *software* usado pelo sistema operacional do computador, para ter acesso ao meio de transmissão, precisa estar de acordo com os padrões.



Filme

Transcendence - A Revolução

Ano: 2014

Sinopse: Dr. Will Caster, a maior autoridade do mundo em inteligência artificial, está conduzindo experimentos altamente controversos, na intenção de criar um robô com grande variedade de emoções humanas. Quando extremistas antitecnologia tentam matá-lo, Caster convence sua esposa, Evelyn, e seu melhor amigo, Max Waters, a testar seu novo invento nele mesmo. Só que a grande questão não é se eles podem fazer isto, mas se eles devem dar este passo.

Referências

CDIM, Daniel. **Redes de Computadores.** Disponível em: <https://www.ebah.com.br/content/ABAAAfZKcAD/rede-computadores>. Acesso em: 12/06/2019

Editorial Que Conceito. Sao Paulo. Disponível em: <https://www.queconceito.com.br/rede-wireless>. Acesso em: 30/05/2019.

KUROSE, James F; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-dow. 6 ed. São Paulo: Pearson Education do Brasil, 2013.

LIMA FILHO, Eduardo Correa. **Fundamentos de rede e cabeamento estruturado.** São Paulo: Pearson Education do Brasil, 2015.

PILLOU, Jean-François. **Tipos de Redes.** Disponível em: <https://br.ccm.net/contents/259-tipos-de-redes>. Acesso em 12/06/2019.

Redes de Computadores. Disponível em: <https://www.guiadacarreira.com.br/cursos/redes-de-computadores/>. Acesso em 12/06/2019.

TANENBAUM, Andrew S. **Redes de Computadores.** / Andrew S. Tanenbaum; **tradução de Vanderberg D. Souza. - Rio de Janeiro: Elsevier, 2003 - 15ª Reimpressão.**

TITTEL, ED; **Redes de Computadores**, Porto Alegre: Bookman, 2003.

WETHERAL, Davi. **Redes de Computadores.** 5º Edição, 2012. Disponível em:<https://estudoderedes.wordpress.com/2012/01/17/meios-de-transmissao-guiados/>



Centro Universitário Cidade Verde

| Unidade 2

Satélites e Equipamentos de Rede



AUTORIA

Auro Lima Carvalho

Introdução

Dando continuidade aos nossos estudos sobre redes de computadores, iremos abordar a comunicação via satélite, que são aquelas que utilizam como forma de transmitir dados ondas de rádio (normalmente micro-ondas) enviadas por satélites artificiais em órbita da Terra.

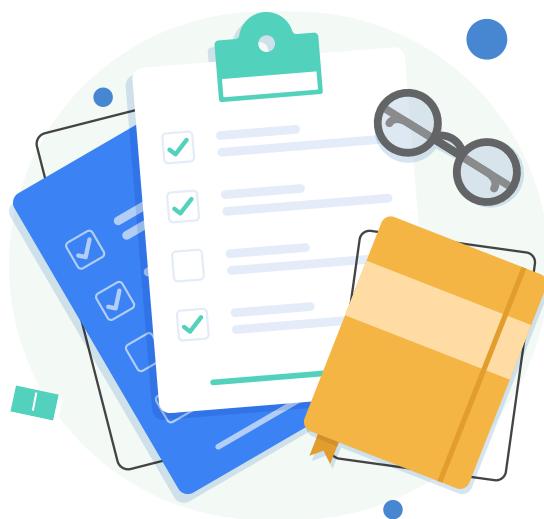
A comunicação via satélite possui a vantagem de estabelecer contato direto com navios e aviões mesmo em movimento, algo que não pode ser feito via cabos. Outra vantagem do envio de mensagens por meio de satélites é chegar até as regiões mais isoladas de comunicação do planeta, mesmo em locais que não tenham infraestrutura de cabos.

Os custos muito elevados tornam a comunicação via satélites inviáveis. Lançar em órbita um satélite artificial é caríssimo e, além de o equipamento necessitará de manutenções periódicas. Algumas empresas especializadas no ramo de comunicação já alugam satélites que já estão em órbita, mas os custos também são elevados ainda.

A comunicação via satélites é bastante utilizada para envio de sinais de televisão e rádio.

Componentes de redes como *hub*, *switch* e roteador são nomes dados a equipamentos que possibilitam a conexão de computadores em rede. Estudaremos exatamente a diferença entre esses dispositivos, e o que cada equipamento faz e quando usar cada um, também sobre a evolução dos padrões de comunicação.

Bons estudos!



Plano de Estudo



Satélites de Comunicações.



Satélites terrestres de baixa órbita.



Equipamentos de Rede.

Objetivos de Aprendizagem



Destacar o histórico, o papel e funções dos satélites de comunicação.



Conhecer os tipos de satélites.



Apresentar os equipamentos de redes, funcionamento e meios de transmissão de dados.



Compreender as topologias dos equipamentos de redes e meios de transmissão.





Satélites de Comunicações



AUTORIA
Auro Lima Carvalho

Na década de 1950 e no início dos anos 60, as pessoas tentavam configurar sistemas de comunicações emitindo sinais que se refletiam em balões meteorológicos metalizados. Infelizmente, os sinais recebidos eram muito fracos para que tivessem algum uso prático. Em seguida, a Marinha dos EUA detectou uma espécie de balão meteorológico que ficava permanentemente no céu - a Lua - e criou um sistema operacional para comunicação entre o navio e a base que utilizava a Lua em suas transmissões.

O progresso no campo da comunicação celeste precisou esperar até que o primeiro satélite de comunicação fosse lançado. A principal diferença entre um satélite artificial e um real é que o artificial amplifica os sinais antes de enviá-los de volta, transformando uma estranha curiosidade em um avançado sistema de comunicação.

Os satélites de comunicação possuem algumas propriedades interessantes, que os tornam atraentes para muitas aplicações. Em sua forma mais simples, um satélite de comunicações pode ser considerado um grande repetidor de micro-ondas no céu. Ele contém diversos **tranponders**; cada um deles ouve uma parte do espectro, amplifica os sinais de entrada e os transmite novamente em outra frequência, para evitar interferência com o sinal de entrada. Os feixes descendentes podem ser largos, cobrindo uma fração substancial da superfície terrestre, ou estreitos, cobrindo uma área com apenas centenas de quilômetros de diâmetro. Esse modo de operação é conhecido como funcionamento como espelho (bent pipe).



REFLITA

Os satélites podem cair?

Sim, mas os riscos são pequenos. Os satélites orbitam em diferentes alturas, velocidades e caminhos. Eles conseguem permanecer em órbita porque sua velocidade está em equilíbrio com a força da gravidade. Quando isso deixa de acontecer – quando o satélite perde velocidade por algum motivo – o satélite pode cair na Terra ou continuar em linha reta e ir para o espaço. No entanto, é mais provável que o satélite se desintegre antes de chegar ao solo.

[ACESSAR](#)

De acordo com a lei de Kepler, o período orbital de um satélite varia de acordo com o raio da órbita elevado à potência 3/2. Quanto mais alto o satélite, mais longo o período. Perto da superfície da Terra, o período é de cerca de 90 minutos. Consequentemente, os satélites de baixa órbitas saem da visão com bastante rapidez, e assim são necessários muitos deles para proporcionar coberturas contínua. A uma altitude de aproximadamente 35.800 km, o período é de 24 horas. Na altitude de 384.000km, o período é de cerca de um mês, como podemos atestar qualquer pessoa que observe a Lua regularmente.

O período do satélite é importante, mas não é o único fator para se determinar onde posicioná-lo. Outra questão é a presença dos cinturões de *Van Allen*, camadas de partículas altamente carregadas que são capturadas pelo campo magnético terrestre. Qualquer satélite em órbita dentro deles seria destruído com bastante rapidez pelas partículas carregadas com alta energia presas pelo campo magnético da Terra.



Em 1945, o escritor de ficção científica Arthur C. Clarke calculou que um satélite na altitude de 35.800km em órbita circular equatorial pareceria permanecer imóvel no céu, e assim não precisaria ser rastreado (Tanenbaum, 2003, p117).

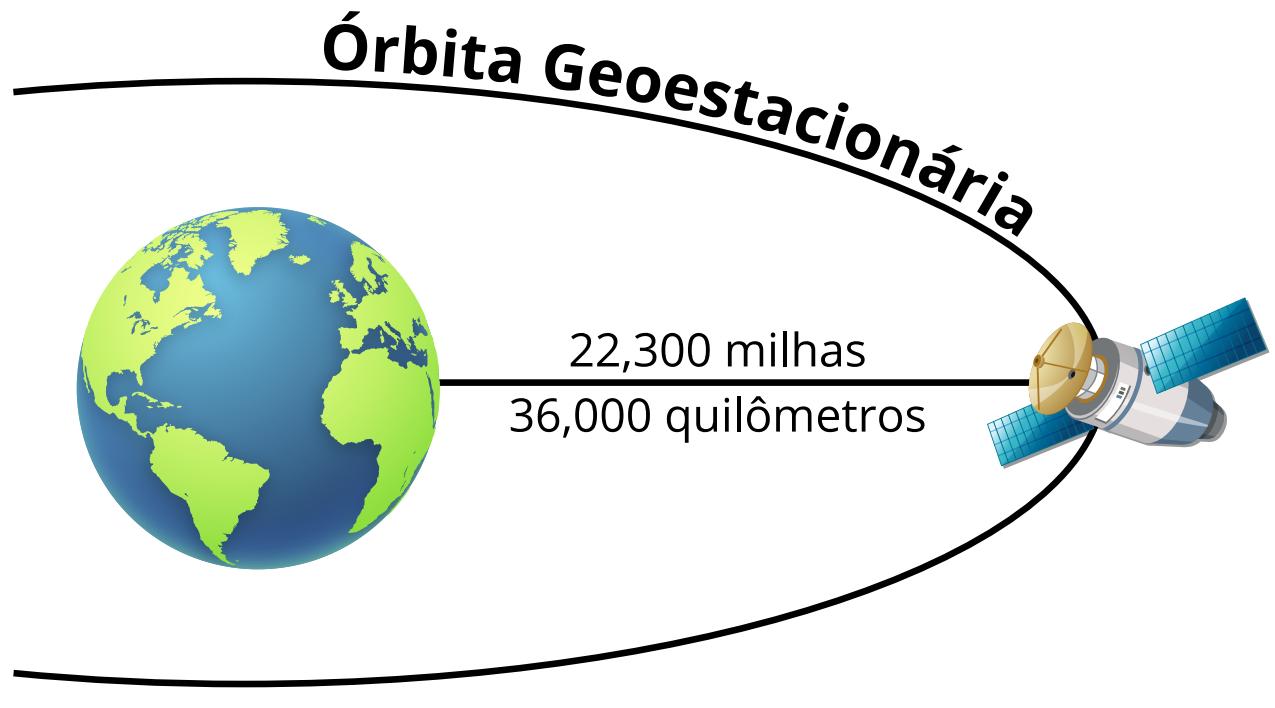
Satélites Estacionários

Este tipo de satélite fica sempre localizado acima da linha do Equador, a uma altitude de aproximadamente 36 mil km e move-se ao redor da terra em uma velocidade angular idêntica à da rotação do planeta. Com isso, do ponto de vista de um observador terrestre, o satélite sempre parece estar parado no céu.

A grande vantagem deste tipo de satélite é que para que o seu sinal seja captado, basta apontar a antena para o ponto certo do céu. Depois disso, não é mais necessário mudar a posição da antena e nem usar equipamentos caros para prever o movimento do satélite.

A desvantagem é que como todos os satélites estacionários devem estar sobre a linha do equador a uma mesma altitude, existe um espaço limitado para colocá-los no espaço. Além disso, países que ficam localizados a uma mesma longitude podem entrar em conflito para decidir quem irá colocar um satélite para atender à sua população. Tais conflitos normalmente são julgados pela União Internacional de Telecomunicações, uma organização internacional.

Figura 1: Órbita geoestacionária



Fonte: Susana Ferreira, Escola: Escola Secundária de Caldas de Vizela, Data de Publicação: 20/12/2007.

Satélites em Órbita Terrestre Baixa.

Estes são os satélites que ficam a uma altura entre 350 e 1400 km. Qualquer satélite que fique a uma altura inferior a esta seriam instáveis, pois sua velocidade sofreria interferência da atmosfera.

Como satélites nesta altitude precisam de menos energia para ser enviados e para enviar dados devido a uma distância menor da Terra, manter um satélite nesta altitude é mais barato. A desvantagem é que como eles não possuem órbitas estacionárias, para manter a comunicação com um ponto da Terra, é preciso usar uma rede de satélites. Por outro lado, pelo fato de os satélites estarem muito próximos da Terra, as estações terrestres não precisam de muita potência, e o retardamento de ida e volta é de apenas alguns milissegundos.

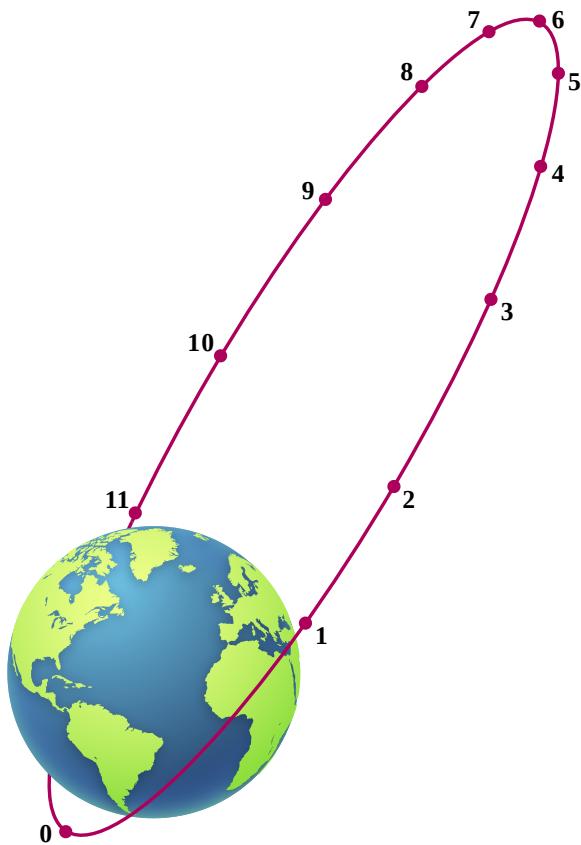
Satélites terrestres de órbita média

Entre os dois cinturões de Van Allen, localizados em altitudes mais baixas, localizam-se os satélites MEO(Medium-Earth Orbit). Vistos da terra, os mesmos se movimentam muito devagar em longitude, gastando em média seis horas para fazer a volta completa na Terra. Como consequência, são acompanhados à medida que se movem no céu. Pelo fato de estarem em órbitas mais baixas que os GEOs,

eles têm uma área de cobertura menor no solo e exigem transmissores menos potentes para alcançá-los. Nos dias atuais, esses modelos de satélites cairam em desuso pra telecomunicações, os 24 satélites GPS (Global Positioning System) que estão em órbita a cerca de 18.000 km de altitude são exemplos de satélites MEO.

Satélite Molniya

Figura 2: Órbita Molniya



Fonte: ÓRBITA MOLNIYA. In: WIKIPÉDIA, a encyclopédia livre. Flórida: Wikimedia Foundation, 2019. [Disponível aqui](#)

Satélites deste tipo fazem uma órbita elíptica ao redor da Terra. Isso faz com que eles se movam, mas passem a maior parte do tempo em uma determinada latitude. Este tipo de satélite é usado principalmente na Rússia. Em 1967, uma rede nacional de televisão soviética foi criada e funcionava graças a satélites deste tipo.

Como satélites estacionários não funcionam bem para transmitir dados para pontos muito distantes da linha do Equador, os satélites molniya são a forma mais eficiente de transmitir dados para regiões localizadas em latitudes altas.

Satélites de Molniya são tipicamente usados para a telefonia e televisão na Rússia. Além disso, podem ser usados para sistemas de rádio móveis mesmo em latitudes menores, pois carros viajando através de áreas urbanas precisam de satélites em

grandes altitudes para manter uma boa conectividade mesmo quando próximos de construções altas.



Equipamentos de Redes



AUTORIA
Auro Lima Carvalho

Tittel (2003), quase todas as redes modernas são criadas pela conexão de vários dispositivos físicos para estabelecer um caminho desde o dispositivo de transmissão até o dispositivo de recepção, daremos enfoque aos mais comuns, como placas de redes, cabos, nobreak, *hubs*, repetidores, pontes, roteadores, etc.

Placas de Redes - adaptadores ou NIC

Uma NIC é um dispositivo de hardware responsável pela comunicação entre os computadores da rede toda placa possui um endereço MAC (que identifica cada placa de rede no mundo e este deve ser único. Se duas placas tiverem o mesmo endereço MAC, o servidor não saberá a quem entregar a informação e poderá congestionar toda a rede, acontecerá um conflito entre o endereço Físico x Lógico na rede.

