Estratégia Concursos

Aula 00

MP-GO (Assistente Programador) Passo Estratégico de Conhecimentos Específicos

Autor:
Thiago Rodrigues Cavalcanti

29 de Novembro de 2023

2. Arquiteturas de redes: conceitos. Topologias de rede. Tipos: LAN, MAN e WAN. Protocolos de comunicação e suas aplicações em um ambiente de redes. Gestão de redes e serviços. Características e funções do modelo ISO/OSI e TCP/IP. Teoria Geral de Redes. Máscaras IP (classes, CIDR e VLSM). Estudo do comportamento dos dados em cabeamento lógico quanto aos quesitos: atenuação, colisão e ruídos. 3. Cabeamento: conceitos; tipos; cabos para redes locais; procedimentos para crimpagem de cabeamento; normas técnicas

Sumário

Apresentação 3
O que é o Passo Estratégico? 3
Análise Estatística 4
Roteiro de revisão e pontos do assunto que merecem destaque 5
Redes de Computadores 5
Redes locais (LAN), metropolitanas (MAN) e de longa distância (WAN) 6
Definições Importantes 11
Topologia da Rede 13

Definições Importantes 16
Modelos de Arquitetura 17
Modelo TCP/IP 18
Camada de Aplicação 19
Camada de Transporte 19
Camada de Internet / Rede 20
Camada de Interface com a Rede 21
Principais Protocolos X Camadas TCP/IP 22
Modelo OSI 22
Camada de Aplicação 23
Camada de Apresentação 23
Camada de Sessão 24
Camada de Transporte 24
Camada de Rede 24
Camada de Enlace 25
Camada Física 25
Protocolos e suas respectivas camadas no modelo OSI 25
Camada física 25
Cabo Par Trançado 26
Camada de Enlace de Dados 28
Multiplexação (divisão do canal) 29
Protocolos de acesso aleatório 29
Protocolos de revezamento 30

Subcamada de acesso ao meio 30
CSMA com Detecção de Colisão (CSMA/CD) 30
CSMA com Prevenção de Colisão (CSMA/CA) 31
Token Ring 31
Noções básicas de transmissão de dados 32
Modos de Transmissão 33
Aposta estratégica 35
Questões estratégicas 37
Questionário de revisão e aperfeiçoamento 44
Perguntas 45
Perguntas com respostas 46

APRESENTAÇÃO

Olá Senhoras e Senhores,

Eu me chamo Thiago Cavalcanti. Sou funcionário do Banco Central do Brasil, passei no concurso em 2010 para Analista de Tecnologia da Informação (TI). Atualmente estou de licença, cursando doutorado em economia na UnB. Também trabalho como professor de TI no Estratégia e sou o analista do Passo Estratégico de Informática.

Tenho graduação em Ciência da Computação pela UFPE e mestrado em Engenharia de Software. Já fui aprovado em diversos concursos tais como ANAC, BNDES, TCE-RN, INFRAERO e, claro, Banco Central. A minha trajetória como concurseiro durou pouco mais de dois anos. Neste intervalo, aprendi muito e vou tentar passar um pouco desta minha experiência ao longo deste curso.

O QUE É O PASSO ESTRATÉGICO?

O Passo Estratégico é um material escrito e enxuto que possui dois objetivos principais:

a) orientar revisões eficientes;

b) destacar os pontos mais importantes e prováveis de serem cobrados em prova.

Assim, o Passo Estratégico pode ser utilizado tanto para **turbinar as revisões dos alunos mais adiantados nas matérias, quanto para maximizar o resultado na reta final de estudos por parte dos alunos que não conseguirão estudar todo o conteúdo do curso regular.**

Em ambas as formas de utilização, como regra, **o aluno precisa utilizar o Passo Estratégico em conjunto com um curso regular completo.**

Isso porque nossa didática é direcionada ao aluno que já possui uma base do conteúdo.

Assim, se você vai utilizar o Passo Estratégico:

a) **como método de revisão**, você precisará de seu curso completo para realizar as leituras indicadas no próprio Passo Estratégico, em complemento ao conteúdo entregue diretamente em nossos relatórios;

b) **como material de reta final**, você precisará de seu curso completo para buscar maiores esclarecimentos sobre alguns pontos do conteúdo que, em nosso relatório, foram eventualmente expostos utilizando uma didática mais avançada que a sua capacidade de compreensão, em razão do seu nível de conhecimento do assunto.

Seu cantinho de estudos famoso!

Poste uma foto do seu cantinho de estudos nos stories do Instagram e nos marque:

@passoestrategico

Vamos repostar sua foto no nosso perfil para que ele fique famoso entre milhares de concurseiros!

ANÁLISE ESTATÍSTICA

A análise estatística estará disponível a partir da próxima aula.

ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Para revisar e ficar bem preparado no assunto, você precisa, basicamente, seguir os passos a seguir:

Redes de Computadores

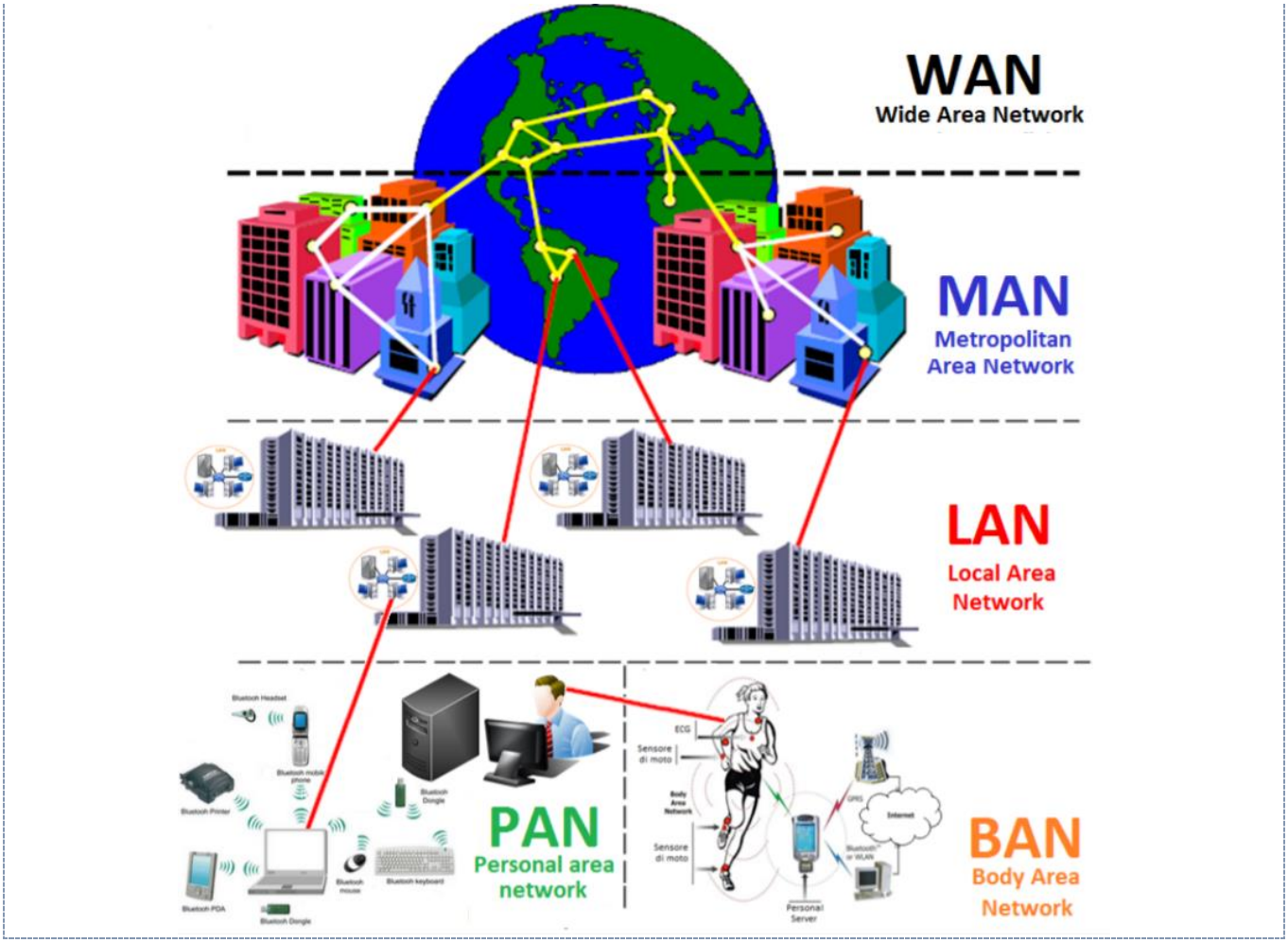
É importante entendermos que as redes de comunicação atualmente envolvem tanto telecomunicação quanto computação, e possuem como principal finalidade suprir a necessidade humana de **se comunicar à distância**. Essa necessidade surgiu desde os primórdios da humanidade e passou por diversos modelos de comunicação. Em um sistema de telecomunicações, as informações do emissor são convertidas em sinais elétricos para que possam trafegar pelo sistema até chegarem ao destino, onde são novamente convertidas em informações inteligíveis pelo destinatário. [Observe a ideia de codificação e decodificação].

Na década de 1830, Samuel Morse criou um dos primeiros aparelhos a utilizar sinais elétricos para transmitir informações, o telégrafo. Para enviar e receber as informações, no final da década, Morse concluiu a elaboração de um dos códigos mais conhecidos na comunicação e que leva seu nome, o Código Morse. A partir deste sistema, hoje temos o telefone, o rádio, a televisão, a Internet a cabo e muitas outras tecnologias.

Para termos uma base para os principais destaques que faremos a seguir, precisamos saber que as redes de computadores, utilizam o mesmo princípio de transmissão, onde as informações são convertidas em sinais elétricos. **Para que haja comunicação entre os dispositivos, além do sinal é necessário que todos "falem" a mesma linguagem.** Aqui entram os protocolos, que são responsáveis pelos padrões de comunicação. A partir das redes de computadores que é possível conectar vários dispositivos (hosts) no mundo inteiro.

Sobre esse tópico, você precisa que as redes são classificadas em **Rede Local (LAN)**, **Rede Metropolitana (MAN)** e **Rede de Longa Distância (WAN)**. E dentro dessas classificações surgem alguns ramos direcionados para as redes sem fio. Além disso, duas outras classificações também são muito cobradas em concursos públicos, a **Rede de Área de Armazenamento (SAN)** por conta do *Cloud Storage* e a **Rede de Área Pessoal (PAN)** por conta da Internet das Coisas (do inglês, *Internet of Things*, IoT) e das conexões de pequenas distâncias para compartilhar e controlar dispositivos.

Curiosidade: Existe um tipo de rede chamado **BAN (Body Area Network)** cujo raio de atuação de poucos metros e está associada a um conjunto de sensores que cobre os seres humanos. Veja na figura abaixo uma estruturação das redes cuja presença é maior em provas de concursos:



INDO MAIS
FUNDO!

Agora vamos destacar os principais pontos de cada uma das classificações, apresentando sempre que possível imagens e comparações entre elas.

Redes locais (LAN), metropolitanas (MAN) e de longa distância (WAN)

LAN

As *Local Area Networks*, ou Redes Locais, interligam computadores presentes dentro de um mesmo espaço físico. Isso pode acontecer dentro de uma empresa, de uma escola ou dentro da sua própria casa, sendo possível o compartilhamento de informações (ex.: arquivos) e recursos (ex.: impressora) entre os dispositivos

conectados. Como exemplo de meios de conexão neste modelo temos os cabos e rede e os roteadores Wi-Fi (quando os dipositivos dessa rede são conectados exclusivamente de forma sem fio, a classificação passa a ser WLAN – Wireless Local Area Network).