Tipos de placas de redes:

- Placas Wireless - PCI
- Placas Wireless - Portátil
- Placa PCI - RJ45

Nobreak

Fornecimento de energia sem interrupções aos equipamentos de rede é a principal função do equipamento *Nobreak*, mesmo sem energia nenhuma fornecida da rede elétrica. Este armazenamento é graças ao uso de baterias, que podem gerar várias horas de fornecimento de energia, dependendo da configuração do *nobreak*. Existem nobreaks de baixa, média e alta potência. Os nobreaks de baixa potência, oferecem autonomia de até 15 minutos, suficiente para o usuário salvar e fechar todos os arquivos com segurança. Os de alta potência utilizam motores a combustão na geração de energia, como por exemplo, gasolina ou diesel para permanecer ligado o quanto for necessário.

Há três categorias de *nobreak*:

- Convencional
- Inteligente
- Senoidal

Convencional apenas recebe energia e estabiliza o envio na rede, sem gerenciamento.

O inteligente possui uma interface entre *nobreak* e o computador, permitindo a monitoração do sistema e das baterias do aparelho através de software próprio para este fim. Os softwares de monitoração permitem a emissão de relatórios e gráficos de ocorrências de falhas de energia e a execução de shutdown ou fechamento dos programas que estão sendo executados na falta de energia elétrica, e os restabelece no retorno da energia.

Senoidal é um equipamento de fornecimento de energia que equaliza e equilibra as ondas em seu formato mais puro (senoidal) padronizando o fornecimento de energia a fim de garantir a segurança e o funcionamento correto de aparelhos mais sensíveis como, por exemplo, aqueles utilizados na área hospitalar e médica.



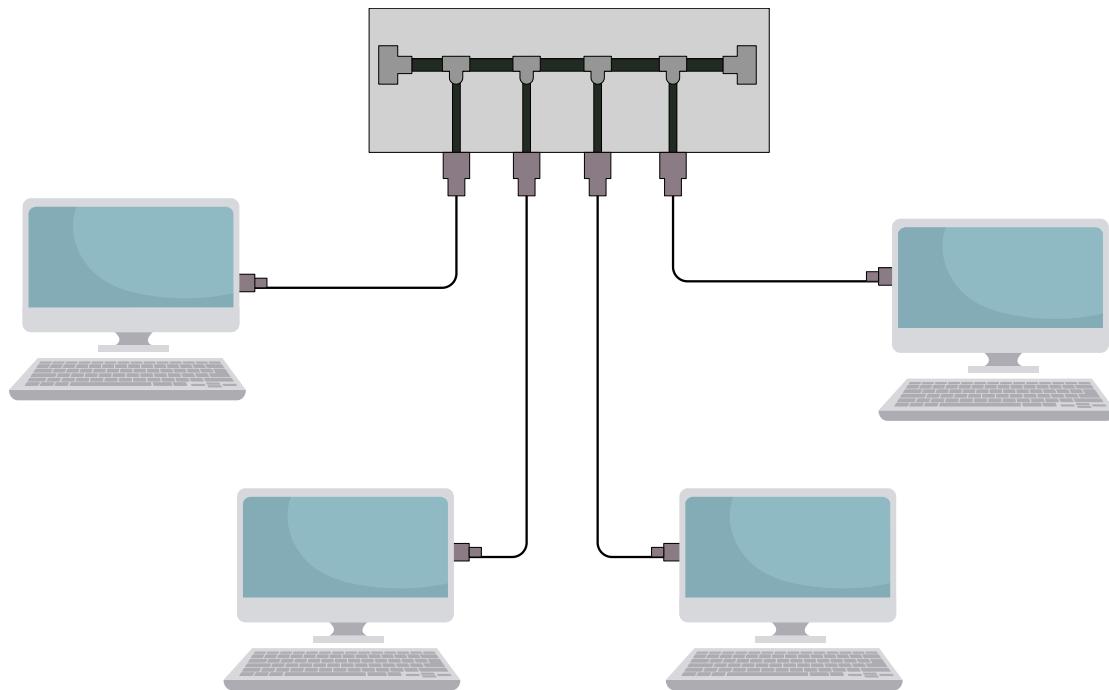
Hubs



AUTORIA
Auro Lima Carvalho

Os *Hubs* são componentes de redes responsáveis por centralizar e distribuir quadros de dados por toda a rede física. Funcionando assim como equipamento central, que recebe os dados transmitidos pelas estações e os repassam para todas as demais.

Figura 3: Hubs



Fonte: acesse o link [Disponível aqui](#)

O que é Broadcast?

Broadcast (do Inglês, "transmitir"), é o processo onde se propaga e difunde determinada informação, onde sua principal característica é que a informação está sendo enviada para todos os receptores ao mesmo tempo na rede. A televisão aberta e o rádio são exemplos práticos de transmissões através de broadcast, onde várias antenas de transmitem o sinal televisivo (ou, radiodifusor) através de ondas eletromagnéticas e são captadas por aparelhos de TVs (ou, rádios) que ao captar poderá sintonizar o sinal. Em informática, o broadcast é utilizado em *hubs* (concentradores) ligados em redes LAN, MAN, WAN.

Figura 4: Hub

Fonte: @fotoslaz em Freepik

Existem vários tipos de *hubs*, vejamos:

- **Passivos:** O termo “*Hub*” é um termo comum para definir qualquer tipo de componente concentrador. Os concentradores de cabos que não possuem alimentação elétrica são chamados *hubs* passivos, funcionam como um espelho, reenviando os sinais recebidos para as estações conectadas nele. Um *hub* passivo somente distribui um determinado sinal, sem fazer nenhum tipo de amplificação, e a conexão de cabos entre micros, passando pelo *hub*, não pode ser maior que 100 metros permitidos pelos cabos de par trançado.
- **Ativos:** São modelos de *hubs* que regeneram os sinais recebidos na rede em suas portas antes de enviá-los para todas as portas conectadas a ele. Exerce o papel de repetidor. No *hub* passivo o sinal trafega apenas 100 metros somados os dois trechos de cabos entre as estações, usando um *hub* ativo o sinal pode trafegar por 100 metros até o *hub*, e depois mais 100 metros após ser retransmitido por ele, completando seu trajeto.
- **Inteligentes:** São *hubs* que permitem todo o tipo de controle operacional. Este controle é feito via software capaz de encontrar qualquer tipo de erro que prejudique o desempenho da rede e desconectar estações com problemas de tráfego ou mesmo que derrube a rede inteira. Localizar pontos de congestionamento na rede, e criar ações para normalizar o tráfego, detectar e bloquear tentativas de invasão e acessos não autorizados à rede, etc., esse modelo depende do modelo e fabricante do *Hub*.

Cascateamento

Existe a possibilidade de conectar dois ou mais *hubs* entre si. Quase todos os *hubs* possuem uma porta chamada “Up Link” que se destina justamente a esta conexão. Basta ligar as portas Up Link de ambos os *hubs*, usando um cabo de rede normal para que os *hubs* passem a se enxergar.

Sendo que existem alguns *hubs* mais baratos não possuem a porta “Up Link”, mas com um cabo cross-over pode-se conectar dois *hubs*. A única diferença neste caso é que ao invés de usar as portas Up Link, usará duas portas comuns.

Note que caso você esteja interligando *hubs* passivos, a distância total entre dois micros da rede, incluindo o trecho entre os *hubs*, não poderá ser maior que 100 metros, o que é bem pouco no caso de uma rede grande. Neste caso, seria mais recomendável usar *hubs* ativos, que amplificam o sinal.

Figura 5: Roteador com porta uplink



Fonte: Tech Terms [Disponível aqui](#)

Empilhamento

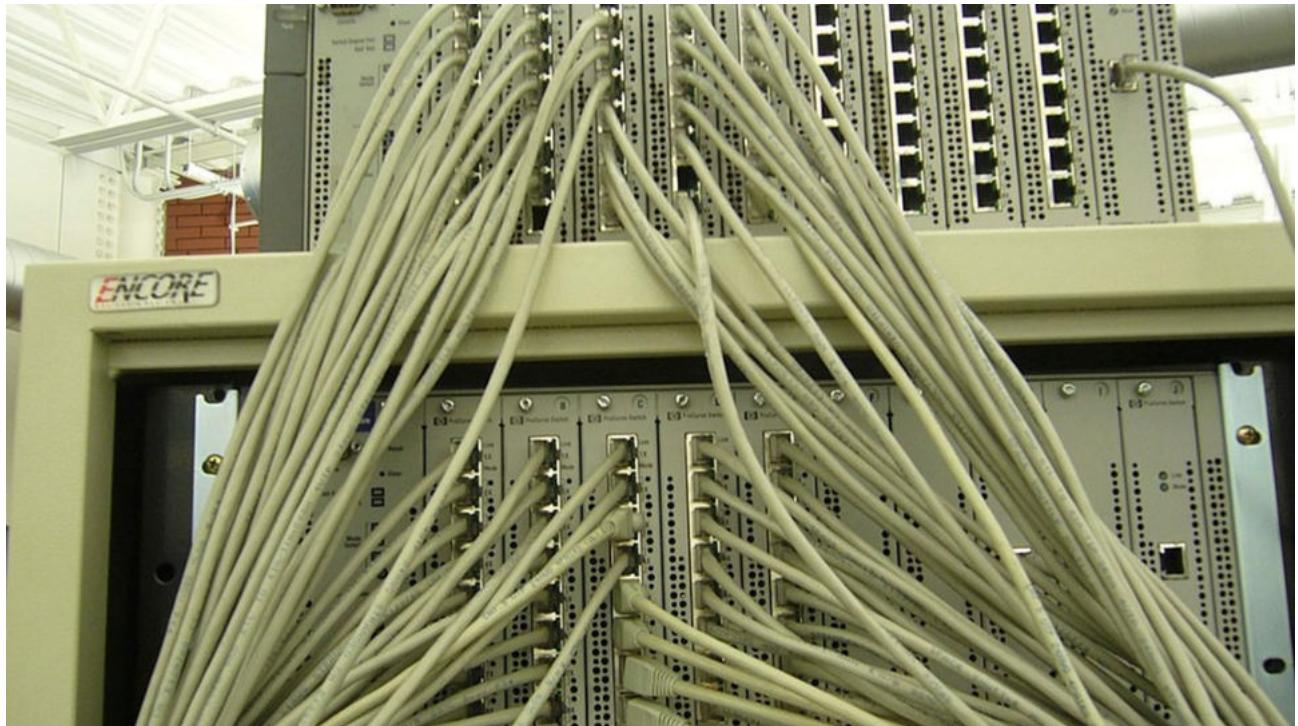
O recurso de conectar *hubs* usando a porta Up Link, ou usando cabos cross-over, é utilizável apenas em redes pequenas, pois qualquer sinal transmitido por um micro da rede será retransmitido para todos os outros. Quanto mais Computadores

tivermos na rede, maior será o tráfego e mais lenta a rede será e apesar de existirem limites para conexão entre *hubs* e repetidores, não há qualquer limite para o número de portas que um *hub* pode ter. Assim, para resolver esses problemas os fabricantes desenvolveram o *hub* empilhável.

Esse *hub* possui uma porta especial em sua parte traseira, que permite a conexão entre dois ou mais *hubs*. Essa conexão especial faz com que os *hubs* sejam considerados pela rede um só *hub* e não *hubs* separados, eliminando estes problemas. O empilhamento só funciona com *hubs* da mesma marca.

A interligação através de porta específica com o cabo de empilhamento (*stack*) tem velocidade de transmissão maior que a velocidade das portas.

Figura 6: Hubs empilháveis



Fonte: @Takuya Oikawa em Wikimedia Commons



Repetidores



AUTORIA
Auro Lima Carvalho

O repetidor é um dispositivo responsável por ampliar o tamanho máximo do cabeamento da rede. Ele funciona como um amplificador de sinais, regenerando os sinais recebidos e transmitindo esses sinais para outro segmento da rede.

Como o nome sugere, ele repete as informações recebidas em sua porta de entrada na sua porta de saída. Isso significa que os dados que ele mandar para um micro em um segmento, estes dados estarão disponíveis em todos os segmentos, pois o repetidor é um elemento que não analisa os quadros de dados para verificar para qual segmento o quadro é destinado. Assim ele realmente funciona como um “extensor” do cabeamento da rede. É como se todos os segmentos de rede estivessem fisicamente instalados no mesmo segmento.

Apesar de aumentar o comprimento da rede, o repetidor traz como desvantagem diminuir o desempenho da rede. Isso ocorre porque, como existirão mais máquinas na rede, as chances de o cabeamento estar livre para o envio de um dado serão menores. E quando o cabeamento está livre, as chances de uma colisão serão maiores, já que teremos mais máquinas na rede.

Atualmente não encontram-se repetidores como equipamento independentes, esse equipamento está embutido dentro de outros, especialmente do *hub*. O *hub* é, na verdade, um repetidor (mas nem todo repetidor é um *hub*), já que ele repete os dados que chegam em uma de suas portas para todas as demais portas existentes.



Bridges (Pontes)



AUTORIA

Auro Lima Carvalho

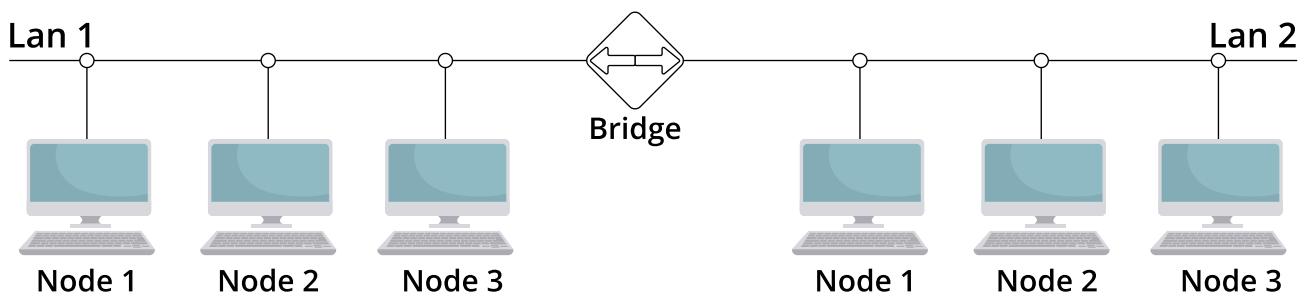
Assim que o número de usuários começou a exceder o limite de um único segmento de rede, houve a necessidade de se criar um novo segmento para ligar duas redes juntas. Isso foi feito por um dispositivo chamado ponte(bridge). Originalmente, as pontes tinham só duas portas, uma para cada rede. Entretanto, ao contrário dos *hubs*, as pontes, atualmente, inspecionam os dados que passam através delas e tomam decisões sobre se devem mandá-los para a outra rede ou não. Essa decisão baseia-se nos endereços MAC nas redes Ethernet e no número do anel nas redes Token Ring.

Pontes Ethernet escutam o tráfego enviado por computadores e outros dispositivos de rede e, então, gravam o endereço MAC do computador, que está localizado no campo Endereço da Fonte do cabeçalho do quadro da Ethernet, e a porta da qual o endereço foi assimilado. Se a ponte recebe , então, um quadro da outra rede que é destinado para o endereço MAC assimilado da primeira rede, ela enviará o quadro para a primeira rede. (TITTEL 2003).

Como vimos anteriormente que os repetidores transmitem todos os dados que recebe para todas as suas saídas, assim, quando uma máquina transmite dados para outra máquina presente no mesmo segmento, todas as máquinas da rede recebem esses dados, mesmo aquelas que estão em outro segmento.

A ponte é um repetidor Inteligente. Ela tem a capacidade de ler e analisar os quadros de dados que estão circulando na rede. Com isso ela consegue ler os campos de endereçamentos MAC do quadro de dados. Fazendo com que a ponte não replique para outros segmentos dados que tenham como destino o mesmo segmento de origem. Outro papel que a ponte em princípio poderia ter é o de interligar redes que possuem arquiteturas diferentes.

Figura 7: Ponte



Fonte: acesse o link [Disponível aqui](#)



Switches



AUTORIA

Auro Lima Carvalho

O *switch* é um *hub* que, em vez de ser um repetidor é uma ponte. Com isso, em vez dele replicar os dados recebidos para todas as suas portas, ele envia os dados somente para o micro que requisitou os dados através da análise da Camada de link de dados onde possui o endereço MAC da placa de rede do micro, dando a idéia assim de que o *switch* é um *hub* Inteligente, além do fato dos *switches* trazerem micros processadores internos, que garantem ao aparelho um poder de processamento capaz de traçar os melhores caminhos para o tráfego dos dados, evitando a colisão dos pacotes e ainda conseguindo tornar a rede mais confiável e estável.

Figura 8: Switch



Fonte: @www.heimnetzwerke.net em Wikimedia Commons

De maneira geral a função do *switch* é muito parecida com a de um bridge, com a exceção que um *switch* tem mais portas e um melhor desempenho, já que manterá o cabeamento da rede livre. Outra vantagem é que mais de uma comunicação pode ser estabelecida simultaneamente, desde que as comunicações não envolvam portas de origem ou destino que já estejam sendo usadas em outras comunicações.

Existem duas arquiteturas básicas de *Switches* de rede: "cut-through" e "store-and-forward":

- **Cut-through:** examina o endereço de destino e reencaminhar o pacote.
- **Store-and-forward:** recebe e analisa o pacote por inteiro antes de o reencaminhar. Esta análise do pacote permite localizar alguns erros, evitando a sua propagação pela rede. Atualmente o mercado oferece vários modelos de *Switches* híbridos que possuem ambas arquiteturas.

Diferença entre *Hubs* e *Switches*

- Um *hub* simplesmente retransmite todos os dados que chegam para todas as estações conectadas a ele, como um espelho. Causando o famoso broadcast que causa muito conflitos de pacotes e faz com que a rede fique muito lenta.
- O *switch* analisa e encaminha somente para o destinatário, pois ele identifica as máquinas pelo o MAC address que é estático. Isto traz uma vantagem considerável em termos desempenho para redes congestionadas, além de permitir que, em casos de redes, onde são misturadas placas 10/10 e 10/100, as comunicações possam ser feitas na velocidade das placas envolvidas. Ou seja, quando duas placas 10/100 trocarem dados, a comunicação será feita a 100M bits. Quando uma das placas de 10M bits estiver envolvida, será feita a 10M bits.(TORRES, 2014)



Roteadores



AUTORIA
Auro Lima Carvalho

Embora a separação de segmentos de redes tenham sido útil, todos os dispositivos ligados aos *hubs*, às pontes e aos comutadores ainda estão no mesmo domínio de broadcast, e há limites práticos do número de dispositivos que podem existir em um domínio de broadcast. Então, para separar os domínios de broadcast, foram criados os roteadores, que atuam como fronteiras entre domínios de broadcast. Da mesma maneira que as pontes e os comutadores leem e atuam nos cabeçalhos de camada 2, os roteadores lêem e tomam decisões em cabeçalhos de camada 3, como os cabeçalhos do TPC/IP e do IPX. Portanto, dizemos que os roteadores são dispositivos de camada 3.

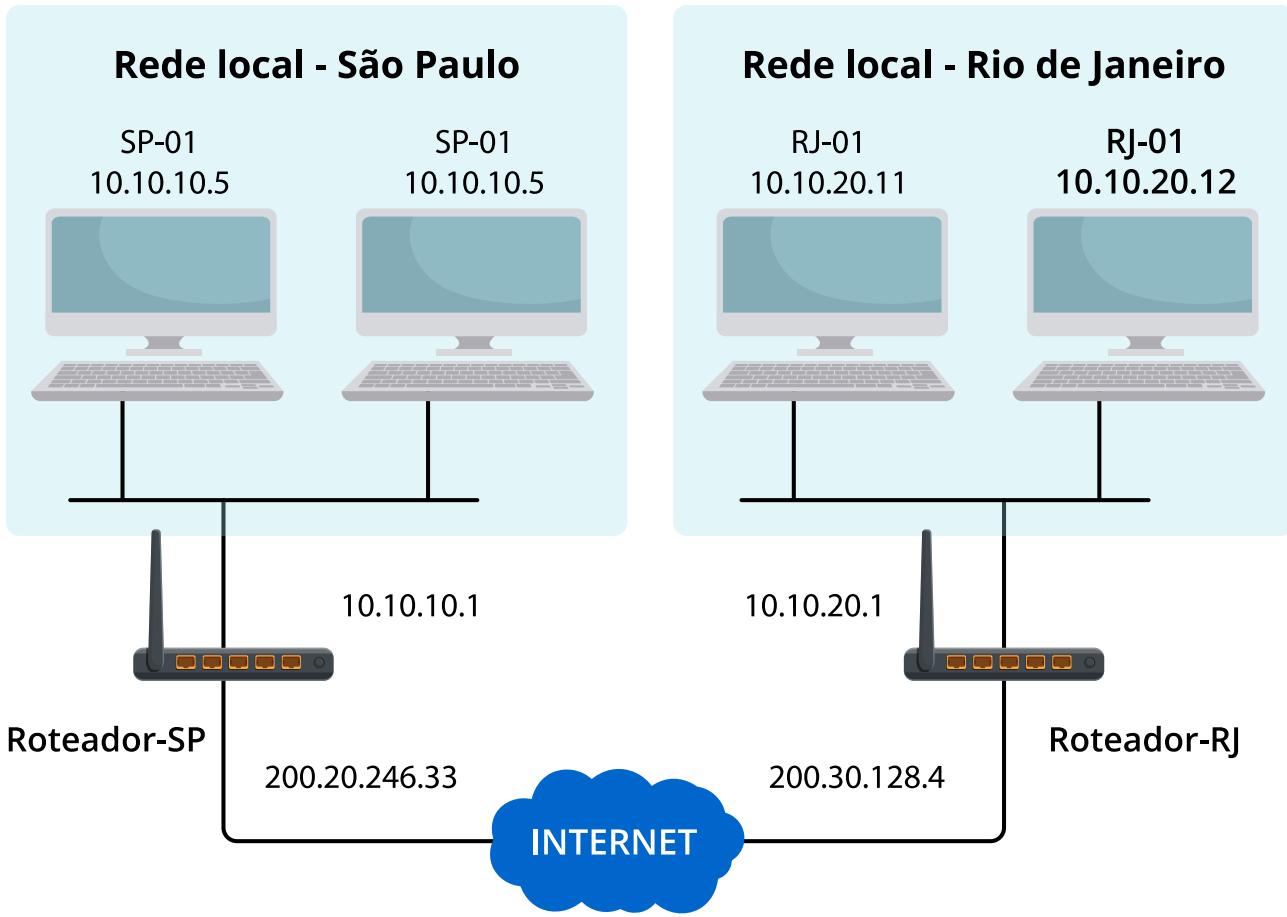
Uma tarefa do roteador é inspecionar cada pacote que lhe foi enviado e determinar se o pacote pertence à rede local IP ou IPX ou a uma rede remota.

Se o destinatário do pacote é uma rede remota e o roteador sabe como chegar àquela rede, o roteador envia o pacote; caso contrário, o pacote é descartado.

Os roteadores também são usados quase que exclusivamente para conectar redes remotas via enlaces de WAN, mas isso não está relacionado à real função de roteamento. É possível usar pontes e outros dispositivos, como PCs, para conectar enlaces de WAN, mas é um procedimento muito raro.

Os roteadores geralmente usam algoritmos e protocolos de roteamento muitos sofisticados para comunicarem-se com outros roteadores a fim de descobrir o melhor caminho para atingir as redes remotas.

O roteador é responsável por encontrar um caminho entre a rede onde está o computador que enviou a mensagem (origem) e a rede onde está o computador que irá receber a mensagem (destino). O roteador pode trabalhar com tabelas de roteamento estático ou dinâmico – sendo que este periférico é o elo de ligação entre uma LAN e uma WAN. O modem também pode ser utilizado dentro da LANs e como “pontes” de ligações entre WANs.



Fonte: acesse o link [Disponível aqui](#)

Roteadores fazem a função de pontes, onde operam na camada de Rede do modelo OSI (camada três), essa camada é produzida não pelos componentes de rede (Endereço MAC das placas de rede, que são valores estáticos), mas sim pelo protocolo muito usado atualmente, o TCP/IP. O protocolo IP é o responsável por criar o conteúdo dessa camada. Isso significa que os roteadores não analisam os quadros físicos que estão sendo transmitidos, mas sim os datagramas produzidos pelo protocolo TCP/IP, os roteadores são capazes de ler e analisar os datagramas IP contidos nos quadros transmitidos pela rede.

O papel principal de um roteador é facilitar um melhor caminho para o datagrama até seu destino. Em redes grandes pode haver mais de um caminho, e o roteador é o elemento responsável por tomar a decisão de qual caminho mais fácil e rápido a percorrer. Ou seja, o roteador é um equipamento de rede cuja função principal é interligar diferentes redes, podendo até interligar redes que tenham arquiteturas diferentes (por exemplo, conectar uma rede Token Ring a uma rede Ethernet, uma rede Ethernet a uma rede x-25).

O que diferencia uma ponte de um roteador é o endereçamento que a ponte utiliza na camada de Link de Dados do modelo OSI, ou seja, o endereçamento MAC nas placas de rede, que é um endereçamento físico. Já roteador, por operar na camada de Rede, usa o sistema de endereçamento dessa camada, que é um endereçamento lógico, nesse caso do TCP/IP, esse endereçamento é o endereço IP.

Nas redes de grande porte, como a Internet, a ponte não consegue identificar os endereços MAC de todas as placas de rede existentes na rede. Quando ponte não identifica um endereço MAC, ela envia o pacote de dados para todas as suas portas. Esse procedimento seria inviável caso os roteadores não existissem, imagine se na Internet cada roteador enviasse para todas as suas portas dados toda vez que ele não soubesse um endereço MAC, a Internet não funcionaria, pelo excesso de dados.

Os roteadores resolveram esse problema pois operam com a leitura dos endereços lógicos, que trabalham em uma estrutura onde o endereço físico não é relevante e a conversão do endereço lógico (Endereço IP) para o endereço físico (endereço MAC) é feita somente quando o data gramma chega à rede de destino.



SAIBA MAIS

*Advanced Research Project Agency (**ARPA**)*, agência norte-americana que surgiu na década de 50 e contribuiu para a criação da rede de longa distância ARPANET em conjunto com universidades conceituadas e centros de pesquisas. Seu objetivo era trabalhar com pesquisas sobre a comunicação e transmissão rápida de dados. Posteriormente seu nome foi alterado para Defense Advanced Research Project Agency (**DARPA**).

[ACESSAR](#)

A grande vantagem de usar endereços lógicos em redes de grande porte é que são mais fáceis de se organizar hierarquicamente, ou seja, pode-se criar um padrão. Mesmo um roteador não sabendo onde esta fisicamente localizada uma máquina destino de um determinado endereço, ele encaminha o pacote de dados para um outro roteador que tenha probabilidade de saber onde esse pacote deve ser entregue (roteador hierarquicamente superior). Esse procedimento continua até o pacote atingir a rede de destino e chegar a máquina de destino. Outra vantagem é que no caso da troca do endereço físico de uma máquina em uma rede, a troca da placa de rede defeituosa não fará com que o endereço lógico dessa máquina seja alterado.

É importante notar, que o papel do roteador é interligar redes diferentes (redes independentes), enquanto que papel dos repetidores, *hub*, pontes e *switches* são de interligar segmentos pertencentes a uma mesma rede.

Protocolos

Os roteadores possuem uma tabela de roteamento, onde listam as redes que eles conhecem. Essa tabela possui uma entrada informando o que fazer quando chegar um datagrama com endereço desconhecido. Essa entrada é conhecida como rota default ou default gateway.

Quando um roteador recebe um datagrama destinado a uma rede conhecida pela sua tabela de roteamento, ele envia esse datagrama a essa rede, pelo caminho por ele traçado e conhecido. Ocorre casos onde ele receba um datagrama destinado a uma rede que ele não conhece o caminho, então o roteador envia o datagrama para o roteador listado como sendo o default gateway. Esse roteador irá encaminhar o datagrama usando o mesmo processo. Caso ele conheça a rede de destino, ele enviará o datagrama diretamente a ela. Caso não conheça, enviará ao roteador listado como seu default gateway. Esse processo continua até o datagrama atingir a sua rede de destino ou o tempo de vida do datagrama ter se excedido o que indica que o datagrama foi descartado no meio do caminho.

Informações de rotas para a envio de pacotes podem ser cadastradas de maneira estática por um administrador da rede ou armazenadas através de processos dinâmicos executando na rede, chamados protocolos de roteamento. O roteamento é o ato de encaminhar pacotes baseando-se em informações da tabela de roteamento. Protocolos de roteamento são protocolos que trocam informações utilizadas para construir tabelas de roteamento.

É importante distinguir a diferença entre protocolos de roteamento (*routing protocols*) e protocolos roteados (*routed protocols*). Protocolo roteado é aquele que fornece informação adequada em seu endereçamento de rede para que seus pacotes sejam roteados, como o TCP/IP e o IPX. Um protocolo de roteamento possui mecanismos para o compartilhamento de informações de rotas entre os dispositivos de roteamento de uma rede, permitindo o roteamento dos pacotes de um protocolo roteado. Note-se que um protocolo de roteamento usa um protocolo roteado para trocar informações entre dispositivos roteadores. Exemplos de protocolos de roteamento são o RIP (com implementações para TCP/IP e IPX) e o EGRP.

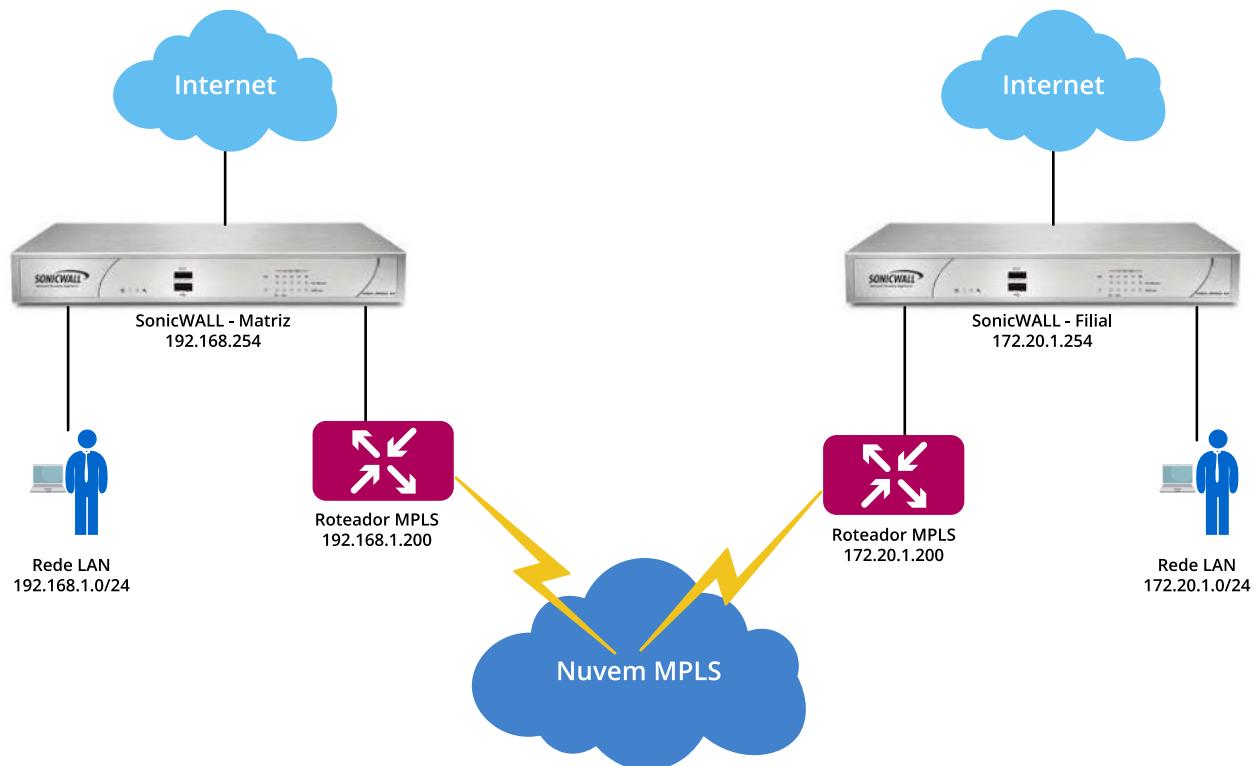
Roteamento estático e roteamento dinâmico

A configuração de roteamento de uma rede específica nem sempre necessita de protocolos de roteamento. Existem situações onde as informações de roteamento não sofrem alterações, por exemplo, quando só existe uma rota possível, o administrador do sistema normalmente monta uma tabela de roteamento estática

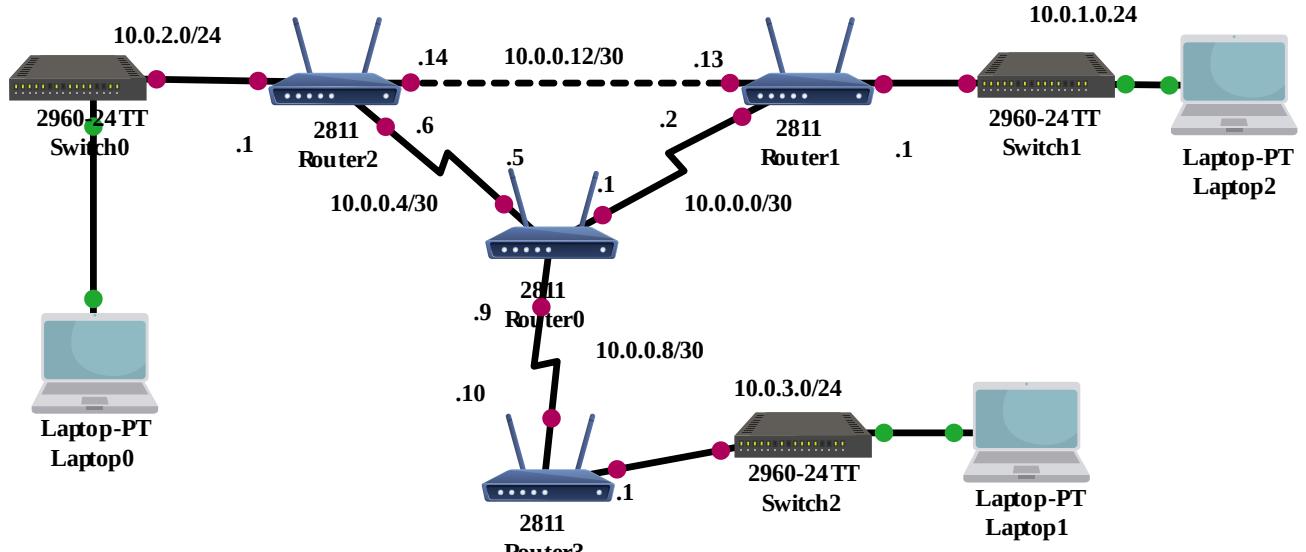
manualmente. Algumas redes não têm acesso a qualquer outra rede e, portanto não necessitam de tabela de roteamento. Dessa forma, as configurações de roteamento mais comuns são:

- **Roteamento estático.**
- **Roteamento dinâmico.**

Demonstração de topologia para roteamento entre unidades - Dell SonicWall



Fonte: acesse o link [Disponível aqui](#)



Fonte: acesse o link [Disponível aqui](#)

A imagem acima nos apresenta o mapa de um pacote de dados transitando pela rede mundial de computadores, onde os pacotes ou datagramas emitidos pelos computadores, recebidos pelo switch e são encaminhados pelos roteadores através do caminho mais curto e menos congestionado da rede.