História

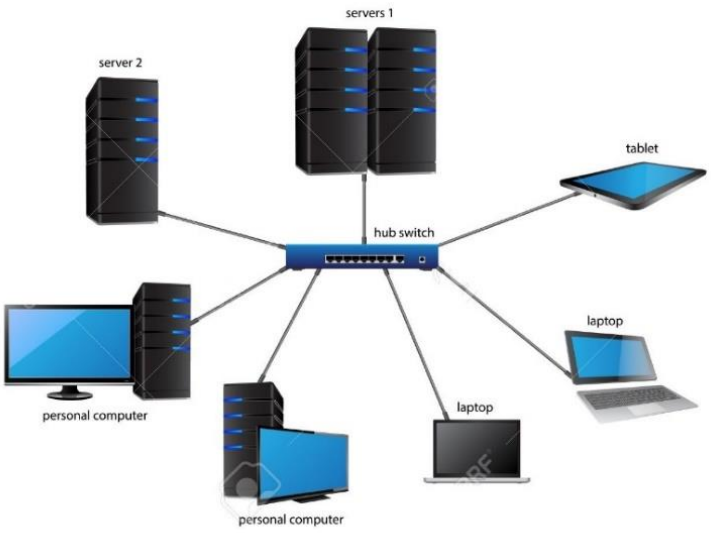
No início da computação, as empresas possuíam apenas um computador central, os mainfraimes, com usuários acessando através de terminais que utilizavam um cabo simples de baixa velocidade.

Com a crescente demanda e uso de computadores em universidades e laboratórios de pesquisa no final da década de 1960, houve a necessidade de fornecer interconexões de alta velocidade entre sistemas de computadores. No final da década de 1970 foram formadas as primeiras LANs, que eram usadas para criar links de alta velocidade entre grandes computadores centrais em um determinado local. De muitos sistemas competidores criados nessa época a Ethernet e ARCNET eram os mais populares.

O crescimento do *Control Program for Microcomputers* (CP/M ou Programa de Controle para Microcomputadores) e dos computadores pessoais baseados em DOS, viabilizaram para que em um único local houvessem vários computadores. Inicialmente, o principal uso das redes era o compartilhamento de espaço em disco e impressoras à laser, que na época eram extremamente caros. Em 1983 surgiu um entusiasmo maior com o conceito de LAN, que cuminou com a declaração pela indústria de computadores como "o ano da LAN"[1].

Componentes

É importante destacar que as LANs são formadas por vários dispositivos que possuem a mesma finalidade: a troca de dados. Entre eles temos os servidores, as estações e os equipamentos de conexão.



Servidores são computadores, que de forma centralizada fornecem serviços a uma rede de computadores de médio e grande porte, chamada de cliente (arquitetura cliente-servidor). Podem desempenhar diversas funções, como armazenamento de arquivos, sistema de correio eletrônico (e-mail), serviços Web (exemplo: sites), segurança (exemplo: proxy e firewall), banco de dados, e muitas

[1] Werner Schäfer, Helmut an de Meulen, **Systems network architecture**, Addison-Wesley, 1992, ISBN 0-201-56533-1 (em inglês)

outras. O sistema operacional dos servidores é apropriado para as funções exercidas, como alta capacidade de processamento e acesso a memória, interligados diretamente ao hardware.

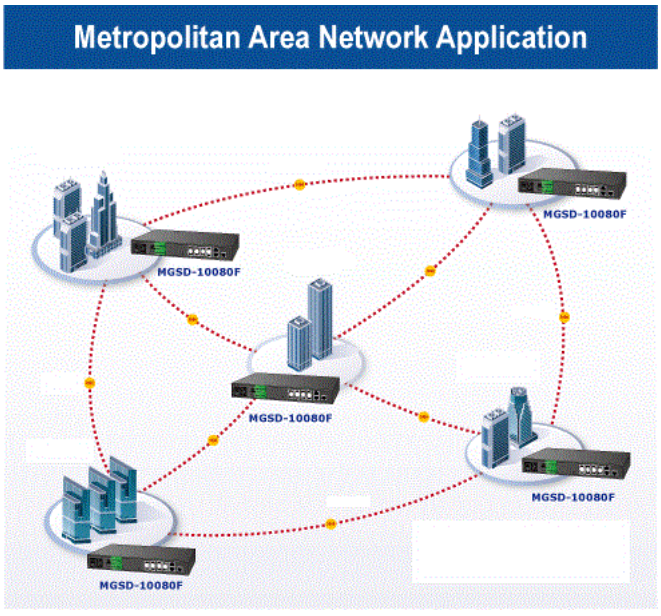
Estações são os clientes da rede que se conectam aos servidores para obter os serviços e as funções mencionadas acima. Geralmente são os computadores, notebooks, tablets e celulares.

Os equipamentos de conexão, também chamados dispositivos de rede, são os meios físicos responsávies pela comunicação entre os componentes participantes da rede. Como exemplo desses dispositivos temos: concentradores, roteadores, repetidores, gateways, switchs, bridges, placas de rede e pontos de acesso wireless. Alinhado com os equipamentos temos os protocolos de comunicação, que como explicado em aulas anteriores são os responsáveis pela padronização da "linguagem" de todos os dispositivos envolvidos.

As classificações das redes de computadores, nos modelos que estamos estudando, têm como base as Redes Locais ou *Local Area Networks* ou LANs. Mudando apenas o alcance e a abrangência de cada uma.

MAN

Para entender as redes metropolitanas, podemos imaginar que uma empresa possui dois ou mais escritórios em uma mesma cidade e seus computadores estejam conectados independente do local (escritório) onde estão ligados. Para isso, existem tecnologias como MPLS (Multi-Protocol Label Switching) que utiliza a rede de uma empresa que fornece Internet para conectar diferentes locais físicos; VPN (Virtual Private Network) que também utiliza a rede de uma empresa que fornece Internet, porém não existe a garantia de qualidade na conexão; e WiMax que conecta por meio sem fio pontos distintos de uma cidade. Neste último caso, a classificação também é alterada e passa a ser WMAN – Wireless Metropolitan Area Network.



História

Esse modelo cresceu a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção do sinal de televisão. Os primeiros sistemas eram compostos por uma grande antena instalada no alto de uma colina próxima, de onde o sinal era conduzido até a casa dos assinantes. Com o tempo algumas empresas começaram a entrar no negócio, obtendo concessões dos governos municipais para conectar por fio cidades inteiras. A etapa seguinte foi a programação de televisão e até mesmo canais inteiros criados apenas para transmissão por cabos. Com frequência, esses canais eram altamente especializados, oferecendo apenas notícias, apenas esportes, apenas culinária, apenas jardinagem, e assim por diante. Entretanto, desde sua concepção até o final da década de 1990, eles se destinam somente à recepção de televisão.

A partir do momento que a Internet passou a ser tornar popular, as operadoras de TV a cabo começaram a perceber que, com algumas mudanças no sistema, elas poderiam oferecer não apenas o serviço de TV, mas também o serviço de Internet em partes não utilizadas do espectro. Nesse momento, o sistema de TV a cabo começou a se transformar, passando de uma forma de distribuição de televisão para uma rede metropolitana[2].

WAN

O último destaque na classificação das redes, são as redes de longas distâncias que permitem a interligação de redes locais em países ou até continentes diferentes, numa grande área geográfica. A Internet é classificada como uma WAN.

História

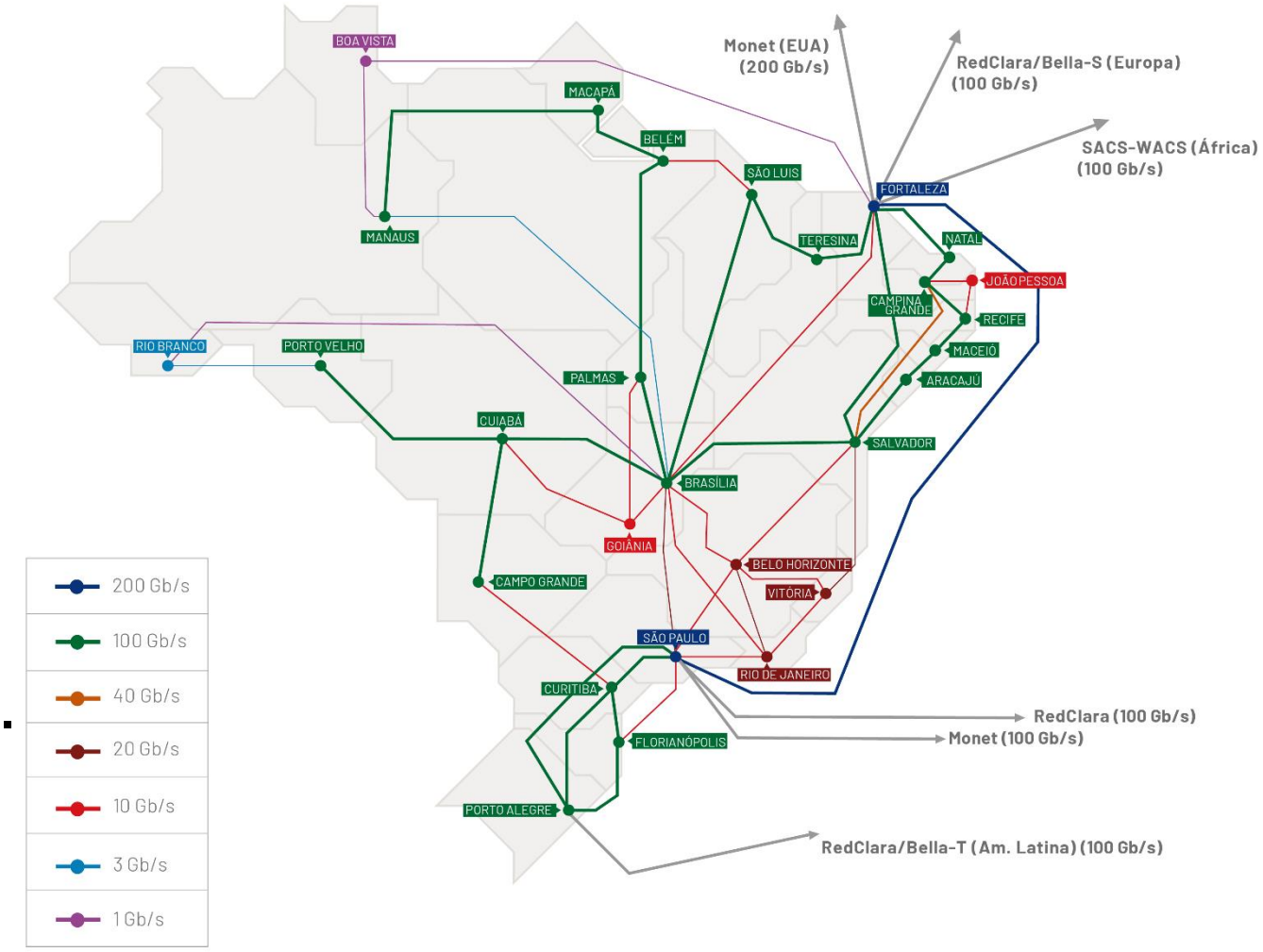
A história da WAN começa em 1965 quando Lawrence Roberts e Thomas Merril ligaram dois computadores, um TX-2 em Massachussets a um Q-32 na Califórnia, através de uma linha telefônica de baixa velocidade.

As WAN tornaram-se necessárias devido ao crescimento das empresas, onde as LAN não eram mais suficientes para atender a demanda de informações, pois era necessária uma forma de passar informação de uma empresa para outra de forma rápida e eficiente. Então surgiram as WAN que conectam redes dentro de uma vasta área geográfica, permitindo comunicação de longa distância.

No Brasil além das redes de consessão das fornecedoras, existe uma rede com esse alcance e abrangência, que é a Rede Nacional de Ensino e Pesquisa, RNP. Abaixo temos uma imagem das conexões estabelecidas pela RNP.

Conexão em 2023

[2] Tanenbaum, Andrew (2003). **Redes de computadores**. Editora CAMPUS, 4º edição. Pág: 19, 21



redeIpê

SAN

As Storage Area Networks, também designadas de redes de armazenamento, têm como objetivo a interligação entre vários computadores e dispositivos de armazenamento (*storage*) numa área limitada. Por exemplo: os grandes centros de armazenamento da Google, que arquivam não apenas e-mails, mas também os arquivos do Google Drive.

PAN

Redes de Área Pessoal utilizam tecnologias sem fio para interligar os mais variados dispositivos dentro de uma distância bastante limitada. Como exemplo desse modelo temos os mouses *Bluetooth*.

As duas últimas classificações (SAN e PAN) não são tão importantes, porém pode ser que sejam citadas em alguma parte da sua prova. Por isso, descrevi de forma sucinta e com exemplos práticos.

Definições Importantes

Nas definições abaixo temos alguns termos que são de grande importância para o assunto base da nossa aula. Por isso, é importante que você anote cada uma delas para fixar em sua mente.

Endereçamento: significa destinar um endereço para cada nó (dispositivo) conectado à rede. Um exemplo é o usado pelas redes de telefonia, onde cada aparelho de telefone possui o seu próprio número.