Conclusão - Unidade 2

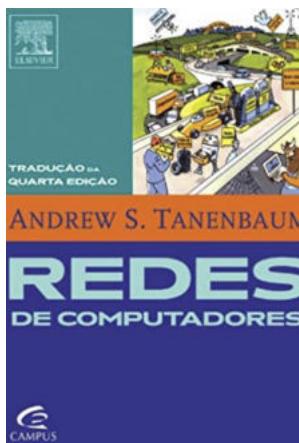
Abordamos nessa unidade sobre os satélites de comunicação, os tipos de satélites, como funcionam na órbita do nosso planeta, as transmissões para canais de televisão e rádios, gerenciamento de gps, dentre outros.

Estudamos também a questão dos custos de um equipamento e a viabilidade de lançamento dos satélites e as manutenções periódicas que se fazem necessários.

Vimos também sobre os equipamentos que compõem as redes de computadores, como *hubs*, *switches* e roteadores, a importância de cada um nas redes, e a eficiência e tecnologia usados nos roteadores no gerenciamento de pacotes de dados na rede mundial de computadores, a *internet*.

Esperamos que tenham apreciado essa unidade e estejam animados para as outras que nos encontraremos logo mais, até breve!!

Material Complementar



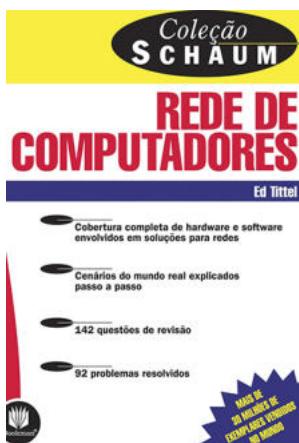
Livro

Redes de Computadores.

Autor: Andrew S. Tanenbaum

Editora: Elsevier

Sinopse: As principais conquistas tecnológicas do século XX se deram no campo da aquisição, do processamento e da distribuição de informações. Entre outros desenvolvimentos, vimos a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria da informática e o lançamento dos satélites de comunicação.



Livro

Redes de Computadores

Autor: Ed Tittel

Editora: Bookman

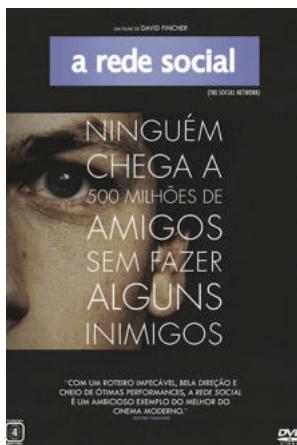
Sinopse: As tecnologias usadas para transferir dados entre computadores envolvem muitas metodologias e componentes diferentes. Uma das principais finalidades da comunicação de dados é permitir que diferentes *hardware*s e sistemas operacionais se comuniquem e se entendam entre si. Para tanto, o meio de transmissão envolvido na comunicação de dados tem que atender a certas especificações de *hardware* e o *software* usado pelo sistema operacional do computador, para ter acesso ao meio de transmissão, precisa estar de acordo com os padrões.



**Livro****Redes de Computadores****Autor:** Gabriel Torres**Editora:** Nova Terra

Sinopse: A obra tem por objetivo ensinar ao leitor, em profundidade, tudo o que precisa saber sobre o tema, seja ele um estudante, um autodidata, um profissional da área ou mesmo um usuário que deseja aprender a montar uma rede segura por conta própria. Seguindo sua marca registrada, o autor utiliza linguagem simples, objetiva e didática.

Em Redes de Computadores – Versão Revisada e Atualizada, os leitores conhecerão as classificações dos diversos tipos de redes, toda a teoria do funcionamento de redes, os protocolos TCP/IP (inclusive o IPv6) em detalhes, as principais arquiteturas de redes locais (com foco em Ethernet e o novo padrão de 10 Gbps) e à distância (X.25, Frame Relay e ATM), tudo sobre as redes Wi-Fi, tutoriais para montar redes caseiras ou comerciais usando o Windows, como montar servidores DNS, web, banco de dados e e-mail (incluindo roteiros detalhados e inúmeras dicas), informações para manter a segurança em dia.

**Filme****A Rede Social****Ano:** 2003

Sinopse: Em uma noite de outono em 2003, Mark Zuckerberg (Jesse Eisenberg), analista de sistemas graduado em Harvard, começa a trabalhar uma nova ideia. Apenas seis anos e 500 milhões de amigos mais tarde, Zuckerberg se torna o mais jovem bilionário da história com o sucesso da rede social Facebook. O sucesso, no entanto, o leva a complicações em sua vida social e profissional. Afinal, ninguém faz 500 milhões de amigos sem fazer alguns inimigos.

Filme ganhador de 4 Globos de Ouro e um dos principais indicados ao Oscar 2011.

Referências

Contribuidores da wiki Wikilivros. Introdução à comunicação entre computadores e tecnologias de rede/Comunicação via satélite. Disponível em: <https://pt.wikibooks.org/wiki/Introdu%C3%A7%C3%A3o_%C3%A0_comunica%C3%A7%C3%A3o_entre_computadores_e_tecnologias_de_rede> Acesso em: 10 de jun. 2019.

COSTA, Wladimir da. **Componentes de uma Rede.** Disponível em: <<https://docplayer.com.br/4248880-Componentes-de-uma-rede-aula-2-prof-wladimir-da-costa.html>> Acesso em: 10 de jun de 2019.

DOIGO, Paulo Steven. **Engenharia eletrônica e telecomunicações.** Disponível em: <<https://www.ebah.com.br/content/ABAAABTK8AI/3288-redes?part=6>> Acesso em: 10/06/2019.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-dow. 6 ed. São Paulo: Pearson Education do Brasil, 2013.

MELO, Alexandre. **Gestão em redes de computadores.** Disponível em: <<https://www.ebah.com.br/content/ABAAAfJQkAB/3288-redes?part=7>> Acesso em: 10/06/2019

PALLETA, Niky. **Curso sistema da informação.** Disponível em: <<https://www.ebah.com.br/content/ABAAABjicAK/apostila-redes-computadores?part=2>> Acesso em: 19/06/2019.

TANENBAUM, Andrew S. **Redes de Computadores.** / Andrew S. Tanenbaum; tradução de Vanderberg D, Souza. - Rio de Janeiro: Elsevier, 2003 - 15ª Reimpressão.

TITTEL, ED; **Redes de Computadores,** Porto Alegre: Bookman, 2003.

TORRES, Gabriel. **Redes de computadores.** 2. Ed. São Paulo: Nova Terra, 2010.



| Unidade 3

Arquitetura de sistemas



AUTORIA
Auro Lima Carvalho

Introdução

Uma das necessidades essenciais de uma rede é a coordenação e o gerenciamento da comunicação entre os diferentes dispositivos. Imagine-se em uma sala com 50 pessoas conversando ao mesmo tempo. Talvez tenha se deparado com essa situação em uma festa ou encontro de pessoas, teria que aumentar seu tom de voz, ou talvez houvesse tanta interferência que seria melhor desistir. Se fizermos uma analogia com redes, não haveria vazão efetiva das informações e ela seria totalmente inútil. Além disso, se dois ou mais pacotes, em uma rede, se encontram no mesmo lugar no meio de transmissão, ocorre uma colisão e a informação é perdida. Uma vez que os sinais viajam a uma velocidade por volta de 70% da velocidade da luz, dois sinais transmitidos no mesmo meio por dois dispositivos diferentes atingirão, ocasionalmente, o mesmo ponto e colidirão. Quando isso acontece, as informações em cada um dos pacotes não terão mais utilidade. Alguma tecnologia se faz necessária para reduzir o número de colisões, ao mesmo tempo em que maximiza o número de mensagens enviadas por segundo sem introduzir atrasos para o dispositivo que estão tentando transmitir. A forma de realizar esses objetivos da comunicação em rede é chamada de problema de múltiplo acesso. Um dos principais papéis da camada de Enlace de Dados da Interconexão de Sistemas Abertos (OSI – *Open Systems Interconnection*) é controlar o acesso ao meio e coordenar as entidades de comunicação para que todos os dispositivos tenham chance de se comunicar.(Tittel – 2003).



Plano de Estudo



Arquitetura de Sistemas Distribuídos.



Aspectos de Projeto e Implementação.

Objetivos de Aprendizagem



Apresentar conceitos sobre as Arquiteturas de Sistemas Distribuídos.



Compreender os tipos de arquiteturas



This is some text inside of a div block.





Arquitetura de Sistemas Distribuídos



AUTORIA
Auro Lima Carvalho

Com a evolução da computação e introdução aos sistemas distribuídos, os fabricantes de computadores voltaram o foco a uma pesquisa insistente com a finalidade de buscar e ampliar mais e mais todo o seu potencial computacional. Aumentando a velocidade procurou fazer uso de computadores de alto nível paralelos. Essas máquinas são montadas com varias CPUs, procurando processar em coletivo, com poder computacional maior do que fosse apenas em uma única CPU. Alocar uma quantidade menor de máquinas em um único local facilita, e o espaço não mais será empecilho se essas máquinas estiverem distribuídas aos quatro cantos do mundo. O que pode se tornar um grande problema é quando esperamos que essas máquinas querem se comunicar com outras máquinas para atuarem juntas na solução de um único problema.

Os sistemas com múltiplos processadores possuem várias CPU's conectadas, atuando em conjunto. Múltiplos processadores são acionados simultaneamente por outros processos diferentes, assim novos problemas de concorrência irão aparecer, esses sistemas podem ser divididos em:

- Fortemente acoplados – processadores compartilham a mesma memória principal.
- Fracamente acoplados – vários processadores/estações interligados acessam a memória local individualmente.

- Sistemas centralizados – Multiprocessador de memória compartilhada onde dois ou mais CPUs compartilham acesso sem limites a uma memória principal. Multiprocessadores de comunicação simples e a sincronização é feita através de técnicas bem definidas e a desvantagem é que são difíceis de construir e por isso tem alto custo.
- Sistemas distribuídos – Multicomputadores, CPUs que não compartilham memória principal, cada CPU tem sua memória individual e é um sistema operacional individualmente gerenciada. Sistemas são conhecidos como cluster – COWS (Cluster os workstations – aglomerados de estações de trabalho).

Qual a finalidade da computação distribuída?

- Com a evolução da tecnologia, computadores de baixo custo, executam o mesmo trabalho que computadores de milhões de dólares executariam.
- O segundo fator é a evolução de redes de alta velocidade.

- Isso resulta na conexão de diversos computadores por meio de uma rede de alta velocidade para operar um sistema de computação colaborativo. Esses sistemas são chamados de sistemas distribuídos.

Surgimento dos sistemas distribuídos

Com o aumento da velocidade e estabilidade das redes de computadores, máquinas de todo o mundo estão cada vez mais interconectados. Nos sistemas distribuídos, computadores remotos trabalham interligados por meio da rede, de maneira que esteja reconhecido como uma única máquina local. As utilizações dos sistemas distribuídos podem ser executadas em máquinas locais e remotas, pois permitem o compartilhar dados, arquivos e demais recursos entre outras máquinas. Os sistemas distribuídos surgem com o intuito de aprimorar a capacidade e a confiabilidade de uma única máquina.

Os sistemas distribuídos se sobrepõem aos sistemas centralizados, pois manipulam atrasos de comunicação e problemas de confiabilidade.

Os grandes desafios da computação distribuída seriam a questão da concorrência, onde os processos disputam os recursos compartilhados, que na maioria das vezes não estão na mesma máquina, inexistência de relógio global onde o gerenciamento dos processos depende de uma ligação entre máquinas, onde o tempo em que as ações dos programas ocorrem, finalmente as falhas independentes – falhas na rede, nos sistemas ou nos processos geralmente não são percebidas nos sistemas distribuídos.

Questões de Projeto

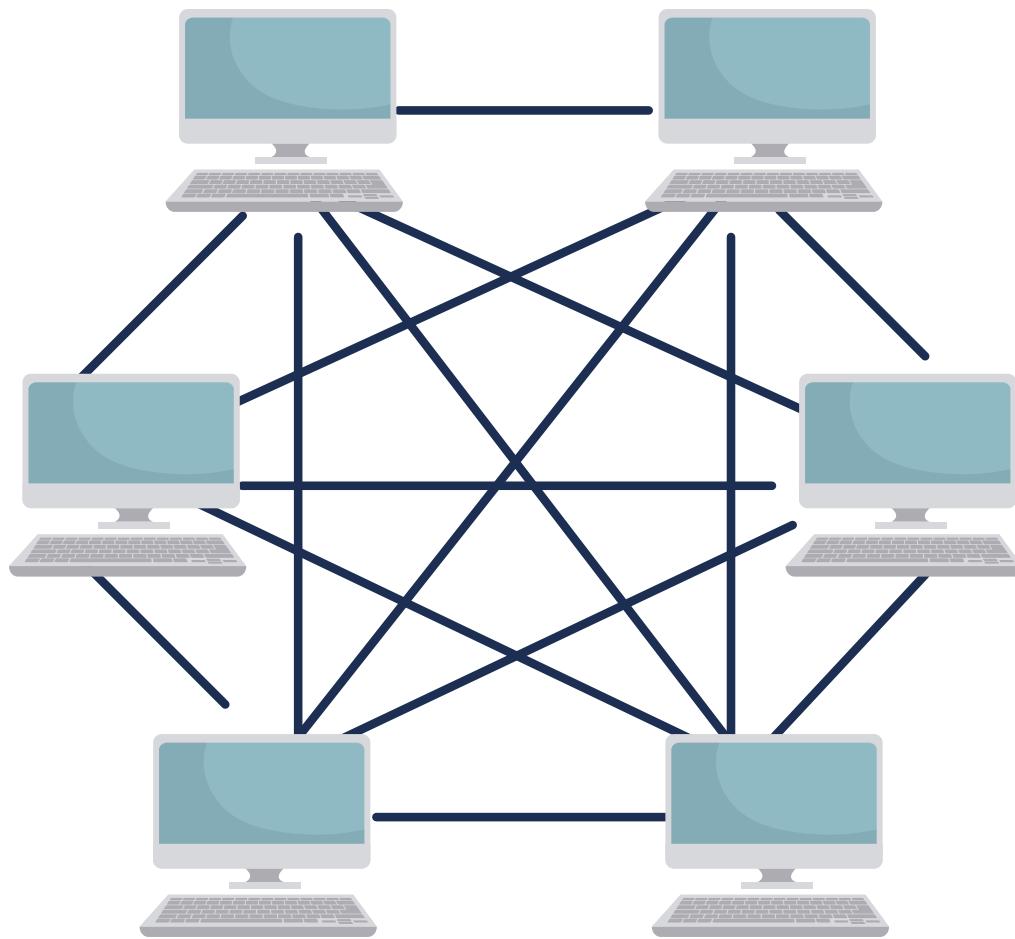
Durante os estágios iniciais de desenvolvimento e implementação das redes, as conexões e comunicações eram ponto a ponto ou malha. Em uma rede ponto a ponto, existe um enlace de transmissão dedicado entre dois dispositivos. Esse tipo de projeto tem várias vantagens. Primeiro, a capacidade e outras propriedades físicas das conexões podem ser diferentes entre cada enlace ponto a ponto.

Como os dois dispositivos nesse tipo de conexão têm acesso exclusivo ao meio, eles podem decidir como e quando transmitir sem a necessidade de negociação ou contenção dentro do meio de transmissão. Os detalhes restantes, como formato, tamanho máximo de pacote e esquema de detecção ou correção de erros, podem ser rapidamente decididos por ambas as partes.

Finalmente, é muito mais fácil ter informações seguras e protegidas em uma rede ponto a ponto do que em uma rede compartilhada. Entretanto, conexões ponto a ponto não são práticas nas redes atuais. Por exemplo, o custo de instalar fisicamente os cabos necessários para conectar um dispositivo a todos os outros com uma linha

dedicada seria enorme. Além disso, existem limites no número de conexões que podem ser feitas em um sistema. Na figura abaixo apresenta os números de cabos e conexões que são necessárias para as redes ponto a ponto de 6(seis) dispositivos.

Figura 1: Cabos e conexões necessárias para as redes ponto a ponto de seis dispositivos



Fonte: acesse o link [Disponível aqui](#)

De modo geral, usam-se as transmissões ponto a ponto para conexões em áreas geograficamente distribuídas (exceto satélite), e conexões de longas distâncias e enlaces ponto a ponto são usados nas LANs. Embora haja vantagens econômicas em compartilhar o mesmo meio em uma LAN, esta não é a melhor para uma rede em segmentos geograficamente distribuídos, ou enlace WAN. Por exemplo, as metodologias usadas para determinar o acesso a um meio compartilhado exigem tempo e largura de banda, o que, em um enlace WAN, pode adicionar atrasos consideráveis e reduzir a largura de banda.

Defeito – erro percebido pelo usuário.

Um defeito ocorre a partir do momento que o sistema não cumpre o que foi projetado e especificado. Caso o sistema distribuído seja projetado para oferecer a seus clientes uma série de serviços, o sistema falha quando um ou vários desses serviços não foram fornecidos por completo.

Tipos de falhas

- Trasientes – acontece uma única vez e a falha não se repete.
- Intermittentes – ocorrem e desaparecem por sua própria vontade. Depois, essas falhas reaparecem e assim por diante. Ex: Um conector com contato frouxo, pode falhar várias vezes.
- Permanentes – Continuarão a existir até que o componente faltoso seja substituído. Ex: Chips queimados, bugs de software.

Modelos de falha

- Falha por queda – Uma vez que o servidor para, nada mais se ouve dele. Também é o caso de um sistema operacional que para de funcionar e para o qual só há uma única solução: reiniciá-lo.
- Falha por omissão – Várias são as possibilidades de erro na falha por omissão. Podemos identificá-la, por exemplo quando uma conexão entre um cliente e servidor foi estabelecida corretamente, mas não havia nenhuma thread ouvindo as requisições que chegavam.
- Falha de temporização – Acontece um atraso ou adiantamento na resposta do servidor que está fora do intervalo de tempo.
- Falhas arbitrárias – Conhecidas também como falhas bizantinas, são as mais sérias. O servidor deve estar produzindo saídas que não deveria ter produzido, e que não são detectadas como erros.
- Falha de resposta – É um tipo sério de falha, que pode ocorrer de 2 maneiras:
- Falha de valor - quando falha um mecanismo de busca que retorna sistematicamente páginas da web não relacionadas com qualquer das palavras de busca utilizadas e falha de transição de estado – quando um servidor recebe uma mensagem que não pode reconhecer. Se não for tomada nenhuma providência para manipular tal mensagem, acontecerá uma falha de transição de estado.

Técnicas de tratamento:

Mascaramento de falha por redundância – Se um sistema deve ser tolerante a falhas, o melhor que ele pode fazer é tentar ocultar de outros processos a ocorrência de falhas. A técnica fundamental para mascarar falhas é a redundância que pode ser de 3 tipos:

- **Redundância de informação** – os bits extras são adicionados para permitir recuperação de bits deteriorados.
- **Redundância de tempo** – uma ação é realizada e, se for preciso, essa ação será executada novamente. Ex: Transações de banco de dados. Se uma transação for abortada ela pode ser refeita sem causar nenhum dano.
- **Redundância física** – são adicionados equipamentos ou processos extras para possibilitar que o sistema como um todo tolere a perda ou o mau funcionamento de alguns componentes. A redundância física pode ser feita em hardware ou em software. Ex: Processos extras podem ser adicionados ao sistema, de modo que se uma pequena quantidade deles cair, o sistema ainda pode funcionar corretamente.

Introdução aos modelos de comunicação e arquitetura cliente/servidor

Os modelos de sistemas distribuídos podem ser classificados como:

- Arquiteturais – Aqueles que definem a forma como os componentes interagem.
- Fundamentais – Aqueles que definem o comportamento e as propriedades dos componentes.

A arquitetura ou organização de um sistema representa sua estrutura em termos de componentes especificados separadamente. A maior preocupação é tornar o sistema:

- confiável
- gerenciável
- adaptável
- rentável

O modelo de arquitetura de um sistema distribuído primeiramente simplifica e abstrai as funções dos componentes individuais desse sistema. Em seguida ele considera o posicionamento dos componentes em uma rede de computadores, buscando definir padrões para a distribuição de dados e da carga de trabalho. Considera também os inter-relacionamentos entre os componentes, isto é, seus papéis funcionais e os padrões de comunicação entre eles.



SAIBA MAIS

Qual é melhor?

Essa é a grande questão atual!

Para uma rede doméstica ou de uma pequena empresa, com poucas máquinas e servidores, a troca ou atualização dos cabos de rede de curta distância pouco impactará em melhorias significativas de velocidade de transmissão.

Em grandes empresas, com fluxo enorme de informações e, sobretudo, com transferências constantes de arquivos entre computadores, a atualização dos cabos proporcionará ganho de velocidade e menos interferência no sinal.

Mas, para que isso funcione bem e com qualidade, seu equipamento roteador e as placas de rede das máquinas também precisam acompanhar o nível e a compatibilidade de atualização para que tudo funcione em harmonia, de maneira eficiente.

ACESSAR

Características dos modelos de arquitetura

Os modelos de arquitetura de um sistema distribuído apresentam estrutura em camadas de software de diferentes níveis de abstração que são: plataforma e middleware.

- Plataforma – Denominação frequente para as camadas de hardware e software de nível mais baixo.
- Middleware – Camada de software que tem como objetivo mascarar a heterogeneidade e fornecer um modelo de programação conveniente para os desenvolvedores de aplicações distribuídas.

Para definir o padrão de distribuição, devemos considerar o posicionamento e a carga de trabalho de cada componente. Além disso, as tarefas devem ser alinhadas de maneira a atender os requisitos de desempenho e confiabilidade.

Os modelos de arquitetura são classificados como:

- Cliente/servidor;
- Peer-to-peer;
- De variações (utiliza-se de serviços oferecidos por diversos servidores).

Requisitos de projeto dos modelos de arquitetura:

- Desempenho – Os principais problemas associados à limitação da capacidade de recursos de processamento e de comunicação são reatividade, *throughput* e balanceamento de carga.
- Qualidade de serviço – As principais propriedades não funcionais dos sistemas que afetam a qualidade dos serviços fornecidos aos clientes são a confiabilidade, segurança, desempenho, adaptabilidade e disponibilidade.
- Replicação – Os problemas de desempenho podem ser solucionados em parte através do uso de replicação de dados.
- Dependabilidade - A dependabilidade pode ser definida como correção, segurança e confiabilidade. Trata-se de um requisito necessário à maior parte dos domínios da aplicação, o que significa que é crucial não apenas nas atividades de comando e controle, mas também em aplicações comerciais.

Modelo cliente/servidor

Como a maioria das redes, a internet utiliza um mecanismo simples: um aplicativo é ligado no primeiro e espera que o outro aplicativo faça contato. O segundo aplicativo precisa conhecer a localização na qual o primeiro aplicativo espera contato. O acordo no qual um aplicativo de rede espera pelo contato de outro é conhecido como paradigma cliente/servidor ou arquitetura cliente/servidor. O programa que espera pelo contato é chamado de servidor e o que inicia o contato é conhecido como cliente. Para iniciar o contato, o cliente precisa saber onde o servidor está rodando e especificar a localização para o software de rede.

Como um cliente especifica a localização de um servidor? Por exemplo na internet, a localização é dada por um par de identificadores: O computador e o aplicativo.

Geralmente os aplicativos desenvolvidos para a internet seguem o mesmo paradigma básico quando se comunicam, dois aplicativos estabelecem comunicação, trocam mensagens e então finalizam a comunicação.

Passos:

- O aplicativo servidor é ativado e aguarda o contato de um cliente.
- O cliente especifica a localização do servidor e solicita estabelecimento de uma conexão.
- Após o estabelecimento de conexão, cliente e servidor estão aptos a trocar mensagens.

Com a conclusão da transmissão, cliente e servidor enviam um fim de arquivo (*end of file*) e a conexão é encerrada.



REFLITA

Quais são as vantagens da internet via rádio?

As vantagens mais significativas da internet via rádio são as seguintes:

Custo/benefício

A principal vantagem na contratação de um plano de internet via rádio é o custo/benefício, se comparado às outras formas de conexão banda larga e de internet móvel. Esse plano tende a oferecer velocidades de conexão razoavelmente boas por valores acessíveis. Assim, usuários domésticos que não dispõem de um grande orçamento podem fazer uso de um serviço de qualidade.

Trata-se de um serviço acessível também para quem não têm condições de contratar serviços de banda larga tradicional.

Qualidade;

Outra vantagem é a qualidade. A internet via rádio pode ter extrema qualidade se a instalação e a configuração são feitas da forma correta. E mais: provedores de internet via rádio têm maior alcance e, geralmente, atendem a áreas periféricas (rurais, por exemplo), que costumam não ser atendidas pelos demais serviços de internet, por falta de interesse ou infraestrutura, por conta dos altos custos para instalar e manter cabos e fibras ópticas.

Simplicidade de implementação e manutenção;

Por utilizar o sinal de rádio e transmiti-lo por meio de torres e antenas, essa conexão também dispensa a instalação de uma linha telefônica, tornando o processo mais simples e menos oneroso.

Na comparação com a internet a cabo, por exemplo, a manutenção da internet via rádio é muito mais simples e barata, uma vez que todos os problemas relacionados ao rompimento de cabos (quando ocorre uma tempestade), por exemplo, são mitigados.

ACESSAR

Características de clientes e servidores

Em geral, a interação cliente/servidor tem as mesmas características. O software cliente é uma aplicação qualquer arbitrária que se torna um cliente temporariamente, quando o acesso remoto for necessário, mas pode executar também outro processamento local. Esse software é diretamente invocado por um usuário e executa somente para uma sessão. Essa execução ocorre localmente no computador pessoal de um usuário. O software cliente inicia ativamente o contato com o servidor, e quando necessário pode acessar múltiplos serviços, mas contata de forma ativa, um servidor remoto de cada vez. O software cliente não exige hardware especial ou sistema operacional sofisticado.

Em contrapartida, o software servidor é um programa privilegiado, de propósito especial, dedicado a fornecer um serviço, mas pode tratar simultaneamente de múltiplos clientes remotos. O software servidor executa em um computador compartilhado e não em um computador pessoal de um usuário, esperando passivamente pelo contato de clientes remotos. Diferentemente do software cliente, o servidor exige hardware poderoso e um sistema operacional sofisticado.

Requisições, respostas e direção do fluxo de dados

A comunicação entre cliente e servidor pode ser realizada em uma ou ambas as direções. Um cliente envia uma requisição para um servidor e este devolve uma resposta para o cliente. Em alguns casos, um cliente envia uma série de requisições e o servidor emite uma série de respostas. Em outros casos, o servidor fornece saída contínua sem qualquer requisição e assim que o cliente contata o servidor, este começa a enviar-lhe dados.

Protocolos de transporte e interação cliente/servidor

Como a maioria dos aplicativos, cliente e servidor usam um protocolo de transporte para comunicarem-se. Como exemplo, podemos citar um cliente e um servidor que usam a pilha do TCP/IP. Um aplicativo cliente ou servidor interage diretamente com um protocolo da camada de transporte para estabelecer uma comunicação e enviar ou receber informações. O protocolo de transporte usa então, os protocolos das camadas mais baixas para enviar e receber mensagens individuais. Desse modo, um computador necessita de uma pilha completa de protocolos pra executar um cliente ou um servidor.

Múltiplos serviços em um computador

Um sistema suficientemente poderoso pode gerenciar a execução de múltiplos clientes e servidores ao mesmo tempo. Pra isso, serão necessárias 2 características

- O computador deve ter recursos de hardware suficientes;
- O computador deve ter um sistema operacional que permita que múltiplos aplicativos executem de modo concorrente. (Ex: UNIX, Linux ou Windows).

*Quando um sistema permite que múltiplos aplicativos estejam ativos ao mesmo tempo, podemos afirmar que esse sistema suporta concorrência. Portanto, um programa que tem mais de um thread de controle é chamado de programa concorrente.



Aspectos de Projeto e Implementação



AUTORIA
Auro Lima Carvalho

A rede global

O arquiteto de redes nos dias atuais enfrenta muitas questões, o que lhe gera um conhecimento muito grande na área. A carga de trabalho que um projetista médio deve enfrentar nos dias atuais são resultados de cinco a dez anos de evolução da tecnologia. No início da década de 1990 não se ouvia falar nesse termo de "arquiteto de redes", pois as redes se limitavam apenas em cliente/servidor e poucos aplicativos a serem compartilhados.

Nos dias atuais as redes estão em mais locais geográficos, inúmeros aplicativos e protocolos. Um projetista de rede deve estar preparado para acumular funções necessárias, gerir segurança, analisar suporte técnico, analista financeiro, etc.,

Todos os projetos atuais de redes precisam ser voltados para a "redes globais", ter potencial para serem acessadas em qualquer canto do planeta, seja no escritório doméstico ou em uma rede de escritórios de grandes corporações, ter potencial para ser global.

Definição do Projeto

Uma grande parte dos projetos de arquiteturas de redes esbarra em duas categorias: substituição ou expansão. Muitas empresas que naturalmente passam pela fase de crescimento e ampliação optam pelo projeto de expansão logo contratam um profissional para elaboração e execução dessa nova ampliação da rede. Já a substituição é apenas onde o cliente manterá atual redes sem ampliação, apenas substituição de equipamentos mais rápidos e modernos, cabeamento atualizado, etc.

Uma outra questão de muita importância deve ser levado em consideração, na implantação de uma rede de comunicação é a sua facilidade de manuseio e manutenção, tanto para operadores da rede quanto para quem irá administrar. A rede deve ter disponível um conjunto elementar de componentes e ferramentas aptos a oferecer os serviços necessários a seus usuários, mas também facilidades para viabilizar a adição de novos equipamentos e a manutenção do sistema por seus administradores.

Recomenda-se dividir o projeto de implementação em duas partes básicas: parte física e parte lógica:

- **Topologia Física** – Esse projeto é composto pelo cabeamento, dispositivos de rede dentre outros elementos do hardware. Ela determina a forma como a rede será organizada;
- **Topologia Lógica** – (rede lógica) permite que as partes físicas atuem em conjunto. A rede lógica é o conjunto de recursos que os usuários acessam ao utilizar a rede, como espaço disponível e usado em disco rígido, impressoras

aos quais o computador tem acesso quando conectado em rede e aplicativos liberados, etc.

Metodologia de projeto

A metodologia utilizada em um projeto, resume em um plano para administrar e gerir qualquer modelo de projeto, normalmente dividida em três partes: especificação do escopo (objetivos do projeto), especificação das atividades executadas (aplicações dos usuários) e as especificações de como as demais partes envolvidas deverão interagir entre si.

Diferente do planejamento específico solicitado por um outro projeto, por exemplo, especificações e ações para instalação de rede elétrica residencial ou predial, a metodologia aplicada seria plano genérico que pode ser usado nos mais variados tipo de projeto. Logo, o planejamento próprio de um determinado projeto nada mais é do que uma subdivisão da metodologia de projeto adotada.

A aplicação da metodologia deverá se estruturar com o intuito de incluir um projeto lógico antes mesmo de projetar um projeto físico e ter um levantamento dos requisitos dos usuários do sistema previamente antes de levar em consideração outras variáveis. Novas informações devem entrar progressivamente no projeto, ser interativa, à medida que o projeto evolui, mais se conhece melhor os requerimentos dos usuários, a fim de atualizar desvios e prováveis falhas.