Meio: o ambiente físico usado para conectar os hosts de uma rede. O meio pode ser algum tipo de cabo (coaxial, par trançado, fibra ótica) ou através de ondas de rádio (Wi-Fi, bluetooth). Nos dispositivos, as placas de rede são a interface que realizam a conexão entre eles e o meio.

Protocolo: como falei anteriormente, os protocolos são regras que os dispositivos devem seguir para se comunicarem uns com os outros. Como exemplos de protocolos podemos citar o TCP/IP (*Transmission Control Protocol / Internet Protocol*) - protocolo para controle de transmissão e para a Internet, o FTP (*File Transfer Protocol*) - protocolo para a transmissão de arquivos entre computadores e HTTP (*HyperText Transfer Protocol*) - protocolo de transmissão de hipertextos (página da Web).

Roteamento: indica o caminho que os dados devem seguir do emissor ao destinatário, quando são transmitidos entre redes diferentes.

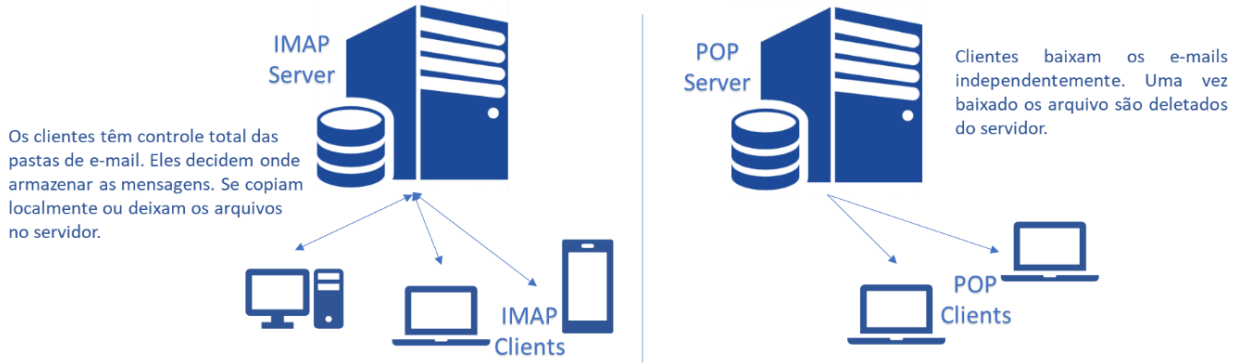
Download: Download (em português: descarregamento) significa obter (baixar) um conteúdo (um ou mais arquivos) de um servidor remoto para um computador local. Para isso são utilizados aplicativos específicos que se comunicam com o servidor através de protocolos pré-definidos. Por exemplo: os navegadores que acessam os dados de um servidor normalmente utilizando o protocolo HTTP.

Upload: Upload (em português: carregamento) é a operação inversa ao download. Ao fazer um upload, o usuário envia conteúdo do seu computador para um servidor remoto.

Firewall: Firewall (em português: parede de fogo) é uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet, através de uma política de segurança. Seu objetivo é permitir que somente dados autorizados sejam transmitidos e/ou recebidos.

Correio eletrônico: Correio eletrônico, conhecido popularmente como e-mail (abreviatura de *eletronic mail*), é um serviço que possibilita a troca de mensagens, textos, figuras e outros arquivos através de sistemas eletrônicos de comunicação.

Existem três protocolos de correio eletrônico baseados na Internet. O primeiro e mais antigo é o ***Simple Mail Transfer Protocol (SMTP)***, responsável **apenas pelo envio de mensagens** entre duas contas de usuários do e-mail. Os dois protocolos restantes gerenciam o acesso às mensagens que chegaram à conta do usuário de e-mail. Estes dois protocolos de "servidor de e-mail" são o ***Post Office Protocol (POP)*** e o ***Internet Message Access Protocol (IMAP)***. O funcionamento dos protocolos pode ser visto na figura abaixo.



Navegador: Navegador Web, navegador da Internet (em inglês: browser) é um aplicativo que possibilita a seus usuários acessarem documentos HTML (páginas ou sites) hospedados em um servidor da rede. Entre muitos, temos por exemplo: Internet Explorer, Edge, Firefox, Google Chrome, Safari e Opera.

Hiperlink: São links inseridos em páginas da Web, que quando clicados abrem outra página que pode ser do próprio site ou de outro site. A nova página também pode ser um formulário ou uma página de e-mail para se enviar uma mensagem.

URL: URL é a sigla correspondente à palavra "*Uniform Resource Locator*", que foi traduzida para a língua portuguesa como Localizador Uniforme de Recursos. Em outras palavras, URL é um endereço virtual com um caminho que indica onde está o que o usuário procura, e pode ser tanto um arquivo, como uma máquina, uma página, um site, uma pasta etc. Um URL é composto de um protocolo, que pode ser tanto HTTP, que é um protocolo de comunicação, FTP que é uma forma rápida de transferir arquivos na internet, etc. O formato do URL é definido pela norma RFC 1738.

Portal: Um portal é um site da Internet projetado para aglomerar e distribuir conteúdo de diferentes fontes de maneira uniforme, sendo um ponto de acesso para uma série de outros sites pertencentes ou não ao

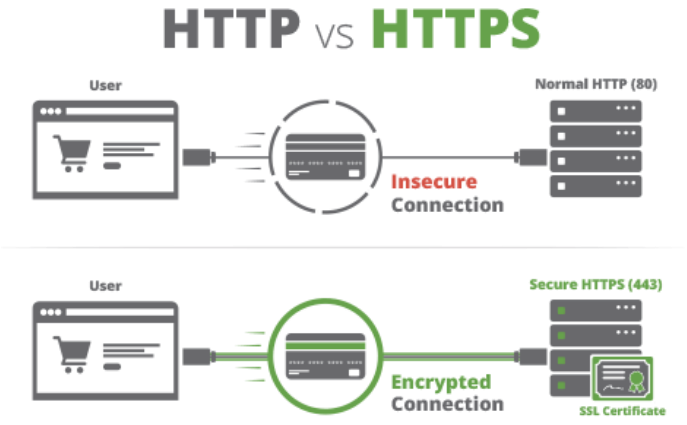
mesmo domínio. Um exemplo de portal é o g1.globo.com. A partir dele você pode acessar os sites de notícias de cada uma das regiões do país, o site do globoesporte.com, e muitos outros sites oferecidos pelo globo.com.

WEP: WEP é a sigla de Wired Equivalent Privacy, que foi o algoritmo de segurança mais usado do mundo, criado em 1999 e que é compatível com praticamente todos os dispositivos Wi-Fi disponíveis no mercado. Por conta da sua popularidade, logo foram descobertas falhas de segurança e por isso acabou se tornando um algoritmo inseguro. Oficialmente, o WEP não é considerado um padrão desde 2004, quando a Wi-Fi Alliance — associação que certifica produtos sem fio e promove a tecnologia — encerrou o suporte a ele.

WPA: WPA é a sigla para Wi-Fi Protected Access. Foi o algoritmo que substituiu o WEP tornando-se o protocolo-padrão da indústria, a partir de 2003. Como ele foi criado de forma a não tornar os dispositivos WEP obsoletos, uma série de elementos do protocolo antigo foi reaproveitada e, com ela, diversos dos problemas do antecessor também acabaram presentes na nova versão. Por este motivo, foi criada uma versão mais segura, a WPA2.

WPA2: É a sigla para a mais nova versão do WPA e também é o sistema-padrão atual, implementado pela Wi-Fi Alliance em 2006. A grande diferença está na maneira como o sistema processa as senhas e os algoritmos de criptografia.

SSL: SSL é a abreviação de *Secure Sockets Layer*, trata-se de uma ferramenta de encriptação de páginas antes de serem transmitidas pela internet que autentifica as partes envolvidas. É muito utilizada para pagamentos online com cartão de crédito. Diversas versões dos protocolos de segurança estão em uso generalizado em navegação na web, serviços de e-mail, mensagens instantâneas e VoIP. Resumindo o SSL torna a conexão segura. Veja a figura ao lado.



Topologia da Rede

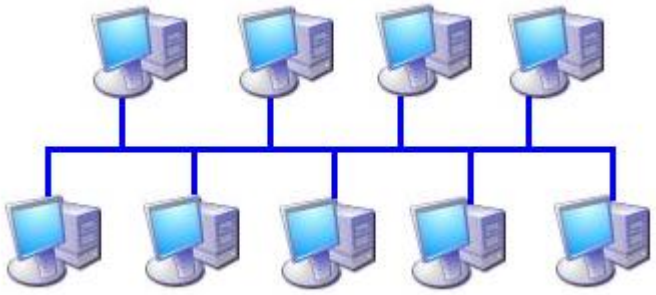
O termo topologia ou mais especificamente topologia da rede, diz respeito ao layout físico da rede, ou seja, como os computadores, cabos e outros componentes estão ligados na rede. Topologia é o termo padrão que muitos profissionais usam quando se referem ao design básico da rede.

A escolha de uma determinada topologia terá impacto nos seguintes fatores: tipo de equipamento de rede necessário, capacidades do equipamento, crescimento da rede e a forma como a rede será gerenciada

A topologia pode determinar como os computadores se comunicam na rede. Diferentes topologias necessitam de diferentes métodos de comunicação e esses métodos têm grande influência na rede. As topologias padrão mais usadas são as seguintes: **Barramento, Estrela e Anel**.

Barramento

A topologia de barramento também conhecida como barramento linear. Este é o método mais simples e comum de conectar os computadores em rede. Constituem em um único cabo, chamado tronco (e também backbone ou segmento), que conecta todos os computadores da rede em uma linha única.



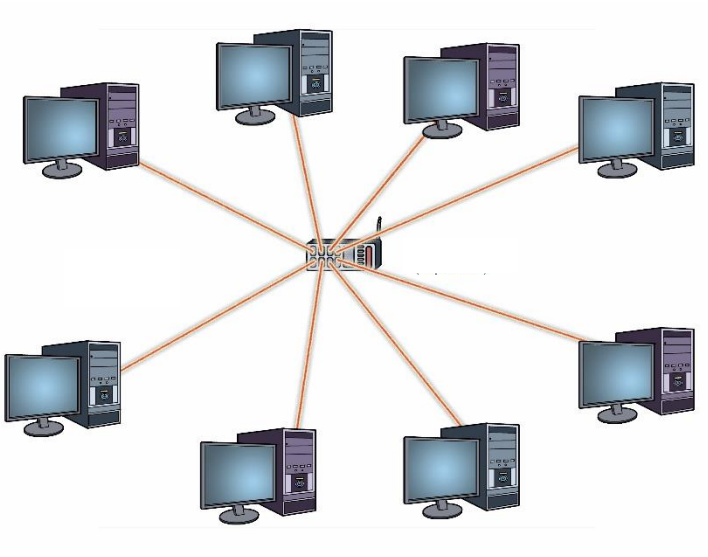
Os computadores em uma rede de topologia de barramento comunicam-se endereçando os dados a um computador em particular e inserindo estes dados no cabo sob a forma de sinais eletrônicos. Os computadores se comunicam em um barramento, segundo três conceitos: envio do sinal, repercussão do sinal e terminador.

Os dados da rede sob a forma de sinais eletrônicos são enviados para todos os computadores na rede; entretanto, as informações são aceitas apenas pelo computador cujo endereço coincida com o endereço codificado no sinal original. Apenas um computador por vez pode enviar mensagens. Os dados são enviados para todos os computadores, mas apenas o computador de destino aceita.

Como os dados, ou sinais eletrônicos, são enviados a toda a rede, eles viajam de uma extremidade a outra do cabo. Se o sinal tiver permissão para prosseguir sem interrupção, continuará repercutindo para frente e para trás ao longo do cabo, impedindo que os outros computadores enviem sinais. Portanto, o sinal deve ser interrompido depois que tiver tido a oportunidade de alcançar o endereço de destino adequado.

Com a função de impedir que o sinal repercuta um componente chamado terminador é colocado em cada extremidade do cabo para absorver sinais livres. A absorção do sinal libera o cabo para que outros computadores possam enviar dados.