Um projeto metodologia voltado na melhoria de uma rede de computadores já existente, deve dividir o processo de planejamento quatro fases distintas:

- Projeto informacional - levantamento aos usuários das informações sobre os problemas que existe na atual rede e a criação das especificações para a nova rede;
- Projeto conceitual - nessa etapa, cria-se a concepção para a nova rede que corresponda da melhor maneira às necessidades dos usuários, mas que não prejudique o funcionamento do sistema em uso;
- Projeto preliminar - desenvolvimento da criação lógica e física da nova rede, que atenda os critérios técnicos e econômicos estabelecidos nas fases anteriores;
- Projeto detalhado - finalização do projeto, fase onde a disposição, e a forma, as dimensões e as tolerâncias de todos os componentes da nova rede são fixadas. Nessa fase apresenta-se a efetiva execução e funcionamento do projeto, criação do protótipo, testes e aceitação da nova rede.



Conclusão - Unidade 3

Nessa terceira unidade falamos sobre a importância do gerenciamento da comunicação entre dispositivos, ainda sobre tráfego de dados e a questão da colisão entre eles que pode ocorrer a perda de pacotes nessa ação. Tecnologias existem para amenizar essas colisões entre pacotes na rede, maximizando a quantidade de mensagens envidas por segundo sem atrasos e tendo sucesso na entrega no destino.

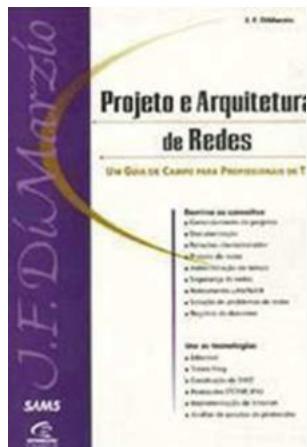
Abordamos também sobre os mais diversos tipos de arquiteturas em redes, sobre custos dessas arquiteturas, redes de alta velocidades, chamados sistemas distribuídos. Falamos sobre a evolução do processamento até os dias atuais.

Foi levantado nesta unidade também questões sobre implementação de projetos de redes, onde as comunicações eram ponto a ponto, suas vantagens e desvantagens. Falhas em sistemas distribuídos, tipos de falhas e técnicas de tratamento dessas falhas, questões de segurança, etc.

Na segunda parte da nossa unidade, abordamos sobre os aspectos de implementação, onde o objetivo básico de uma rede de comunicação é garantir que todos os recursos sejam compartilhados com rapidez, segurança e de forma mais confiável possível. Os projetos devem seguir rígidas regras de metodologias e padrões e metas estabelecidas pela equipe do projeto.

Esperamos que tenham gostado dessa unidade e continuem entusiasmados para o nosso próximo e último assunto da disciplina, bons estudos.

Material Complementar



Livro

Projeto e Arquitetura de Redes

Autor: DiMarzio J. F.

Editora: Elsevier editora.

Sinopse: As tecnologias usadas para transferir dados entre computadores envolvem muitas metodologias e componentes diferentes. Uma das principais finalidades da comunicação de dados é permitir que diferentes hardware e sistemas operacionais se comuniquem e se entendam entre

si. Para tanto, o meio de transmissão envolvido na comunicação de dados tem que atender a certas especificações de *hardware* e o *software* usado pelo sistema operacional do computador, para ter acesso ao meio de transmissão, precisa estar de acordo com os padrões.



Livro

Projetos e Implementação de REDES

Autor: Lindeberg Barros de Sousa

Editora: Érica; Edição: 1^a (8 de abril de 2013)

Sinopse: O livro aborda fundamentos básicos de comunicação, planejamento e elaboração de projetos e arquiteturas de redes de computadores. Apresenta conceitos de redes de comunicação, princípios de telecomunicações, configuração de equipamentos e a arquitetura TCP/IP. Explica o funcionamento de redes Windows, LAN, WAN e a montagem de um plano de endereçamento, destaca ISDN (Integrated Services Digital Network), a estrutura de redes Frame-Relay, além de redes públicas e digitais. Descreve, ainda, segurança e gerenciamento de redes, englobando VPNs (Virtual Private Network) e firewalls. Na terceira edição, revisada, alguns textos e figuras foram atualizados, incluindo novos fundamentos, como o MPLS (Multiprotocol Label Switching).

Referências

DIMARZIO, J. F. **Projeto e arquitetura de redes: um guia de campo para profissionais de TI / J.F. DiMarzio: tradução de Vanderberg D. Souza.** - Rio de Janeiro: Elsevier, 2001 - 3º reimpressão.

GIL, Mauro Cesar Cantarino. **Arquitetura de Sistemas Distribuídos.** Disponível em: <https://www.passeidireto.com/arquivo/6517119/resumo-arquitetura-de-sistemas-distribuidos>. Acesso em 16/06/2019.

PINHEIRO, José Maurício. **Considerações para projetos de redes.** Disponível em: <https://www.ispblog.com.br/2018/07/13/consideracoes-para-projetos-de-redes/>. Acesso em 17/06/2019.

PINHEIRO, José Maurício. **Interconexão de Redes - Uma visão de projeto.** Disponível em: https://www.projetoderedes.com.br/artigos/artigo_interconexao_de_redes_uma_visao_de_projeto.php. Acesso em 16/06/2019.

TANENBAUM, Andrew S. **Redes de Computadores.** / Andrew S. Tanenbaum; **tradução de Vanderberg D. Souza.** - Rio de Janeiro: Elsevier, 2003 - 15^a Reimpressão.



Centro Universitário Cidade Verde

| Unidade 4

Sistemas e segurança



AUTORIA

Auro Lima Carvalho

Introdução

A informação é a base de tudo, é com base nelas que conseguimos tomar nossas decisões. Por ser tão importante, perder uma informação pode custar muito para uma organização. Sendo assim, com o passar dos anos, as organizações vem investindo na tecnologia da informação, com o intuito de proteger, compartilhar e torná-la disponível, sempre considerando o fator custo x benefício. Não adianta ter informação, se ela não estiver disponível 24 horas por dia, pois nunca sabemos quando ela será necessária. Por isso as organizações passaram a investir mais em novas tecnologias que possibilitem além da segurança, a disponibilidade, pois elas são a matéria prima de muitas empresas.

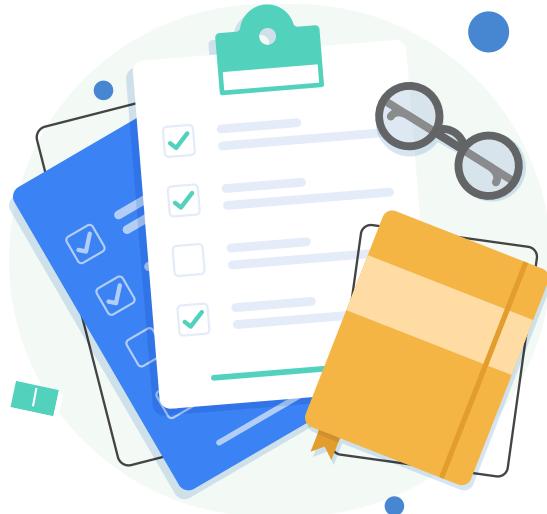
A cada dia, surgem novas tecnologias, e fica difícil para as organizações definirem qual é a mais adequada para suas necessidades, levando em consideração, que tais necessidades podem mudar com o passar do tempo, assim como a estrutura da organização, ou até mesmo o segmento, além de suprir as necessidades da organização, a tecnologia deve ser flexível. O compartilhamento de informações se mostra um assunto muito amplo, pois, diversos fatores, sejam eles internos ou externos, influenciam no meio em que a informação deve ser compartilhada.

No cenário atual, possuímos basicamente duas formas de compartilhar a informação:

- a) Compartilhamento por meio físico;
- b) Compartilhamento em nuvem.

Ambos os modos de compartilhamento citados acima, possuem suas vantagens e desvantagens. Com tanta opção de tecnologia no mercado, fica difícil para o usuário escolher qual lhe suprirá suas necessidades de forma simples e eficiente. Demonstraremos através dessa unidade, as principais diferenças, vantagens e desvantagens entre o sistema de arquivos distribuído físico e o sistema de arquivos em nuvem.

Na segunda parte da nossa unidade, trataremos da segurança, onde o termo nos traz à memória todos os itens e assuntos que e refere à proteção dos dados e à prevenção de acessos indesejáveis. Além disso, não existe uma única definição para o termo *segurança de rede*. O que é importante são os itens e os recursos que uma organização ou uma empresa julgam importante manter protegidos, para que suas operações tenham sucesso. Cada rede, empresa e organização precisam ser consideradas caso a caso. Só depois que todos os dados tiverem sido coletados de acordo com a importância desses itens e/ou serviços é que uma política de segurança pode ser desenvolvida e implementada.



Plano de Estudo



Sistemas de arquivos distribuídos.



Segurança.

Objetivos de Aprendizagem



Conhecer os principais sistemas de arquivos distribuídos.



Abordar assuntos sobre requisitos de segurança em sistemas de informação.





Sistema Distribuído



AUTORIA
Auro Lima Carvalho

Segundo Coulouris, Dollimore e Kindberg (2007), um sistema distribuído é formado por um conjunto de software e hardware, localizados em computadores distintos que estão interligados através de uma rede. Esses computadores não precisam necessariamente estar no mesmo meio físico, em certos casos, os computadores que fazem parte do mesmo sistema distribuído podem estar em continentes diferentes.

De acordo com Tanenbaum e Steen (2007), apesar do sistema distribuído ser na maioria das vezes, composto por vários computadores, ele aparece para o usuário como um único sistema. Uma particularidade interessante é que as diferenças entre os computadores e a maneira como eles se comunicam estão ocultas ao usuário e da mesma maneira ocorre com a organização interna do sistema distribuído.

Para Coulouris, Dollimore e Kindberg (2007), um sistema de arquivos distribuído permite que os programas armazenem e acessem arquivos a partir de qualquer computador em uma rede, permitindo assim que o armazenamento ocorra em servidores reduzindo a necessidade de armazenamento no disco local e facilitando o backup dos dados importantes de uma organização.

Com base nos autores, pode-se concluir a definição de sistema distribuído, levando em conta certas consequências descritas a seguir:

- a) Concorrência: Em uma rede de computadores, a execução concorrente de programas sempre existirá. A capacidade do sistema de manipular recursos compartilhados pode ser ampliada sempre que necessário, precisa-se apenas adicionar a rede novos recursos.
- b) Inexistência de relógio global: a coordenação de programa que cooperam entre si é feita através da troca de mensagens. Todavia, existem limites para precisão na qual os computadores podem sincronizar seus relógios em uma rede – não existindo uma noção única do tempo correto, tornando-se assim, uma consequência direta do fato que a única comunicação se dá pelo envio de mensagens em rede.
- c) Falhas independentes: todos os sistemas estão suscetíveis a falhas. Nos sistemas distribuídos, a falha de um computador ou a falha na rede, não resulta em um travamento total do sistema, cada componente do sistema pode falhar independentemente, deixando os outros ainda em funcionamento.

O principal motivo de se construir um sistema distribuído é o fato do mesmo proporcionar de forma simples e eficaz o compartilhamento de recursos. Podemos caracterizar como recursos tudo aquilo que está dentro da rede, isto é, desde os componentes de software e hardware até os dados inseridos pelos usuários.

Metas

De acordo com Tanenbaum e Steen (2007), o fato de se poder montar um sistema distribuído, não significa que em todos os casos, ele será a opção ideal para suprir suas necessidades. Um sistema distribuído deve oferecer fácil acesso a seus recursos, deve ocultar o fato de que seus recursos são distribuídos por uma rede e deve ser flexível.

Acesso a recursos

Para Tanenbaum e Steen (2007), conectar os usuários aos recursos facilita a colaboração de troca de informações, por isso a principal meta de um sistema distribuído deve ser facilitar aos usuários o acesso a recursos remoto e seu compartilhamento de maneira controlada e eficiente. Dentre os vários motivos para justificar o compartilhamento de recursos, podemos citar como principal a economia.

Por exemplo, em uma empresa de pequeno porte, que possui uma ampla sala com diversos computadores, é mais fácil comprar uma impressora e compartilhá-la com todos os computadores (que serão acessados pelos usuários) do que comprar uma impressora para cada computador.

Transparência na distribuição

Segundo Tanenbaum e Steen (2007), uma meta importante do sistema distribuído, é ocultar o fato de que os processos e recursos estão sendo distribuídos por computadores distintos. A capacidade de um sistema distribuído apresentar suas aplicações como se fosse um único sistema é denominado transparente.

De acordo com os autores, os aspectos mais importantes de transparência em um sistema distribuído que devem ser levados em consideração são:

- a) Transparência de Acesso: oculta a diferença na representação de dados e no modo de acesso a um recurso.
- b) Localização: oculta o local em que um recurso está localizado, isto é, o usuário não sabe qual a localização física de um recurso no sistema.
- c) Migração: oculta que um recurso pode ser movido para outro local sem afetar seu modo de acesso;
- d) Realocação: oculta que um recurso pode ser movido para outro local, mesmo quando está em uso;
- e) Replicação: oculta que recursos são replicados. A replicação é feita em locais que estão próximos do verdadeiro arquivo e com o mesmo nome do arquivo original;
- f) Concorrência: oculta que um recurso pode ser compartilhado por usuários concorrentes;
- g) Falha: oculta a falha e a recuperação de recursos. Apesar da transparência de distribuição ser indicada para qualquer sistema distribuído, há situações em que ocultar completamente dos usuários todos os aspectos da distribuição não é uma boa ideia.



SAIBA MAIS

Jornalista desafia Hackers e correu Mal

O jornalista Kevin Roose, da estação televisiva Fusion, decidiu desafiar alguns hackers da DEFCON (maior convenção hacker do mundo) para que estes tentassem invadir a sua vida privada online. O resultado foi assustador, para além de perder o acesso às suas contas (de email e bancárias), os hackers deram-se ao "luxo" de tirar fotografias com a webcam e "prints" de tela sem o seu consentimento.

O que muitos poderiam considerar “masoquismo”, é na verdade uma excelente matéria para avaliar quão vulneráveis podemos estar, e o que pode ser feito para melhorar a nossa segurança na Internet.

Acesso aos dados pessoais

A primeira técnica usada foi bastante surpreendente. Usando apenas "engenharia social" os hackers foram capazes de obter acesso ao email do jornalista, ligando para a linha de apoio da empresa telefónica. Fazendo-se passar pela mulher e colocando um vídeo de uma criança a chorar (do YouTube), a "hacker" foi capaz de "expulsar" o jornalista da sua própria conta de email.

Outra técnica usada pelos hackers foi o "Phishing". Esta técnica já se encontra bem documentada, na prática, os hackers enviam um email à vítima, fingindo ser uma entidade credível (por exemplo, um banco), solicitando informação sensível, como os dados pessoais ou senha.

ACESSAR

Ciladas

De acordo com Tanenbaum e Steen (2007), existem N fatores que devem ser levados em consideração ao se desenvolver um sistema distribuído, devido a isso, Peter Deutsch, que trabalhava na Sun Microsystems, formulou uma lista de falsas premissas que todos adotam ao desenvolver um sistema distribuído:

- a) A rede é confiável;
- b) A rede é segura;
- c) A rede é homogênea;
- d) A topologia não muda;
- e) A latência é zero;
- f) A largura da banda é infinita;
- g) O custo de transporte é zero;
- h) Há só um administrador.

Heterogeneidade

Segundo Coulouris, Dollimore e Kindberg (2007), tanto a rede quanto os computadores que fazem parte dela são sistema heterogêneo. Tais aspectos se aplicam a heterogeneidade:

- a) Redes;
- b) Hardware de computador;
- c) Linguagens de programação;
- d) Implementações de diferentes desenvolvedores;

Para os autores, programas escritos por diferentes desenvolvedores não podem se comunicar, a não ser que utilizem padrões comuns, por exemplo, para realizar a comunicação via rede e usar uma mesma rede, tais padrões devem ser estabelecidos.

Sistema abertos

De acordo com Coulouris, Dollimore e Kindberg (2007), um sistema aberto é aquele que pode ser estendido e reimplementado de várias maneiras, tanto a parte de software quanto a de hardware. O que determina se um sistema distribuído é aberto ou não, é dado principalmente pelo grau com que novos serviços podem ser adicionados e disponibilizados para uso por uma variedade de programas e usuários. Segundo os autores, a característica de um sistema aberto é obtida a partir do momento que suas principais interfaces são publicadas.