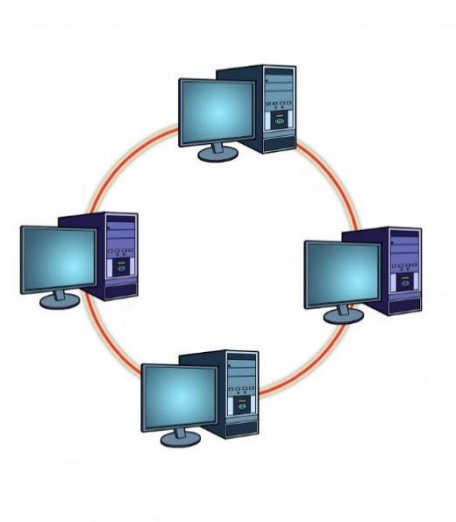
Estrela



Nessa topologia não há mais um único segmento ligando todos os computadores na rede. Eles estão ligados por meio de vários cabos a um único dispositivo de comunicação central, que pode ser um hub ou um switch. Este dispositivo possui várias portas onde os computadores são ligados individualmente, e é para onde converge todo o tráfego. Quando uma estação A deseja se comunicar com uma estação B, esta comunicação não é feita diretamente, mas é intermediada pelo dispositivo central, que a replica para a toda a rede, novamente somente a estação B processa os dados enviados, as demais descartam. Hubs e switches intermedeiam esta comunicação entre as estações de formas diferentes. Por exemplo, se um hub replica todo o tráfego que recebe para todas as suas portas, o mesmo não ocorre com o switch. A grande vantagem da topologia estrela em relação à de barramento, é que uma falha no cabo não paralisará toda a rede.

Somente aquele segmento onde está a falha será afetado. Por outro lado, a rede poderá ser paralisada se houver uma falha no dispositivo central. Os cabos utilizados se assemelham aos cabos utilizados na telefonia, porém com maior quantidade de pares. São cabos par-trançados, vulgarmente chamados de UTP e possuem conectores nas extremidades chamados de RJ-45.

Anel



Nessa topologia, as estações estão conectadas por um único cabo como na de barramento, porém na forma de círculo. Portanto não há extremidades. O sinal viaja em loop por toda a rede e cada estação pode ter um repetidor para amplificar o sinal. A falha em um computador impactará a rede inteira.

O método de transmitir dados ao redor de um anel chama-se passagem de símbolo. Um símbolo é passado de computador a computador até que cheque a algum que tenha dados para enviar. O computador que envia modifica o símbolo, anexa um endereço eletrônico aos dados e os envia ao longo do anel. Um computador captura o símbolo e o transmite ao longo do anel, os dados passam por cada computador até encontrarem aquele com o endereço que coincida com o endereço nos dados. O computador receptor devolve a mensagem ao computador emissor indicando que os dados foram recebidos. Após a verificação, o computador emissor cria um novo símbolo e o libera na rede.

Comparação entre as topologias:

Topologia	*Ponto Positivos*	*Pontos Negativos*
Estrela	- Maior tolerância a falhas - Facilidade de instalação - Monitoramento centralizado	- Custo de instalação maior porque requer mais cabos
Anel	- Facilidade de instalação razoável - Requer poucos cabos - Desempenho uniforme	- Se uma estação parar, todas as outras param - Dificuldade para a identificação de problemas
Barramento	- Facilidade de instalação razoável - Requer poucos cabos - Facilidade de compreensão das ligações	- Lentidão em períodos de uso intenso - Dificuldade para a identificação de problemas - Possibilidade de colisão

Para estruturar as funcionalidades de uma rede computadores, devido a sua grande complexidade, decidiu-se criar uma estrutura/arquitetura de camadas. Imagine um computador com diversas aplicações abertas utilizando a rede quando um dado é recebido. Como seria possível saber para qual das aplicações essa informação deveria ser repassada? A partir dessa estrutura de camadas, tornou-se possível entregar os dados para a aplicação correta.

Cada camada é independente nas suas funções e realiza um conjunto de serviços para que o dado possa chegar ao destino. Apesar da independência, as camadas fornecem serviços para a camada superior e utilizam serviços da camada inferior. Vamos estudar agora as camadas de acordo com os modelos OSI/ISO e TCP/IP.

Definições Importantes

Nas definições abaixo temos alguns termos que são de grande importância para o assunto base da nossa aula. Por isso, é importante que você anote cada uma delas para fixar em sua mente.

Endereçamento: significa destinar um endereço para cada nó (dispositivo) conectado à rede. Um exemplo é o usado pelas redes de telefonia, onde cada aparelho de telefone possui o seu próprio número.
Meio: o ambiente físico usado para conectar os hosts de uma rede. O meio pode ser algum tipo de cabo (coaxial, par trançado, fibra ótica) ou através de ondas de rádio (Wi-Fi, bluetooth). Nos dispositivos, as placas de rede são a interface que realizam a conexão entre eles e o meio.

Protocolo: como falei anteriormente, os protocolos são regras que os dispositivos devem seguir para se comunicarem uns com os outros. Como exemplos de protocolos podemos citar o TCP/IP (*Transmission Control Protocol / Internet Protocol*) - protocolo para controle de transmissão e para a Internet, o FTP (*File Transfer Protocol*) - protocolo para a transmissão de arquivos entre computadores e HTTP (*HyperText Transfer Protocol*) - protocolo de transmissão de hipertextos (página da Web).
Roteamento: indica o caminho que os dados devem seguir do emissor ao destinatário, quando são transmitidos entre redes diferentes.

Para estruturar as funcionalidades de uma rede computadores, devido a sua grande complexidade, decidiu-se criar uma estrutura/arquitetura de camadas. Imagine um computador com diversas aplicações abertas utilizando a rede quando um dado é recebido. Como seria possível saber para qual das aplicações essa informação deveria ser repassada? A partir dessa estrutura de camadas, tornou-se possível entregar os dados para a aplicação correta.

Cada camada é independente nas suas funções e realiza um conjunto de serviços para que o dado possa chegar ao destino. Apesar da independência, as camadas fornecem serviços para a camada superior e utilizam serviços da camada inferior. Vamos destacar cada camada de acordo com os modelos OSI/ISO e TCP/IP.

Modelos de Arquitetura

A arquitetura das redes de computador é formada por níveis, interfaces e protocolos. Cada nível oferece um conjunto de serviços através de uma interface ao nível superior, usando funções realizadas no próprio nível e serviços disponíveis nos níveis inferiores.

Cada nível deve ser pensado como um programa ou processo, implementado por hardware ou software, que se comunica com o processo no nível correspondente em outra máquina. Os dados transferidos em uma comunicação de um nível não são enviados diretamente ao processo do mesmo nível em outra máquina, mas descem verticalmente através de cada nível adjacente em sua máquina até o nível 1 (nível físico, responsável pela única comunicação entre as estações de fato), para depois subir através de cada nível adjacente na estação receptora até o nível de destino.

Este mecanismo de comunicação é conhecido como protocolo de nível N, logo, o protocolo de nível N é um conjunto de regras e formatos, através dos quais informações ou dados do nível N são trocados entre as entidades do nível N, localizados em sistemas distintos com o intuito de realizar as funções que implementam os serviços do nível N.

Existem três elementos-chave que definem os protocolos de rede:

1. **sintaxe:** representa o formato dos dados e a ordem pela qual eles são apresentados;

2. **semântica:** refere-se ao significado de cada conjunto sintático que dá sentido à mensagem enviada;
3. **timing:** define uma velocidade aceitável de transmissão dos pacotes.

O padrão mais cobrado em provas de concursos é o TCP/IP que veremos nas próximas páginas. E o que eu preciso saber deste conteúdo professor? Você precisa conseguir descrever cada uma das camadas, saber qual o tipo de unidade de dados e quais os protocolos presentes em cada camada. É isso que apresentaremos abaixo!

Modelo TCP/IP

O padrão *Transmission Control Protocol/Internet Protocol* (TCP/IP), surgiu a partir de uma necessidade específica do Departamento de Defesa dos Estados Unidos. Seu desenvolvimento inicial, em 1969, foi financiado pela Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos (DoD). O modelo de referência TCP/IP e a pilha de protocolos TCP/IP tornam possível a comunicação de dados entre dois computadores quaisquer, em qualquer parte do mundo, a aproximadamente a velocidade da luz.

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

Em cada camada o bloco de dados possui um nome diferente. Esses blocos de forma geral tem o nome de PDU (*Protocol Data Unit*, que em português significa Unidade de Dados de Protocolo). Abaixo listei o nome do PDU de cada camada.

TOME NOTA!

Camada	PDU
Aplicação	dados ou mensagens
Transporte	segmento
Internet	pacote ou datagrama
Interface de Rede	bit ou quadro

Agora vamos a partir da abordagem TOP-DOWN (de cima para baixo) estudar cada uma dessas camadas.

Camada de Aplicação

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

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

A camada de aplicação comunica-se com a camada de transporte através de uma porta. As portas são numeradas e as aplicações padrão usam sempre uma mesma porta. Por exemplo, o protocolo SMTP utiliza sempre a porta 25, o protocolo HTTP utiliza sempre a porta 80 e o FTP as portas 20 (para a transmissão de dados) e a 21 (para transmissão de informações de controle).

O uso de um número de porta permite ao protocolo de transporte (tipicamente o TCP) saber qual é o tipo de conteúdo do pacote de dados (por exemplo, saber que o dado que ele está a transportar é um e-mail) e no receptor, saber para qual protocolo de aplicação ele deverá entregar o pacote de dados, já que, como estamos a ver, existem inúmeros. Assim ao receber um pacote destinado à porta 25, o protocolo TCP irá entregá-lo ao protocolo que estiver conectado a esta porta, tipicamente o SMTP, que por sua vez entregará o dado à aplicação que o solicitou (o cliente de e-mail).

> Existem vários protocolos que operam na camada de aplicação. Os mais conhecidos são o HTTP, SMTP, FTP, SNMP, DNS e o Telnet.

Camada de Transporte

A Camada de Transporte está localiza entre as camadas de Aplicação e de Internet na pilha TCP/IP. Ela é responsável por fornecer serviços à camada de aplicação, e recebe serviços da camada de Internet.

No geral, a camada de transporte tem o papel de fornecer funções que permitam a comunicação entre processos de aplicações (softwares) entre computadores diferentes. Assim, a camada de transporte fornece um mecanismo pelo qual diversas aplicações distintas podem enviar e receber dados usando a mesma implementação de protocolos das camadas mais baixas.

Para que isso seja possível, a camada de transporte deve realizar diversas tarefas distintas (porém relacionadas entre si). Por exemplo, os protocolos da camada de transporte devem conseguir discernir quais dados provém de quais aplicações, combinar esses dados em um fluxo de dados que será enviado às camadas mais baixas da pilha de protocolos, e efetuar as tarefas inversas no host de destino, separando os dados e os entregando às aplicações que os devem processar (processos). Além disso, a camada de transporte pode dividir grandes quantidades de dados que devem ser transmitidos em pedaços - ou segmentos - menores para que sua transmissão seja possível.

E, ainda, a camada de transporte pode fornecer serviços de conexão para as aplicações (e outros protocolos) de camadas de nível superior. Esses serviços podem ser orientados a conexão, ou sem conexão, dependendo do protocolo utilizado.

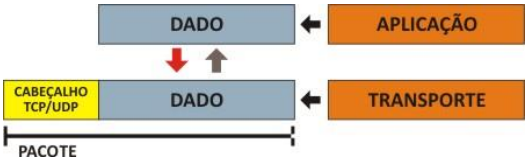
Os protocolos da camada de transporte também podem assegurar uma comunicação confiável entre os hosts, realizando controle de fluxo (taxa de transmissão de dados) e detecção de erros, além de permitir o reenvio de dados quando são perdidos ou descartados.

Funções da Camada de Transporte

- Comunicação entre processos (processo-processo)
- Controle de Fluxo
- Controle de Erros
- Multiplexação e Demultiplexação
- Controle de Congestionamento de rede
- Estabelecer e gerenciar conexões

Protocolos da Camada de Transporte

A Camada de Transporte do modelo TCP/IP define dois protocolos de transporte padrão: o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*). O TCP implementa um protocolo de fluxo de dados confiável, podendo assegurar que os dados sejam entregues de forma confiável em seu destino, pois fornece um serviço orientado à conexão. Já o UDP implementa um protocolo de fluxo de dados não-confiável, sem conexão, e que, portanto, não pode garantir a entrega dos dados ao host de destino.

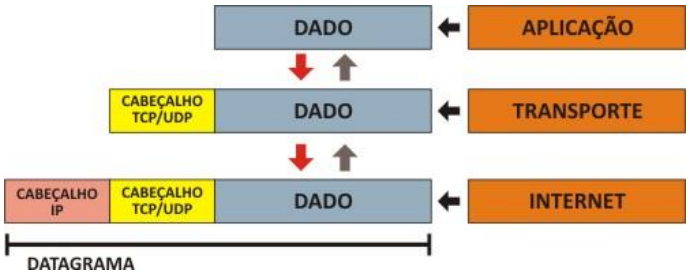


Camada de Internet / Rede

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

Na transmissão de um dado de programa, o pacote de dados recebidos da camada TCP é dividido em pacotes chamados datagramas. Os datagramas são enviados para a camada de interface com a rede, onde são transmitidos pelo cabeamento da rede através de quadros. Esta camada não verifica se os datagramas chegaram ao destino, isto é feito pelo TCP.

Há vários protocolos que podem operar nesta camada: **IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) e RARP (Reverse Address Resolution Protocol).**

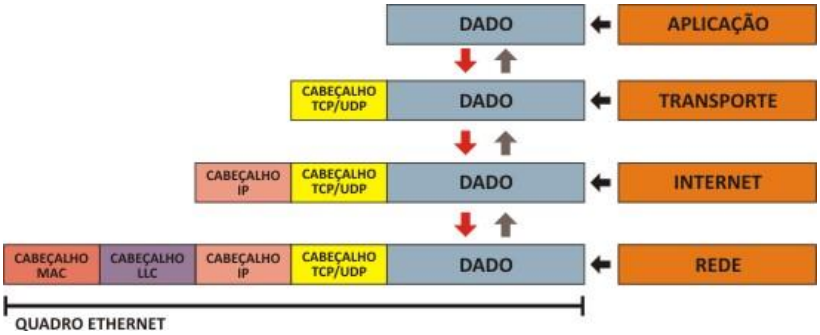


Camada de Interface com a Rede

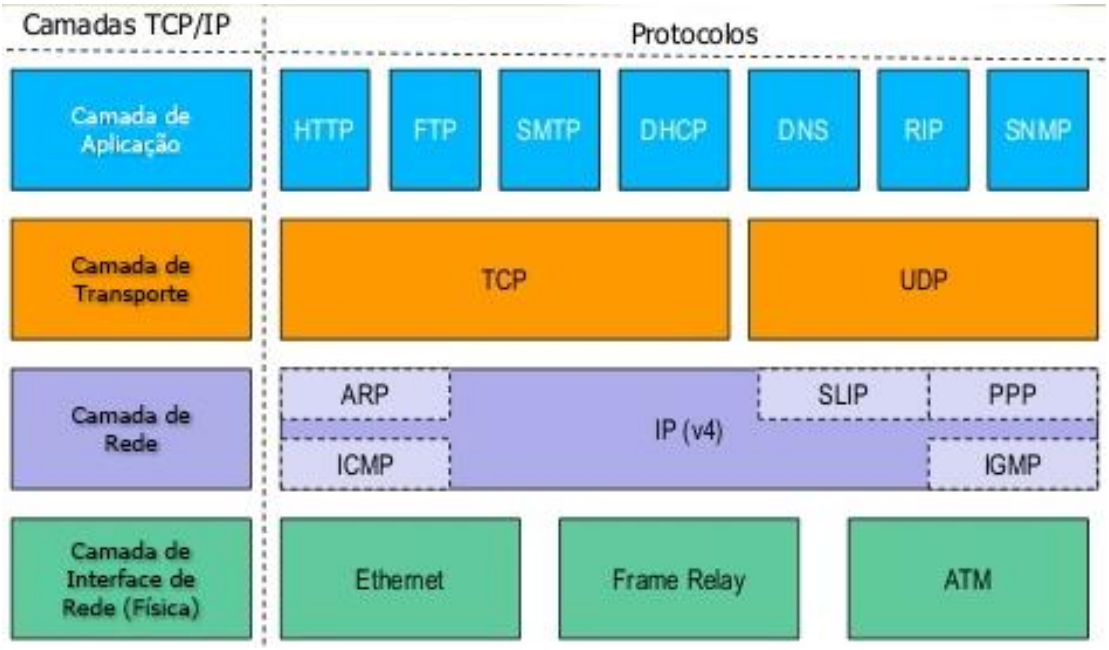
Os datagramas gerados na camada Internet são enviados para a camada Interface com a Rede, durante a transmissão de dados, ou a camada de Interface com a Rede pegará os dados da rede e os enviará para a camada de Internet, na recepção dos dados.

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

Logic Link Control (LLC): responsável por adicionar ao pacote, qual protocolo da camada de internet vai entregar os dados para a serem transmitidos. Quando esta camada recebe um pacote, ela sabe para qual protocolo da camada de internet deve ser entregue.
Media Access Control (MAC): responsável por montar o quadro que vai ser enviado pela rede e adiciona tanto o endereço origem MAC quanto o endereço destino, que é o endereço físico da placa de rede.
Physical: responsável por converter o quadro gerado pela camada MAC em eletricidade (no caso de uma rede cabeada) ou em ondas eletromagnéticas (para redes wireless).



Principais Protocolos X Camadas TCP/IP



Modelo OSI

O principal modelo para o desenvolvimento de padrões para interconexão de sistemas é o modelo OSI (*Open Systems Interconnection*), que está descrito em um documento da ISO[3]. O objetivo deste modelo é fornecer uma base comum que permita o desenvolvimento coordenado de padrões para interconexão de sistemas remotos. Neste modelo, nossa explicação será mais sucinta, pois é menos relevante do que o TCP/IP apresentado acima.

O Modelo OSI possui sete níveis de protocolos, apresentados na imagem abaixo com um resumo de suas funções:

[3] A ISO (*Internation Organization for Standardization*) é uma organização internacional fundada em 1946 que tem por objetivo a elaboração de padrões internacionais. Existem 89 países membros, sendo o Brasil representado pela ABNT e os EUA pela ANSI.

Resumo das Camadas do Modelo OSI

Aplicação	Prover serviços de rede às aplicações
Apresentação	Criptografia, codificação, compressão e formatos de dados
Sessão	Iniciar, manter e finalizar sessões de comunicação
Transporte	Transmissão confiável de dados, segmentação
Rede	Endereçamento lógico e roteamento; controle de tráfego
Link de Dados	Endereçamento físico; transmissão confiável de quadros
Física	Interface com meios de transmissão e sinalização

Da mesma forma do modelo TCP/IP, em cada camada o bloco de dados (PDU) possui um nome diferente. Abaixo listei o nome do PDU de cada camada.

Camada	PDU
Aplicação	dados ou mensagens
Apresentação	dados ou mensagens
Sessão	dados ou mensagens
Transporte	segmento
Rede	pacote ou datagrama
Enlace de Dados	quadro ou frame
Física	bit

Camada de Aplicação

Nesta camada são definidas funções de gerenciamento e mecanismos genéricos que servem de suporte à construção de aplicações distribuídas. Ela dá suporte às chamadas de procedimentos remotos, ou seja, para a aplicação que utiliza esta camada não fará diferença onde o procedimento será implementado, o importante é que a computação seja realizada e sua saída fornecida localmente.

Camada de Apresentação

Nesta camada são realizadas transformações adequadas aos dados, por exemplo, compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrão de rede e vice-versa.

Esta camada precisa conhecer a representação da informação (sintaxe dos dados) no seu sistema local e a representação no sistema de transmissão, podendo realizar as devidas conversões, como, formatação de dados e transformação de dados.

Camada de Sessão

Os principais serviços fornecidos pela camada de sessão são:

O gerenciamento de token - define a permissão a um dos nós onde a conexão foi estabelecida para começar a transmitir dados, evitando assim concorrência no diálogo.

O controle de diálogo - é uma forma de interromper uma conversação por um instante de tempo qualquer e voltar este diálogo do ponto interrompido.

O gerenciamento de atividade - pode garantir que atividades de maior prioridade executem sua atividade e no final da sessão irá retornar a atividade interrompida do ponto em que se encontrava.

Camada de Transporte

Na camada de transporte a comunicação é fim a fim, isto é, entidade da camada de transporte se comunica com a entidade da camada de transporte da máquina destino, fato que não ocorria nos outros níveis. Até a camada de rede, o protocolo atuava em todos hospedeiros e comutadores de pacotes que se encontravam no caminho entre a origem e o destino da mensagem.

A camada de transporte realiza controle de fluxo da origem ao destino, podendo este fluxo passar por diversos comutadores no caminho. Diferente da camada de enlace que realiza o controle entre as máquinas ligadas apenas no mesmo enlace.

Podemos ainda citar como funções o controle de sequência de pacotes fim a fim, a detecção e recuperação de erros de transmissão, a blocagem de mensagens e a multiplexação (controle do compartilhamento de uso) do acesso a camada de rede.

Camada de Rede

O objetivo da camada de rede é fornecer uma independência quanto as considerações de chaveamento e roteamento associados ao estabelecimento de conexões entre hospedeiros remotos na rede e a troca de mensagens entre os hospedeiros em qualquer local dentro da rede.

Existem duas filosofias quanto ao serviço fornecido nesta camada: datagramas e circuito virtual. No serviço datagrama (não orientado à conexão) cada pacote (unidade de dados) não tem relação alguma de passado ou futuro com qualquer outro pacote, devendo assim carregar de forma completa seu endereço de destino.

No serviço de circuito virtual (orientado à conexão) é necessário que o transmissor primeiro envie um pacote de estabelecimento de conexão. Cada conexão possui um identificador que irá marcar todos os pacotes pertencentes a esta conexão.

Camada de Enlace

O objetivo desta camada é detectar e opcionalmente corrigir erros que por ventura ocorram na camada física. A camada de enlace assim converte um canal de transmissão não confiável em um canal confiável entre dois hospedeiros interligados por um enlace (meio físico) para uso da camada de rede.

Outra questão tratada pela camada de enlace é como evitar que o transmissor envie ao receptor mais dados do que este tem condições de processar. Esse problema é evitado com um mecanismo de controle de fluxo.

Camada Física

O protocolo de camada física dedica-se à transmissão de uma cadeia de bits. Ao projetista desse protocolo cabe decidir como representar 0´s e 1´s, quantos microssegundos durará um bit, como a transmissão será iniciada e finalizada, bem como outros detalhes elétricos e mecânicos.

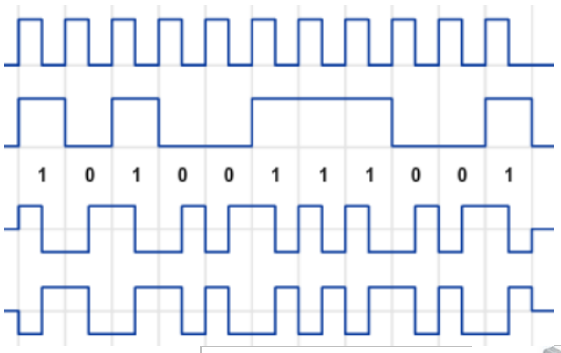
Protocolos e suas respectivas camadas no modelo OSI

Da mesma forma do modelo TCI/IP, as camadas do modelo OSI possuem protocolos próprios traduzem a "linguagem" necessária desde os sinais elétricos até cada uma das aplicações. Esses protocolos são os responsáveis por realizar a entrega correta dos dados recebidos e enviados pelas camadas superiores e inferiores.

Camada física

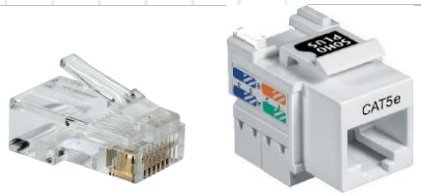
Esta camada define as características técnicas dos componentes envolvidos no processo de conexão, ou seja, os meios de conexão, que irão trafegar os dados. Essas características padronizam tamanho e forma de **cabos** e **conectores**, valores de **sinais elétricos**, e o significado de cada **sinal transmitido**. Ela fornece os requisitos

para transportar pelo meio físico os bits que formam o quadro da camada de Enlace de Dados, ou seja, na camada física os dados trafegam em formato de bits.

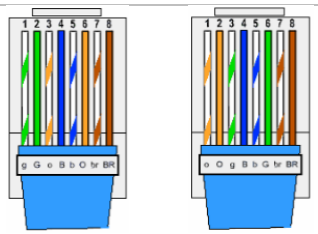


Os padrões de sinais permitem que vários dispositivos consigam operar em conjunto a partir de um mesmo meio físico. Ao lado podemos observar a forma de vários sinais digitais.