Esse processo é semelhante àquele realizado por organizações de padronizações, porém este ignora os procedimentos oficiais, que em sua maioria são pesados e lentos. Para os autores, os projetistas dos protocolos Internet elaboram uma série de documentos, denominado Requests For Comments (RFCs), onde cada um era identificado por um número. Porém RFCs não são os únicos meios de publicação. Sistemas projetados de acordo com tais padrões são denominados sistemas distribuídos abertos.

Segurança

De acordo com Coulouris, Dollimore e Kindberg (2007), o firewall não garante o uso dos recursos dentro da internet, nem o uso apropriado da mesma. Dois usuários trocam informações sigilosas utilizando uma rede. A segurança não é apenas a questão de ocultar o conteúdo da informação, mas também garantir que seja identificado o agente ou usuário de cada mensagem, e garantir que tal identificação esteja correta.

Escalabilidade

De acordo com Neuman (1994, apud TANENBAUN; STEEN 2007), no mínimo três dimensões diferentes devem ser consideradas ao medir a escalabilidade de um sistema. Em primeiro lugar, se o sistema é escalável em relação a seu tamanho, isto é, se é fácil adicionar mais usuários e recursos ao sistema. Em segundo lugar, o sistema escalável em termos geográfico é o sistema que permite que usuários e recursos estejam longe uns dos outros. Em terceiro lugar, o sistema pode ser escalável em termos administrativo, garantindo assim o fácil gerenciamento independente da dimensão e heterogeneidade do sistema.

Um sistema distribuído escalável é aquele que permanece eficiente quando há um aumento significativo no número de recursos e no número dos usuários, completa Coulouris, Dollimore e Kindberg (2007). Um sistema distribuído escalável apresenta os seguintes desafios:

- a) Controlar o custo dos recursos físicos;
- b) Controlar a perda de desempenho;
- c) Impedir que os recursos de software se esgotem;
- d) Evitar gargalos de desempenho;

Computação em Nuvem

Segundo Veras (2012) computação em nuvem foi desenvolvido com a finalidade de oferecer serviços de baixo custo, fácil acesso e garantir características tais como disponibilidade e escalabilidade. Ela garante uma maneira eficaz de potencializar e flexibilizar os recursos computacionais, sendo assim um ambiente redundante que é capaz de continuar a funcionar corretamente com o mau funcionamento de um ou mais componentes, completa Taurion (2009).

São as características essenciais que, quando agrupados, diferem a computação em nuvem dos demais sistemas. Self-service sob demanda segundo Mell e Grance (2011), onde o usuário pode unilateralmente prever a capacidade computacional, como o desempenho do servidor ou seu armazenamento, sem a necessidade de interação humana, os recursos estão disponíveis através da rede e são acessados por meio de mecanismos padrão que promovem o uso de plataformas de cliente, seja ele moderado ou demasiado (por exemplo, celulares, laptops e estações de trabalho).

Conforme Mell e Grance (2011) recursos de computação do provedor estão reunidos para servir a múltiplos usuários, com diferentes recursos físicos e virtuais atribuídos e realocados dinamicamente de acordo com a demanda. O usuário geralmente não tem controle ou conhecimento sobre a localização exata dos recursos disponibilizados.

Mell e Grance (2011) explica que recursos podem ser elasticamente provisionados e liberados, em certos casos, automaticamente, para escalar de maneira mais eficiente conforme a demanda. Sistemas em nuvem controlam e otimizam o uso dos recursos, como por exemplo a capacidade de processamento, utilização da memória, armazenamento e etc. O uso dos recursos pode ser monitorado, controlado e relatado, proporcionando transparência para o provedor e consumidor do serviço utilizado.

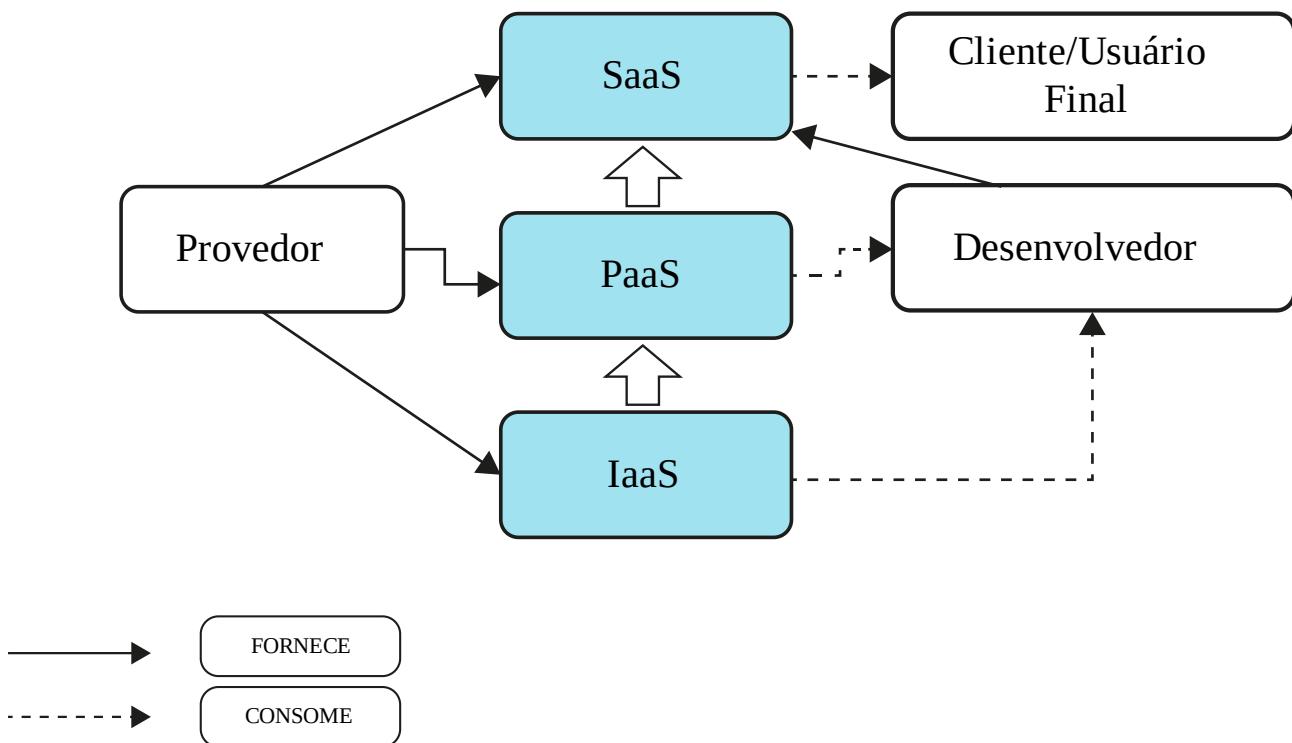
Modelos de Serviços

Segundo Veras (2012), existem três principais modelos de serviços para *Cloud Computing*, descritas a seguir:

- Infraestrutura como um serviço (Infrastructure as a Service - IaaS): o usuário não possui o controle na unidade física, contudo, através de mecanismos de virtualização, possui controle sobre armazenamento, máquinas virtuais, aplicativos instalados e um controle limitado dos recursos de rede. Um exemplo de IaaS é o serviço E2C, oferecido pela Amazon.
- Plataforma como um serviço (Platform as a Service - PaaS): é aquela que suporta à instalação e execução de aplicativos na nuvem. Exemplos de PaaS são a AppEngine do Google e o Windows Azure da Microsoft.
- Software como um serviço (Software as a Service - SaaS): é viável para um grande número de clientes que passam a ser hospedados na nuvem, os aplicativos são oferecidos como serviços e todo o controle e gerenciamento da rede, sistemas operacionais, servidores e armazenamento é feito pelo provedor de serviço. Como exemplos de SaaS podemos citar o Google Apps e SalesForce.com.

Segundo Veras (2012), a Figura menciona os papéis desempenhados na arquitetura baseada em nuvem e destaca quem fornece serviço e quem consome. O modelo IaaS suporta o PaaS, que suporta o modelo SaaS.

Figura 1: Papéis em Cloud Computing



Fonte: (Veras 2012).

De acordo com Veras (2012), o provedor de serviços considerado ideal é aquele responsável por disponibilizar e gerenciar toda estrutura de Cloud Computing, fazendo com que os usuários finais, não tenham preocupações com esse tipo de problema. Para isso o provedor fornece o serviço dentre uma das três modalidades. O desenvolvedor utiliza os recursos para gerar serviços para o usuário final, que por sua vez, paga a conta.

Modelos de implementação

Segundo Veras (2012), existem quatro principais modelos de implantação de *Cloud Computing*, descritos abaixo:

- a) Nuvem Privada (*Private Cloud*): é aquela que quase sempre é operada e gerenciada pela organização cliente. Os serviços são utilizados apenas pela organização, isto é, não estão publicamente disponíveis. Em alguns casos pode ser gerenciado por terceiros. As nuvens privadas são basicamente subdivididas em:
 - Nuvem privada, hospedada pela empresa. Aconselha-se este modelo quando os aspectos fortes em regulamentação e controle precisam ser considerados
 - Nuvem privada, hospedada em provedor de serviço. Aconselha-se este modelo para aplicações de forma geral e aplicações de missão crítica.
- b) Nuvem Pública (*Public Cloud*): é oferecida de modo pague-por-uso, é utilizada em organizações públicas ou por grandes corporações onde é necessária ampla capacidade de processamento e armazenamento.
- c) Nuvem Comunitária (*Community Cloud*): esta nuvem é compartilhada por várias organizações com interesses em comum. A nuvem comunitária pode ser gerenciada tanto pelas organizações que fazem parte da comunidade ou por terceiros.
- d) Nuvem Híbrida (*Hybrid Cloud*): é composta por duas ou mais nuvens, dentre os tipos citados anteriormente, que continuam a ser entidades únicas, porém, conectadas de uma nuvem computacional.

Comparativo entre sistema e nuvem e sistema local

Pontos positivos

O sistema em nuvem possui maior flexibilidade e escalabilidade em relação ao tradicional (físico). Traz maior economia de energia, visto que os serviços estarão hospedados em servidores fora da empresa. O custo com colaboradores também diminui, já que a infraestrutura estará hospedada em um fornecedor especializado que na maioria das vezes fica responsável pelo suporte ao mesmo.

Suas atualizações são automáticas, de forma geral, as mais pesadas são semanais e existe uma automanutenção diária. O backup, quando feito em nuvem dispensa disco ou qualquer outra forma de armazenamento físico por parte da empresa. Quando a demanda de serviço é menor, o serviço em nuvem é uma excelente opção, já que na maioria das vezes, alocar ou comprar um servidor acaba ficando mais caro, pois nem sempre se encontram servidores com configurações que são compatíveis com a necessidade do cliente, por tanto, o cliente acaba não fazendo uso total do desempenho da máquina ou o desempenho de algum dispositivo da mesma não supri sua necessidade. Por exemplo, o cliente adquire um servidor muito eficiente em questão de processamento, porém deixa a desejar no quesito armazenamento ou o servidor possui alto desempenho em todos os pontos, porém o cliente necessita apenas do espaço em disco mais robusto.

Pontos negativos

Uma questão de grande importância para o cliente é a segurança, e uma questão que sempre se levanta é o fato de que as informações do contratante estão armazenadas em um local desconhecido onde a segurança do mesmo não pode ser totalmente gerenciada pelo cliente, em certos casos. A velocidade da internet é outro fator importante, já que o acesso sempre será feito de forma externa, gerando assim quantidade de tráfego de dados extremamente alta, que por consequência gera um custo excessivo para o contratante da *cloud computing*, pois a internet no Brasil além de não ter a mesma qualidade de países desenvolvidos possui um preço exorbitante.

Conclusão sobre Computação em nuvens

Com base nos autores e nas ferramentas estudadas, pode-se concluir que os serviços e servidores em nuvem estão crescendo constantemente graças a seu sistema flexível e de alta disponibilidade. Uma barreira que precisa ser vencida é a da segurança, já que as informações ou serviços específicos é a matéria prima de muitas empresas, o fato de estarem sob a responsabilidade de terceiros ainda não é uma situação aceitável para muitos, e por causa desse e outros fatores, acabam optando pela estrutura tradicional, isto é, estrutura física.

Disponibilidade, flexibilidade e escalabilidade são diferenciais que vem sendo cada vez mais requisitados pelo cliente na hora de implementar um serviço. Tais conceitos são à base da computação em nuvem e é isso que a faz tão superior quando comparada as estruturas físicas.



Segurança



AUTORIA
Auro Lima Carvalho

O termo segurança traz a memória todos os tipos de itens e assuntos que se referem a proteção dos dados e à prevenção de acessos indesejáveis. Além disso, não existe uma única definição para o termo *segurança de rede*. O que é importante são os itens e os recursos que uma organização ou uma empresa julgam importante manter protegidos, para que suas operações tenham sucesso.

Cada rede, empresa e organização precisam ser consideradas caso a caso. Só depois que todos os dados tiverem sido coletados de acordo com a importância desses itens e/ou serviços é que uma política de segurança pode ser desenvolvida e implementada. As políticas de segurança não aparecem de forma genérica. Uma vez determinada as necessidades, uma organização pode começar a construir políticas de segurança modeladas de acordo com as implementações existentes, mas as políticas precisarão ser melhoradas e modificadas para se adequarem às especificidades da organização. TITTEL(2003).

Outro aspecto de segurança das redes e dos sistemas envolve o planejamento para eventuais cortes prolongados de energia ou perda de instalações físicas como resultado de um incêndio. Nesses tipos de situações, os dispositivos físicos, os computadores e os softwares podem ser destruídos, de modo que necessário existirem procedimentos para recuperação após o desastre.

De acordo com a Gartner Research, divisão da Gartner Inc., que produz análises sobre assuntos comerciais e tecnológicos, sobre tendências e acontecimentos da atualidade, duas entre cinco empresas que passaram por um desastre fecham suas atividades em cinco anos. As empresas podem melhorar as estatísticas - mas só se elas tomarem as precauções necessárias antes e depois do desastre. (TITTEL, 2003).

É demais importante para o estudo da Segurança da Informação a distinção entre dados e informação:

- Dados nada mais é que o conjunto de informações organizadas, geralmente resultando na experiência de outras informações dentro de um conjunto de armazenamentos. Os dados podem se apresentar em números, imagens e palavras, ou seja, informações ainda não tratadas, com pouco significado.
- Informação é o resultado do processamento, manipulação e organização de dados de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe. Uma informação é um conjunto de dados estruturados e padronizados de forma a fornecer um sentido para alguém.

Ameaças

As ameaças a uma rede podem ser bastantes óbvias, ou podem vir disfarçadas como atividades ou ações insuspeitas. As organizações possuem dados que são, em geral, de uso privado da empresa, e não para o consumo público. Em alguns ambientes, alguns dados podem se prestar ao acesso público, enquanto outros não. Nessas situações, há a necessidade de se criar verdadeiras barreiras para impedir o acesso não-autorizado do lado público para o lado privado,

A segurança em uma rede envolve segurança física e segurança de *software*. Os aspectos físicos incluem o controle do acesso físico ao equipamento. Uma organização precisa determinar quem pode andar em suas dependências e a quais áreas se pode ter acesso permitido. Por exemplo, não se deve permitir que o indivíduo que entrega o jornal bem cedo pela manhã entre na sala do servidor ou na de conexão de telefone. Por outro lado, os administradores do servidor e das telecomunicações precisam ter acesso ao servidor e/ou à sala de conexão dos telefones, mas acesso restrito a outras áreas que não envolvam as responsabilidades de seus cargos.

Ter acesso aos equipamentos físicos faz com que seja muito mais fácil a um indivíduo obter acesso não-autorizado a uma área, ou simplesmente roubar o *hardware* para, mais tarde, fazer um escrutínio dele. Não importa quantos esquemas de proteção de *software* estejam ativos, se a segurança física for frágil ou se mostrar ausente, o *software* não pode superar os buracos da segurança física.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança da informação poderá ser afetada por questões de comportamento e pelo uso de quem a utilizará, ambiente onde se instala, infraestrutura, ou por usuários mal intencionadas que possuem a finalidade de furtar, danificar ou alterar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade - é quem representa atualmente, orientam e faz análise e o planejamento da implementação da segurança para grupos de informações na qual será protegido. Irretratabilidade e a autenticidade também são itens que precisam ser monitorados. A evolução do comércio na web e da sociedade da informação, a privacidade nas transações tornou-se alvo de preocupação.

Os atributos básicos (segundo os padrões internacionais) são:

Confidencialidade

- *Integridade*

Disponibilidade

O nível de segurança almejado, precisa de uma "política de segurança" que é elaborado pela entidade ou responsável, para garantir que a estabilidade e os princípios do nível alcançado sejam mantido.

Para a elaboração desta política, deve-se levar em consideração:

- Riscos atrelados à ausência de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Mecanismos de segurança.

O suporte para as recomendações de segurança pode ser encontrado em:

- Controles físicos: são dispositivos que bloqueia o contato ou acesso direto a informação ou a infra-estrutura que a suporta.