Já os padrões de conectores, determinam a forma de conexão (por existirem diferentes cabos, eles podem ser conectados de maneiras diferentes) e a finalidade de cada modelo de conector.



Conectores RJ45 (Macho e Fêmea)



Padrões de conexão (A e B)

Conector RS-232

Conector Coaxial

Conector BNC

Conectores de fibra ótica

Cabo Par Trançado

O cabo par trançado, ou twisted pair, possui um maior custo benefício e por esse motivo são os mais utilizados em redes LAN. Possuem velocidades, no mínimo, 10 vezes maiores que o cabo coaxial e maior maleabilidade.

Eles são constituídos de 4 pares de cabos torcidos. O fato dos pares serem trançados faz com que o nível de ruído e interferência externa seja reduzido. As normas e padronizações desses cabos são definidos pela ANSI/EIA (American National Standards Institute/Electronic Industries Alliance). Para todos os cabos desse tipo, se aplica a distância máxima de 100m.

Existem 9 categorias de cabo par trançado. Elas se diferenciam pela taxa de transmissão e aplicação:

Categoria	Taxa de transmissão	Aplicação
CAT 1	Até 1 Mbps	Voz analógica
CAT 2	4 Mbps	IBM Token Ring
CAT 3	10/16 Mbps 16 Mhz	10BASE-T Ethernet
CAT 4	16/20 Mbps 20 MHz	Token Ring de 16Mbps
CAT 5	100 Mbps (1Gbps com 4 pares) Até 100 MHz	Substituído pelo 5e 100BASE-TX e 1000BASE-T
CAT 5e	100 Mbps (10Gbps - protótipo) Até 125 MHz	Gigabit Ethernet 1000BASE-T
CAT 6	Até 250 MHz	Banda larga 1000BASE-TX
CAT 6a	Até 500 MHz	10GBASE-T
CAT 7	600-700MHz	100GBASE-T Vídeo em Full Motion

Além dessas categorias, o cabo par trançado pode ser classificado quanto à sua blindagem. Os cabos sem blindagem são chamados de UTP (Unshilded Twisted Pair). Já os cabos blindados, são divididos em três tipos:

- FTP (Foiled Twisted Pair): possuem uma blindagem mais simples feita de folha de aço ou liga de alumínio com o objetivo de reduzir a interferência externa. Porém, não é blindado contra crosstalk (interferência entre os pares de cabos).
- STP (Shielded Twisted Pair): essa categoria já se utiliza de uma blindagem para cada par de cabos. Com isso, é possível reduzir o crosstalk, aumentando a tolerância a distâncias maiores que os 100m estabelecidos pelo padrão.

- SSTP (Screened Shielded Pair) ou SFTP (Screened Foiled Twisted Pair): é uma categoria que une as características dos cabos FTP e STP, isto é, há a blindagem para cada par bem como a blindagem externa de todos os cabos. Foi criado para ser usado em ambientes suscetíveis a grandes interferências externas com distâncias maiores.

Camada de Enlace de Dados

O enlace é o caminho que um pacote vai percorrer entre o transmissor e o receptor, denominados de nós. A camada de enlace tem como principal objetivo transferir datagramas (quadros) entre esses nós, a partir da conversão do fluxo de dados sem formatação da camada física. Para isso ela é capaz de detectar e corrigir erros, controlar o acesso dos enlaces compartilhados, realizar o endereçamento e transferir de forma confiável os dados com controle de fluxo. As interfaces de rede (Ethernet e WiFi) fazem parte desta camada.

Para realizar todas essas tarefas a camada de enlace utiliza protocolos como: PPP, LAPB (X.25) e ethernet. Entre os padrões determinados por esses protocolos está o que define que cada placa de rede de possuir um endereço físico único. Em redes do padrão IEEE 802, e outras não IEEE 802 como a FDDI, esta camada é dividida em outras duas camadas: Controle de ligação lógica (LLC), que fornece uma interface para camada superior (rede), e controle de acesso ao meio físico (MAC), que acessa diretamente o meio físico e controla a transmissão de dados.

Os protocolos e padrões desta camada, diferente das camadas superiores que são baseados em RFCs, são definidos por empresas de comunicações ou organizações de engenharias (ANSI, IEEE e ITU). Abaixo temos uma tabela com os principais protocolos correlacionados com a organização responsável.

Organização	Protocolo
ISO	HDLC (High Level Data Link Control)
IEEE	802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless)
ITU	Q.922 (Frame Relay Standard), Q.921 (ISDN Data Link Standard), HDLC (High Level Data Link Control)
ANSI	3T9.5, ADCCP (Advanced Data Comunications Control Protocol)

Existem dois tipos de enlace: o ponto a ponto e o broadcast (difusão). No enlace ponto a ponto, mesmo que exista uma conexão física de vários hospedeiros (hosts), haverá somente a comunicação entre um único remetente numa extremidade do enlace com outro remetente na outra extremidade do enlace. Podemos comparar esse modelo de enlace a o sistema de telefonia, onde mesmo que o remetente esteja interconectado a uma central telefônica só vai haver troca de informações quando este discar e a outra pessoa do outro lado da linha atender. Protocolos que utilizam esse tipo de comunicação: PPP e HDLC. No enlace broadcast vários nós (computador, servidor, etc.), remetentes e receptores, estão conectados em um único canal de transmissão. Como exemplo deste tipo de comunicação temos a televisão tradicional.

As redes antigas de difusão, exerciam uma questão fundamental na camada de enlace de dados, de controle do acesso ao canal compartilhado quando utilizavam ainda o padrão 802.3 - 10BaseX nas chamadas topologias em barramento. Este problema foi resolvido através da subcamada especial da camada de enlace de dados, a subcamada MAC - Controle de Acesso ao Meio.

As redes de computadores possuem regras que possibilitam o acesso múltiplo. Vários protocolos foram implementados na camada de enlace para permitir e controlar esses acessos. Podemos dividi-los em três categorias: Protocolos de Divisão do Canal; Protocolos de Acesso Aleatório; e Protocolos de Revezamento.

Multiplexação (divisão do canal)

Uma forma simples para a comunicação ser efetiva (sem colisões), é dividir o tempo de comunicação e entregar para cada um dos nós. Imagine uma rede com dez computadores e um tempo de 20 segundos para comunicação, por vez. Assim, é possível dividir o tempo pelo número de computadores, onde teríamos 2 segundos por computador, em cada rodada. Esse tipo de divisão é feita pelo **TDM (multiplexação por divisão de tempo)** que divide o tempo em quadros temporais, onde dentro desses quadros existem N compartimentos, onde N é igual ao número de computadores. Para cada TDM taxa de transmissão em bits são alocados slots (intervalos) no tempo para cada canal de comunicação.

O **FDM (multiplexação por divisão de frequência)** divide de forma semelhante, porém, em vez de espaços iguais de tempo, tem-se faixas iguais de frequência. Essas são técnicas eficientes considerando que todos os nós transmitem informações frequentemente. Porém, se em dado momento apenas um nó transmitir informações, este somente o poderá fazer através de sua "faixa", mesmo que nenhum outro nó esteja transmitindo. Dessa forma o canal broadcast fica ocioso em grandes períodos de tempo.

No **CDMA (multiplexação por divisão de código)** um sistema de múltiplo acesso permite a separação de sinais que coincidam no tempo e na frequência. Todos os sinais compartilham o mesmo espectro de frequência, cada sinal é codificado, através de um código específico para cada usuário, e espalhado por toda largura de banda, como um ruído para todos os usuários. A identificação e demodulação do sinal ocorrem no receptor, quando é aplicada uma réplica do código utilizado. Este processo retorna com o sinal de interesse, enquanto descarta todos os outros sinais caracterizados como interferência.

Protocolos de acesso aleatório

Um dos protocolos mais simples é o ***Slotted* ALOHA**. Nele o tempo de transmissão é dividido pelo número de quadro formando intervalos, de fato que um intervalo é igual ao tempo de transmissão de um quadro. Quando um nó tem algum quadro para enviar, ele espera até o início do próximo intervalo e o envia, se for detectada colisão, ele espera um tempo aleatório e envia novamente até que termine os quadros ou que haja uma nova colisão e tenha que esperar outro tempo aleatório. A "chave" desse protocolo é que se vários nós estiverem enviando, os intervalos em que houverem colisões serão desperdiçados e certos intervalos não serão utilizados, porque o tempo aleatório tem um caráter probabilístico. Portanto este não é um protocolo tão eficiente para uma rede com muitos nós que enviam informações constantemente.

Enquanto ***Slotted* ALOHA** precisa que seus nós sincronizem as transmissões de acordo com os intervalos, o primeiro protocolo ALOHA, chamado de **ALOHA Puro** é descentralizado. Quando um quadro chega à camada física ele é enviado imediatamente, sem aguardar o intervalo. Quando ocorre uma colisão, um tempo aleatório é esperado para um novo envio.

Os dois protocolos descritos anteriormente, interrompem a comunicação por um tempo aleatório durante uma transmissão de dados, no caso de algum outro nó esteja se comunicando. O **CSMA** funciona de forma diferente, escutando o canal antes de enviar as informações. Caso algum outro nó o esteja transmitindo, ele espera um tempo para então voltar a escutar o canal broadcast. Outra característica importante é que se quando o canal estiver ocioso e o nó transmitir coincidentemente no mesmo momento que outro, o CSMA interrompe a transmissão, até que algum protocolo determine quando deve tentar transmitir novamente.

Protocolos de revezamento

O protocolo de ***Polling*** requer que um dos nós seja nomeado o nó mestre. Esse nó escolhe de forma circular os nós que precisam transmitir. Quando o nó 1 for transmitir, o nó mestre concede um determinado número de quadros, acabando essa transmissão, o nó 2 inicia e assim sucessivamente. Os intervalos vazios característicos dos protocolos de acesso aleatório já não existem mais, porém não é seguro colocar as transmissões da rede nas mãos de um nó, porque se este falhar, toda a rede para. Outro problema é o tempo de escolha do nó que deverá transmitir. Esse tempo é bastante significativo.

No protocolo de passagem de permissão, chamado ***Token***, essas passagens de permissão são distribuídas por todos os nós. Por exemplo, o nó 1 poderá enviar permissão ao nó 2, o nó 2 poderá enviar permissão ao nó 3, o nó N poderá enviar permissão ao nó 1. Quando um nó recebe a permissão, ele mantém caso precise enviar alguma informação, se não, ele envia para o próximo nó.

Subcamada de acesso ao meio

A Subcamada de Acesso ao Meio (também conhecida pela sigla em inglês MAC) é uma parte da Camada de Enlace de Dados responsável por estabelecer uma lógica quanto ao uso do meio de transmissão em topologias de difusão. O objetivo do MAC é justamente tentar evitar ao máximo as colisões, pois elas fazem com que a rede se torne mais lenta. Os protocolos utilizados por essa subcamada são: ALOHA, CSMA, CSMA/CD, CSMA/CA e Token Ring. Note que alguns protocolos foram citados na Camada de Enlace de Dados.

CSMA com Detecção de Colisão (CSMA/CD)

Um dos grandes problemas do CSMA é que ele não é capaz de perceber quando ocorre uma colisão. Para sanar esta limitação, surgiu o CSMA/CD. A diferença entre o CSMA e o CSMA/CD está no que acontece quando ocorre colisão. Assim que um nó detecta colisão, ele imediatamente interrompe a transmissão de mensagens e envia um sinal de alerta que consiste em uma mensagem de 64 bytes composta apenas de "1"s. Assim todos os nós ao longo de barramento recebem o sinal de alerta que impede que eles também tentem

enviar dados. Quando o sinal de alerta é interrompido e então os nós que desejam enviar alguma informação esperam um tempo aleatório e começam a transmitir.

A grande vantagem do CSMA/CD é que ele avisa a todos os nós da rede que houve uma colisão. Então os outros nós não tentarão enviar mensagens desnecessariamente. Graças a isso, o CSMA/CD possui uma taxa de sucesso de entrega de cerca de 92%. O CSMA/CD não-persistente é o protocolo mais usado em redes de computador com fio.