Mecanismos de segurança como portas, trancas, paredes, blindagem e guardas, etc., apoiam os controles físicos.

- Controles lógicos: são bloqueadores para impedir ou limitar o acesso a dados de informação, que está em local controlado, em geral eletrônico, e que, de outra maneira, estaria exposta a acessos não autorizado por usuários mal intencionados.

Existem mecanismos de segurança que apoiam os controles lógicos:

- *Mecanismos de criptografia.* Transforma a informação de forma a torná-la ininteligível a pessoas fora da organização. É criado algoritmos específicos e uma chave secreta para tal procedimento, a partir de um grupo de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- *Assinatura digital.* Dados criptografados, garantindo a legitimidade do documento associado.

- *Mecanismos de garantia da integridade da informação.*
- *Mecanismos de controle de acesso.* Palavras-chave, sistemas biométricos, firewalls e cartões inteligentes.
- *Mecanismos de certificação.* Garante a certificação de um determinado documento.
- *Integridade.* Sistema em que um serviço/informação é original, isto é, esta protegido contra fraudes por intrusos.
- *Honeypot:* É o nome dado a um software, cuja função é detectar ou impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código, etc.

Requisitos de segurança

A segurança das informações não pode ser validada apenas pela tecnologia existente, as políticas de planejamento e gerenciamento das ações por parte dos gestores é fundamental. Antes que a empresa inicie um projeto de segurança, algumas ações devem ser realizadas em cada etapa, a avaliação de risco é uma forma que a empresa tem para identificar quais são os riscos aos quais ela está suscetível, como também quais controles serão necessários.

Segundo Laudon e Laudon (2007), a avaliação de risco permite que os gestores da empresa em conjunto com os especialistas em segurança consigam determinar qual o prejuízo que a empresa terá caso algum processo não seja controlado. Alguns passos podem ser seguidos pelos gestores quando falamos em avaliação de risco, são eles:

- Desenvolver a consciência dos riscos de tecnologia da informação.
- Quantificar os impactos aos negócios.
- Desenvolver soluções aplicáveis para a realidade da empresa.
- Colocar em prática essas soluções.
- Elaboração de programas de melhoria contínua.

Depois de avaliados os riscos para a informação da empresa, se faz necessário estabelecer uma política de segurança, pois com isso a empresa consegue determinar pessoas responsáveis e o caminho a ser percorrido, os responsáveis têm um norte a seguir para implementação dos recursos. Segundo Laudon e Laudon (2007), a política de segurança permite estabelecer uma hierarquia para os riscos, com definições de prioridade e metas de segurança aceitáveis.

Após avaliação dos riscos, a empresa determina como será a implantação das tecnologias referentes à segurança, essas são de extrema importância, pois são a base desse procedimento juntamente com os colaboradores responsáveis.

Funcionamento de um sistema de segurança

Para um bom funcionamento do sistema de segurança, é necessário que a empresa tenha em mente o que deve ser protegido, contra o que será necessário proteger e como será feita a proteção. Você já pensou entrar na internet do seu computador sem um antivírus? Em poucos minutos diversas invasões poderiam acontecer e dados poderiam ser perdidos, arquivos poderiam ser roubados e informações pessoais proliferadas nas redes. Nas empresas também acontecem esses problemas, pois algumas ainda não estão preocupadas com a segurança dos seus dados e acabam ficando vulneráveis a invasões.

Para Laudon (2004), a segurança dos sistemas de informação está relacionada à proteção dos computadores contra danos e o uso não autorizado, em relação a esse fato existem três importantes aspectos da segurança, que são garantir a segurança dos dados, proteger os PCs e redes e desenvolver os planos de recuperação dos desastres que afetam os sistemas de informação. Esses fatores exigem, por parte dos gestores, uma atenção maior do que em tempos anteriores, pois a necessidade do uso da informação e a dependência do uso da tecnologia aumentaram consideravelmente, uma vez que o mercado está em constante evolução exigindo respostas rápidas e confiáveis.

As estratégias devem ser avaliadas para que mecanismos de defesas sejam adotados, segundo Laudon (2004), elas devem abordar a segurança dos dados, proteção dos PCs e redes e recuperação dos desastres, podendo ser avaliadas da seguinte maneira:

Objetivos da Estratégia de Defesa

Prevenção e detenção	Os controles de desenho quando podem impedir que aconteçam erros, impedir os criminosos de atacar o sistema e, melhor ainda negar acesso às pessoas não autorizadas. A prevenção e a detenção são importantes, principalmente onde potencial de dano é muito alto;
Detecção	Pode ser que não seja economicamente viável evitar todos os perigos as medidas de deteção podem não funcionar. Por isso, os sistemas desprotegidos são vulneráveis a ataques. Da mesma forma como num incêndio, que quando antes ele for detectados, mais fácil de combate-lo e menor será o dano;
Limitação	Esta estratégia visa a reduzir (limitar) as perdas, depois de acontecer algum problema. Os usuários normalmente querem que seus sistemas voltem a funcionar o mais rápido possível. Isso pode ser feito através de um sistema de tolerância as falhas que permite a operação provisória de um sistema defeituoso até que a recuperação total tenha sido efetuada;
Recuperação	O plano de recuperação explica como consertar um sistema de informação danificado o mais rápido possível. Uma das formas de recuperação rápida é substituir os componentes, ao invés de consertá-los:
Correção	Corrigir as causas dos danos aos sistemas pode evitar que o problema aconteça novamente.

Fonte: Turban (2004)

Controle de acesso

Diante desse tema, podemos considerar o termo controle de acesso como sendo o conjunto de políticas e métodos que a empresa adota para evitar que pessoas indevidas accessem os sistemas disponíveis (LAUDON; LAUDON, 2007).

Para obter o acesso à informação, o usuário precisa ser autorizado pela liberação dos acessos como também precisa ser autenticado. Essa autenticação é gerada com o cadastro de senha no sistema, depois de cadastrada, o acesso é liberado e as ferramentas que o usuário utilizará para executar suas atividades diárias. Por exemplo, para um usuário que trabalha no setor financeiro e cadastra o movimento bancário, o gestor irá liberar o acesso ao módulo financeiro e a ferramenta de movimento bancário. Com isso, esse usuário não terá acesso a outros módulos do sistema, como compras, almoxarifado, comercial etc.

Controle Biométrico

O controle biométrico é uma forma de identificação das pessoas que estão liberadas para utilização do sistema de informação por meio de identificações físicas e comportamentais, entre as mais frequentes estão: fotografia do rosto, impressões digitais, geometria da mão, leitura da íris, padrão de vasos sanguíneos na retina do olho humano, voz, assinatura, dinâmica de digitação dentre outras medidas biométricas (LAUDON, 2004).

Algumas empresas já estão adotando esse tipo de controle com os seus servidores, liberando somente as pessoas devidamente identificadas para ter acesso ao local que eles estão armazenados.

Firewall

O firewall é um dispositivo que garante a sua navegação na internet de forma tranquila, ele acompanha as informações que são processadas entre sua máquina e o servidor da empresa, permitindo acessos e bloqueando arquivos que possam danificar dados e a segurança das informações. Firewall é uma combinação de hardware e software que controla o fluxo de tráfego que entra ou sai da rede. Geralmente é instalado entre as redes internas da empresa e as redes externas, como a internet, embora também possa ser utilizado para proteger partes da rede da empresa do restante da rede (LAUDON e LAUDON, 2007, p.226).

Hackers

Para o autor Mattos (2005), os hackers são pessoas que mexem nas coisas, fuçadores, que geralmente começam como um garoto jovem que se interessa por computador, e com isso vai descobrindo que é possível invadir outros computadores, espalhar programas para executar algumas funções, bisbilhotar arquivos alheios etc., e com isso torna-se um criminoso cibernético. Um cracker é um hacker especializado em quebrar proteções, enquanto um hacker se aproveita das falhas de segurança, o cracker elimina a segurança dos sistemas.

Vírus

Os vírus podem causar grandes prejuízos para as organizações, eles são considerados como pequenos programas que capturam dados, travam sistemas operacionais, roubam senhas pessoais e podem também apagar os registros dos dados inseridos no sistema de informação. Os vírus de computador são comparados aos que atacam o organismo humano, pois assim que conseguem acesso a um computador, automaticamente se reproduzem e se proliferam para outras máquinas. Essa proliferação acontece com o uso da internet, ele pode utilizar meios para ser enviado para outros computadores como, por exemplo, falhas de segurança, e-mails ou downloads. Dessa forma, se faz necessária a conscientização dos

colaboradores da organização de utilizar seu computador e os recursos que estão disponíveis de maneira correta, além da segurança instalada pela própria organização.



REFLITA

Redes de Computadores – Curiosidades

Ruas, avenidas e rodovias, isso existe no mundo dos “humanos” em todo local em que se olha. Mais a verdade é que existem também “ruas”, “avenidas” e “rodovias” por assim dizer no mundo virtual.

No “Cyber World” existem as redes de computadores que nada mais são do que locais aonde os pacotes de dados trafegam por “ruas”, “avenidas” e “rodovias” que existem vias cabos, switch, roteadores, servidores, satélites e etc.

Existem ruas em um cabo?

Não é bem uma rua, mas sim, é um caminho aonde o pacote de dados (Pacote de dados, ao acessar a internet e enviar um e-mail, as letras são transformados em binários (0,1) e esses milhões de 0,1 são chamados de pacotes, que tem um destino, mas para chegar ele tem que se comunicar com outros componentes, switch's, roteadores até chegar em um servidor e ao e-mail do destinatário, aonde os dados 0,1 são transformados em letras de novo e exibido no computador do destinatários) trafegam, quando ele sai do computador ele passa por algumas camadas e protocolos na rede, resumindo, um transforma as letras em 00110011 exemplo, outros protocolo coloca um “rótulo” com um endereço IP (IP, numero único de computador na rede) e depois de saber aonde os dados irão, ele entra na rede e viaja até o endereço que está no pacote.

Existem alguns tipos de redes, a local LAN – Local Área Network – Residencias etc.

As redes MAN – Metropolitan Área Netwok. – Redes entre cidades ligadas com fibra, e antena de longo alcance.

E as redes WAN – Wide Área Network – Redes entre países ligadas via satélites.

Com isso fica um pouco claro as redes, pois precisam de espaço para trafegar, sem espaço os pacotes de chocam e se perdem, os famosos erros de Time Out nos sites.

ACESSAR



Conclusão - Unidade 4

Nesta unidade abordamos a importância da informação para as organizações e a tomada de decisão depende muito baseado no sucesso da manutenção dessas informações. Os meios de armazenamento foram destacados, pois é muito importante para todos os envolvidos onde os dados estarão disponíveis com segurança e proteção sempre levando em conta o custo x benefício do investimento em segurança e armazenamento dos dados.

Este é um campo da gestão da informação que está em permanente atualização, e cabe as organizações optar pelo meio mais adaptável a sua realidade diária, levando em conta segurança dos dados e custo.

Vimos também nessa unidade, as principais diferenças, vantagens e desvantagens entre o sistema de arquivos distribuído físico e o sistema de arquivos em nuvem.

Na segunda parte da nossa unidade tratamos da questão da segurança de dados e acessos através das redes, que não existe uma regra para segurança de acessos, depende muito de qual maneira essa informação deve ser protegida e sua importância, e as pessoas que podem ter acesso a elas, cada sistema de rede deve ser considerada caso a caso, só assim é que uma política de segurança pode ser desenvolvida e implementada.

Esperamos que tenham apreciado o material, e temos plena certeza você está preparado(a) para seguir em frente ampliando ainda mais seus conhecimentos e aplicando as técnicas e estratégias aqui abordadas e com isso obter ainda mais sucesso em sua vida profissional. Até uma próxima oportunidade. Sucesso!

Material Complementar



Livro

Redes de Computadores

Autor: Ed Tittel

Editora: Bookman

Sinopse: As tecnologias usadas para transferir dados entre computadores envolvem muitas metodologias e componentes diferentes. Uma das principais finalidades da comunicação de dados é permitir que diferentes hardwares e sistemas operacionais se comuniquem e se entendam entre si. Para tanto, o meio de transmissão envolvido na comunicação de dados tem que atender a certas especificações de hardware e o software usado pelo sistema operacional do computador, para ter acesso ao meio de transmissão, precisa estar de acordo com os padrões.



Livro

Segurança de Redes em ambientes corporativos

Autor: Emilio Tissato Nakamura, Paulo Lício de Geus

Editora: Novatec

Sinopse: A segurança da informação possui influência cada vez maior no sucesso dos negócios. Para aplicar a melhor estratégia de defesa, é preciso conhecer os principais riscos e ataques realizados por hackers, além de entender os principais conceitos de segurança e tecnologias, mecanismos e protocolos disponíveis para a proteção. Forme sua base de segurança, aprendendo sobre segurança de redes, incluindo: o ambiente cooperativo, os riscos que rondam as organizações, a segurança em redes sem fio, a política de segurança, o firewall, os sistemas de detecção de intrusão, a criptografia e a PKI, as redes privadas virtuais, a autenticação e um modelo de segurança. - Conheça os principais ataques que devem ser defendidos. - Entenda os principais conceitos e forme sua base de segurança.



Filme

Blackhat

Ano: 2015

Sinopse: Nicholas Hathaway é um hacker prisioneiro que é liberado para ajudar em uma investigação contra uma rede de hackers mafiosos que planejam atentados catastróficos.

Referências

CORREA, Ana Grasielle Dionísio. **Organização e arquitetura de computadores.** São Paulo: Pearson Education do Brasil, 2017. Disponível em: <https://bv4.digitalpages.com.br>

DENARDIM, Gustavo Weber; BARRIQUELO, Carlos Henrique. **Sistemas operacionais de tempo real e sua aplicação em sistemas embarcados.** São Paulo: Blucher, 2019.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet:** uma abordagem top-dow. 6 ed. São Paulo: Pearson Education do Brasil, 2013. Disponível em: <https://bv4.digitalpages.com.br>

LIMA FILHO, Eduardo Correa. **Fundamentos de rede e cabeamento estruturado.** São Paulo: Pearson Education do Brasil, 2015.

MELL, P.; GRANCE, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST Special Publication 800-145.

RIBEIRO, Marcello Peixoto. **Redes de telecomunicação e teleinformática:** um exercício com ênfase em modelagem. Rio de Janeiro: Interciênciam, 2012. Disponível em: <https://bv4.digitalpages.com.br>

SAMPAIO, Jorge. Armazenamento de arquivos em nuvem grátis, mar. 2016, Disponível em < <https://safeptuga.blogspot.com/2016/03/armazenamento-de-arquivos-em-nuvem.html>> Acesso em: 20 junho 2019.

STALLINGS, Willian. **Arquitetura e organização de computadores.** 10 ed. São Paulo: Pearson Education do Brasil, 2017.

STALLINGS, Willian. **Criptografia e segurança de redes:** princípios e práticas. 6 ed. São Paulo: Pearson Education do Brasil, 2015.

TAURION, C. (2009). **Cloud Computing: computação em nuvem: transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport.

TITTEL, ED; **Redes de Computadores**, Porto Alegre: Bookman, 2003.

TURBAN, E. **Tecnologia da Informação para Gestão**. Trad. SCHINKE, Renate. 3.ed. Porto Alegre: Bookman, 2004.

VERAS, M. (2012). Cloud Computing: **Nova Arquitetura da TI**. 1.ed. Rio de Janeiro: Brasport.



Considerações Finais

Prezado(a) aluno(a),

Ao confeccionar esse material, procurei apresentar a você os principais conceitos com relação a redes de computadores. Para isso foi abordado as definições teóricos e práticos, e esperamos que tenha ficado bem claro para você a importância das redes de computadores, o quanto as topologias de redes influenciam no sucesso do compartilhamento de dados e equipamentos disponíveis na rede.

Destacamos também a importância histórica das redes, sua evolução no passar dos anos desde sua criação até os dias atuais, o surgimento da rede Ethernet e sua importância na transmissão de dados entre máquinas e corporações.

Vimos sobre o surgimento dos satélites de comunicação, suas tecnologias e importância nos meios de comunicação de rádio e TV. Os equipamentos de redes, como se comunicam e a importância da comunicação entre eles.

Ao abordar sobre cabeamento, enfatizamos os principais meios de transmissão e suas vantagens e desvantagens, questões de custos e benefícios dos modelos e tipos de cabos de transmissão.

Pensando numa organização de sistema de redes, como abordado no nosso material, temos sempre que levar em consideração o planejamento e a metodologia empregada no projeto, ouvir nosso cliente, discutir aspectos e dúvidas sobre o projeto com colegas da área e todos aqueles envolvidos no projeto em questão.

A partir de agora, temos plena certeza que você aluno(a) está preparado para seguir seu caminho e se aperfeiçoar cada dia mais e desenvolver suas habilidades se tornando um profissional de referência no mercado da tecnologia.

Até uma próxima. Muito obrigado!