CSMA com Prevenção de Colisão (CSMA/CA)

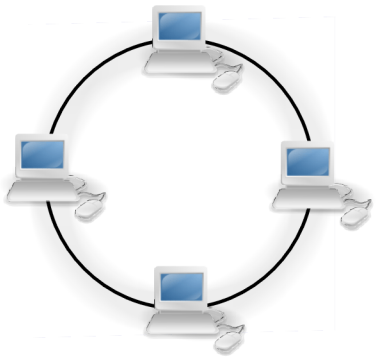
O CSMA/CA funciona quando um nó deseja se comunicar com outro e pede autorização para ele enviando um sinal RTS (Request To Send). Se um nó receber um RTS e estiver livre para se comunicar, ele envia um sinal chamado CTS (Clear To Send). Somente depois de receber um CTS, um nó pode começar a transmitir dados para outro. Toda vez que um nó que não está envolvido na troca de dados percebe um sinal RTS ou CTS na rede, fica sem transmitir dados por algum tempo para que não haja colisão.

Desta forma, a taxa de sucesso pode chegar a 100%. Todas as colisões são evitadas, já que os nós só podem enviar dados quando recebem a confirmação do receptor. As colisões com este protocolo só são possíveis em situações especiais em que cada nó possui um alcance de transmissão diferente ou caso existam nós móveis capazes de se deslocar pela área de transmissão.

O CSMA/CA é, atualmente, o protocolo mais usado em redes sem fio.

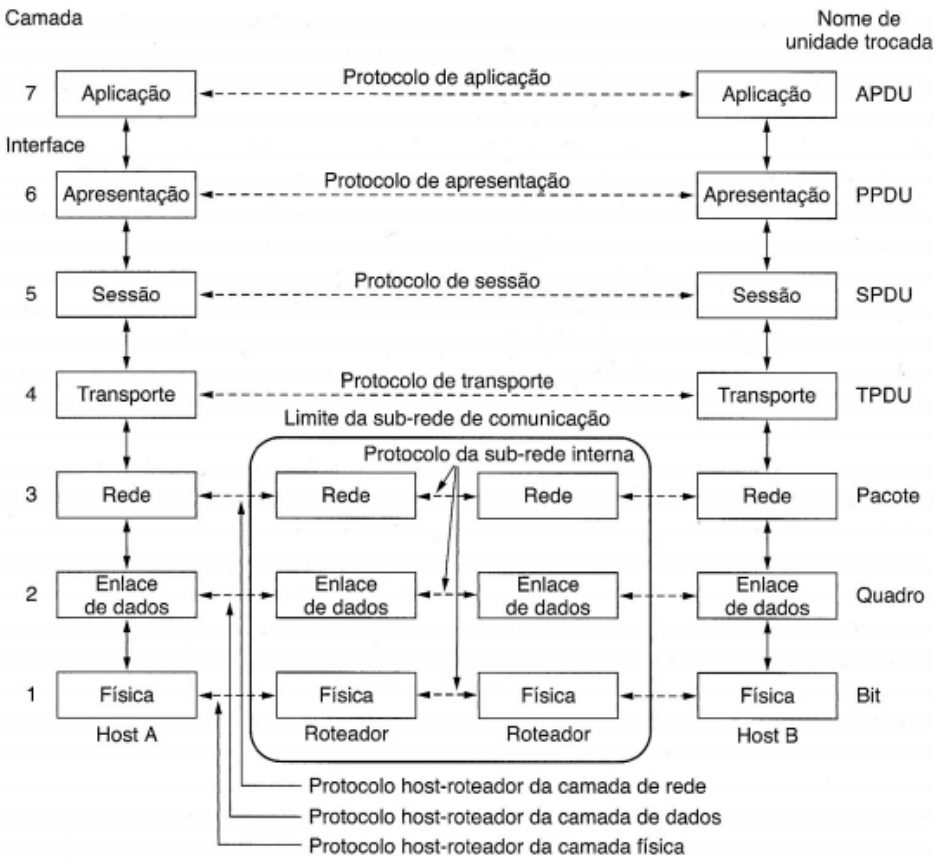
Token Ring

O protocolo Token Ring, foi criado pela IBM na década de 60 e só pode ser usado em redes que possuem uma topologia em anel. Ou seja, todos os nós devem estar ligados à dois outros nós. Nestas redes, existe uma mensagem de 3 bytes conhecida como "token" (também pode ser chamada de ficha ou bastão) que circula pela rede. Só tem permissão para enviar dados o dispositivo que está com o token. Por estes motivos, não ocorrem colisões. Caso um host não deseje se comunicar, basta passar o token para o próximo. Além disso, existe um limite de tempo que cada máquina tem para ficar com o token. Ao lado temos um exemplo de topologia em anel (ring).



Apesar de poder chegar a velocidades superiores que as redes que baseadas no CSMA/CD, o Token Ring é muito pouco usado. O motivo é o alto custo dos equipamentos necessários para manter esse modelo de rede. Até mesmo a própria IBM que desenvolveu o padrão já migrou suas redes para o padrão Ethernet, que usa CSMA/CD.

Abaixo temos uma imagem onde é possível visualizar a disposição das camadas no modelo OSI/TCP.



Noções básicas de transmissão de dados

A transmissão de informação através de sistemas de comunicação, pressupõe a passagem de sinais através dos meios físicos de comunicação que compõem as redes. As propriedades físicas dos meios de transmissão e as características dos sinais transmitidos, apresentam uma série de questões tecnológicas que influenciam na construção e no projeto de redes de computadores. O processo de comunicação envolve a transmissão da informação de um ponto a outro através de uma sucessão de processos.

Nos tópicos anteriores estudamos sobre alguns desses processos, como por exemplo os tipos de enlace e os protocolos que cada um utiliza para controlar o fluxo e evitar colisões. Agora vamos estudar os modos de transmissão.

A transmissão em um canal de comunicação entre dois dispositivos digitais pode acontecer de várias maneiras diferentes, e depende do sentido da troca, o número de unidades de dados, ou bits, enviados ao mesmo tempo e a sincronização entre o transmissor e o receptor.

Os dispositivos de rede usam **três modos** de transmissão para a troca de dados: **simplex, half duplex e full duplex**. A transmissão simplex é unidirecional e o papel de transmissor e receptor não se inverte durante o período de transmissão. A transmissão pode ser realizada para vários receptores ao mesmo tempo, porém

nesse modo o receptor não tem a alternativa de enviar um sinal confirmando o recebimento dos dados. Esse modo é mais utilizado em televisão e rádio.

No modo *half duplex* a transmissão passa a ser bidirecional e o transmissor e o receptor podem tanto transmitir, quanto receber dados, entretanto nunca simultaneamente. Podemos comparar esse modo ao funcionamento dos walkies talkies, onde apenas uma pessoa pode falar por vez, se não a comunicação se torna inviável. A transmissão *half duplex* implementa o protocolo CSMA/CD para ajudar na redução de colisões e detectar quando elas ocorrem.

Na transmissão *full duplex*, o tráfego de dados também é bidirecional e o transmissor e o receptor podem transmitir dados simultaneamente. Nesse modo a detecção de colisões é desabilitada, já que as placas de rede utilizam circuitos separados no cabo para que os quadros enviados pelos dois nós possam ser transmitidos sem nenhum problema. O modo *full duplex* também é chamado apenas de *duplex*. Para utilizar esse modo é necessário que o meio físico seja: um cabo par trançado (cross-over) ou um switch com suporte a *full duplex* ou fibra ótica.

Modos de Transmissão

A transmissão digital consiste na transferência de informações em um suporte físico de comunicação sob a forma de sinais digitais. Assim, dados analógicos deverão ser previamente digitalizados antes de serem transmitidos. Contudo, as informações digitais não podem circular na forma de 0 e 1 diretamente e é por isso que devem ser codificadas na forma de um sinal que possui dois estados como, por exemplo, dois níveis de tensão em relação à massa e a diferença de tensão entre dois fios; a presença/ausência de corrente num fio e a presença/ausência de luz.

Esta transformação da informação binária para a forma de um sinal de dois estados é realizada pelo ETCD, chamado também de decodificador de banda de base. Essa é a origem do nome transmissão da banda de base que designa a transmissão digital:

O modo de transmissão designa o número de unidades elementares de informações (bits) que podem ser transmitidas simultaneamente pelo canal de comunicação, ou seja, trata diretamente, a quantidade de bits a ser transmitida ao mesmo tempo.

Transmissão em modo Paralelo: Na transmissão em modo paralelo, os bits que compõem o carácter são enviados simultaneamente através de várias vias de dados. Uma via é, por exemplo, um fio, um cabo ou qualquer outro suporte físico. A ligação paralela dos computadores de tipo PC necessita geralmente de 10 fios. Estas vias podem ser:

N linhas físicas: neste caso, cada bit é enviado para uma linha física (é a razão pela qual os cabos paralelos são compostos de vários fios em cobertura); uma linha física dividida em vários sub-canais compartilhando a mesma banda. Assim, cada bit é transmitido numa frequência diferente.

Dado que os fios condutores estão próximos numa cobertura, existem perturbações / interferências que degradam a qualidade do sinal.

Transmissão em modo Série: Na transmissão em modo série, os bits que compõem a informação são enviados um a um através de uma única via de dados.

Dados os problemas com a transmissão paralela, é a em modo série que é mais utilizada. Entretanto, como é apenas um só fio que transporta a informação, existe um problema de sincronização entre o emissor e o receptor, ou seja, o receptor não pode a priori distinguir os caracteres (ou mesmo, de maneira mais geral, as sequências de bits) porque os bits são enviados sucessivamente. Existem então dois tipos de transmissão que permitem remediar este problema: Síncrona e Assíncrona.

Transmissão Assíncrona: No modo de transmissão Assíncrono os dados são enviados um a um sem controle de tempo entre um e outro. Agora, imagine que só um bit é transmitido durante um longo período de silêncio, onde o receptor não poderia saber que se trata de 00010000, ou 10000000 ou ainda 00000010. Para remediar este problema, cada dado é precedido de uma informação que indica o início da transmissão deste (a informação de início de emissão chama-se bit START) e termina com o envio de uma informação de fim de transmissão (chamada bit STOP, pode eventualmente haver vários bits STOPS). Normalmente utilizada quando não é estabelecido, no receptor, nenhum mecanismo de sincronização relativamente ao emissor.

Características:

Baixo Rendimento (alto overhead).

Fácil Implementação;

Baixa Velocidade;

Transmissão Síncrono: Na transmissão em modo Síncrono os dados são enviados em blocos e em intervalos de tempo definidos, dados de sincronismo são enviados durante a transmissão para manter o sincronismo entre as máquinas. O receptor recebe continuamente (mesmo quando nenhum bit é transmitido) as informações ao ritmo em que o emissor as envia. É por isso é necessário que emissor e receptor estejam sincronizados à mesma velocidade. Além disso, informações suplementares são inseridas para garantir a ausência de erros na transmissão.

Características:

Boa qualidade de transmissão;

Custo de transmissão mais elevado;

Equipamento mais sofisticado;

Ideais para transmissão de sinais sensíveis a atraso (voz, música, vídeo);

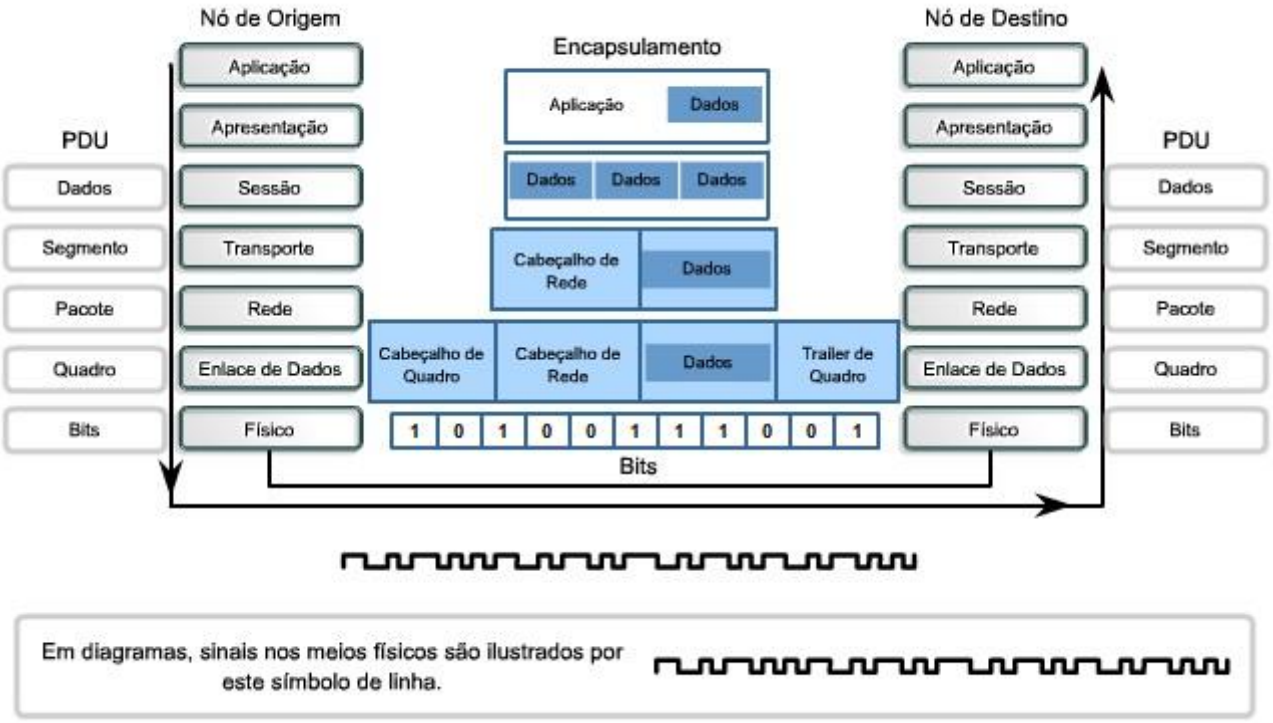
Transmissão com maior confiabilidade;

Adequado para aplicações multimídia.

APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais[4].

[4] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.



Download	Download (em português: descarregamento) significa obter (baixar) um conteúdo (um ou mais arquivos) de um servidor remoto para um computador local. Para isso são utilizados aplicativos específicos que se comunicam com o servidor através de protocolos pré-definidos. Por exemplo: os navegadores que acessam os dados de um servidor normalmente utilizando o protocolo HTTP.
URL	URL é a sigla correspondente à palavra "Uniform Resource Locator", que foi traduzida para a língua portuguesa como Localizador Uniforme de Recursos. Em outras palavras, URL é um endereço virtual com um caminho que indica onde está o que o usuário procura, e pode ser tanto um arquivo, como uma máquina, uma página, um site, uma pasta etc. Um URL é composto de um protocolo, que pode ser tanto HTTP, que é um protocolo de comunicação, FTP que é uma forma rápida de transferir arquivos na internet, etc. O formato do URL é definido pela norma RFC 1738.
SSL	SSL é a abreviação de Secure Sockets Layer, trata-se de uma ferramenta de encriptação de páginas antes de serem transmitidas pela internet que autentifica as partes envolvidas. É muito utilizada para pagamentos online com cartão de crédito. Diversas versões dos protocolos de segurança estão em uso generalizado em navegação na web, serviços de e-mail, mensagens instantâneas e VoIP. Resumindo o SSL torna a conexão segura. Veja a figura ao lado.
Backbone	Os backbones são as espinhas dorsais do tráfego da Internet. É o ponto inicial de referência da Internet, o setor que interliga todos os pontos da rede. Os backbones são pontos das

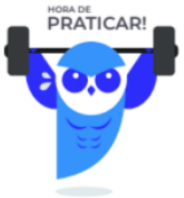
	redes que compõem o núcleo das redes de Internet. São pontos chave da Internet que distribuem pelas redes as informações baseadas na tecnologia TCP/IP.

Imprima o capítulo Aposta Estratégica separadamente e dedique um tempo para absolver tudo o que está destacado nessas duas páginas. Caso tenha alguma dúvida, volte ao Roteiro de Revisão e Pontos do Assunto que Merecem Destaque. Se ainda assim restar alguma dúvida, não hesite em me perguntar no fórum.

QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.



1. (CESPE / EBSERH – 2018)

Julgue o próximo item, em relação aos conceitos da arquitetura cliente-servidor e de Internet e intranet.

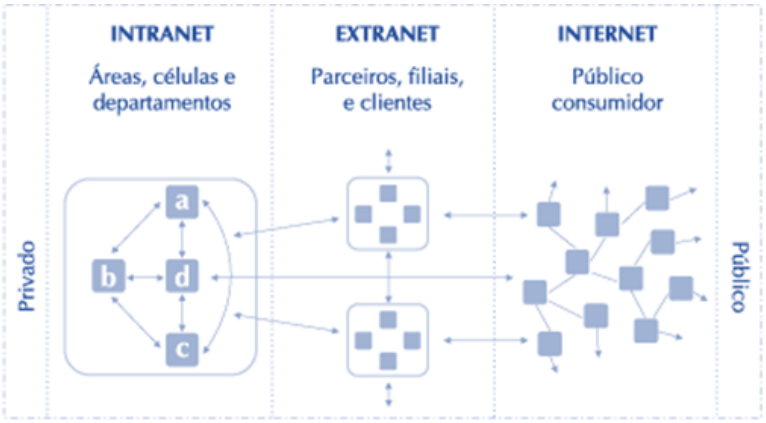
A intranet é uma rede de equipamentos que permite acesso externo controlado, para negócios específicos ou propósitos educacionais, sendo uma extensão da rede local de uma organização, disponibilizada para usuários externos à organização.

Comentários

Na aula apresentei uma tabela comparando Internet e Intranet. Nela é possível ver que apenas a Internet possui comunicação externa. A definição descrita na assertiva se aproxima mais do conceito de Extranet. Uma Extranet é uma rede de computadores que permite acesso externo controlado, para negócios específicos ou propósitos educacionais. Em um contexto de *business-to-business*, uma Extranet pode ser vista como uma extensão de uma intranet da organização que é estendida para usuários externos à organização, geralmente parceiros, vendedores e fornecedores, em isolamento de todos os outros usuários da Internet. Portanto, assertiva incorreta.

O acesso à Extranet, via de regra, pode ocorrer de duas formas: ou por meio de um acesso exigindo usuário e senha, para garantir a autenticidade do usuário, ou ainda por uma rede privada virtual (VPN), que, em termos práticos, cria uma conexão segura tunelada entre o dispositivo fora da Intranet e a Intranet propriamente dita.

Complementando, observe a figura abaixo que mostra um pouco da lógica que interliga os conceitos de intranet, internet e extranet.



Gabarito: errado.

---

2. (CESPE / EBSERH – 2018)

Julgue o próximo item, em relação aos conceitos da arquitetura cliente-servidor e de Internet e intranet.

A Internet foi projetada para ser altamente tolerante a falhas, continuando a transmitir o tráfego mesmo no caso de ocorrer ataques nucleares em várias partes da rede de computadores.

Comentários

Apesar da assertiva ser extravagante, citando inclusive ataques nucleares, ela está correta. Conforme vimos na aula, a Internet surgiu a partir de um projeto militar do governo norte-americano, que no período da Guerra Fria queria desenvolver um sistema em que os computadores das bases militares pudessem trocar informações entre si e que mesmo em caso de ataque nuclear os dados fossem preservados. Até hoje este o modelo (princípio) é mantido e as informações são armazenadas em diferentes servidores distribuídos pelo mundo.

Gabarito: certo.

---

3. (CESPE / TRT - 7ª Região (CE) – 2017)

Assinale a opção correta a respeito dos conceitos de Internet e intranet.

a) Os serviços disponibilizados na intranet de uma corporação nunca estão disponíveis a usuários que não estejam diretamente usando tal rede.

b) Uma intranet pode ser construída simplesmente pelo uso de endereços IP em uma rede na qual se compartilhem recursos.

c) Entre as ferramentas necessárias para o uso da Internet estão os browsers.

d) Embora tenha público restrito, a intranet de uma corporação pode ser ligada à Internet.

Comentários

Vamos analisar cada uma das alternativas para encontrar a correta e entender porque as outras estão erradas.

a) O termo "nunca" restringe a alternativa e se opõe a alternativa D. Logo, temos uma alternativa errada. Lembrando que a ***Intrantet*** é de uso ***restrito*** a seus membros. Uma intranet pode conectar empregados de uma empresa que trabalham em escritórios diferentes ou pode facilitar a logística de pedidos justamente por interligar diferentes departamentos de uma mesma empresa em uma mesma rede.

b) Conforme vimos na aula, a intranet possui muitos outros componentes além do endereço IP. Além desta característica, uma intranet é uma rede **privada**, pertencente a uma organização, **de acesso restrito a seus membros**, que **utiliza os mesmos padrões e protocolos da Internet**, tais como http, tcp, ip, smtp, pop3, etc. **Errada**.

c) O termo "necessárias" condiciona o uso da Internet aos browsers, o que não é verdade. O browser é um ***programa*** desenvolvido para permitir a **navegação** pela Web, capaz de interpretar diversas linguagens, como HTML, ASP, PHP. **Errada**.

d) A alternativa afirma que é possível que uma intranet esteja conectada à Internet. Não restringe a obrigatoriedade, mas diz que é possível. Correta.

Gabarito: alternativa D.

---

4. (CESPE / Prefeitura de São Luís – MA – 2017)

A humanidade vem passando por um processo de revolução tecnológica sem precedentes em sua história cujo maior exemplo é o advento da Internet. A respeito da Internet e dos aspectos a ela relacionados, assinale a opção correta.

a) As informações pessoais disponibilizadas na Internet são de domínio privado e seu acesso por aplicativos é proibido.

b) A Internet, embora tenha impactado as relações sociais, manteve inalteradas as formas de consumo.

c) A utilidade da Internet à pesquisa é restrita, por causa da quantidade de informações falsas disponibilizadas na rede.

d) Com a Internet, uma nova modalidade de contravenção surgiu: o cybercrime, que se manifesta nas ações dos hackers.

e) A Internet é acessível às diferentes classes sociais dos mais diversos países.

Comentários

Essa questão é uma pegadinha do CESPE e existe uma confusão em relação à definição de hacker e cracker. Apesar de o CESPE não fazer distinção entre as duas palavras, utilizando apenas hacker para definir o indivíduo que invade sistemas, seja para benefício ou maleficio, é importante sabermos que existe diferença.

De uma forma geral, hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Ou seja, hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos. No entanto, os crackers têm como prática a quebra da segurança de um software de forma ilegal, para causar algum dano. O termo "cracker" nasceu em 1985, e foram os próprios hackers que disseminaram o nome em sua própria defesa. A ideia era que eles não fossem mais confundidos com pessoas que praticavam o roubo ou vandalismo na internet.

Agora vamos analisar cada uma das alternativas para encontrar a correta e entender porque as outras estão erradas.

a) A Internet é a rede mundial de computadores que tem como característica ser pública. Além disso, seu acesso é realizado através dos navegadores web, que são aplicativos. Errada.

b) Os sites de comércio eletrônico revolucionaram as formas de consumo. Errada.

c) A pesquisa na Internet é um dos principais meios para se obter informações. Errada.

d) Correta.

e) Apesar de estar acessível as diferentes classes, sabemos que nem todos os países possuem esse acesso. Errada.

Gabarito: alternativa D.

---

5. (CESPE / SEDF – 2017)

Com relação aos conceitos básicos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados à Internet e à intranet, julgue o próximo item.

Embora exista uma série de ferramentas disponíveis na Internet para diversas finalidades, ainda não é possível extrair apenas o áudio de um vídeo armazenado na Internet, como, por exemplo, no Youtube (http://www.youtube.com).

Comentários

Existem inúmeros sites e complementos para os navegadores que possibilitam a ação tanto de download do vídeo como apenas do áudio. Portanto, assertiva incorreta.

Gabarito: errado.

---

6. (CESPE / SEDF – 2017)

Com relação aos conceitos básicos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados à Internet e à intranet, julgue o próximo item.

É correto conceituar intranet como uma rede de informações internas de uma organização, que tem como objetivo compartilhar dados e informações para os seus colaboradores, usuários devidamente autorizados a acessar essa rede.

Comentários

Conforme vimos na aula, a Intranet surgiu a partir da necessidade das organizações em ter uma rede privada, acessível apenas por membros da organização, empregados ou terceiros com autorização de acesso. Seguindo os mesmos padrões da Internet, a Intranet é baseada em protocolos TCP / IP, possibilitando o compartilhamento de informações e reduzindo os custos. Portanto, a assertiva está correta.

Gabarito: certo.

---

7. (CESPE / SEDF – 2017)

Com relação aos conceitos básicos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados à Internet e à intranet, julgue o próximo item.

Cookies são arquivos enviados por alguns sítios da Internet aos computadores dos usuários com o objetivo de obter informações sobre as visitas a esses sítios; no entanto, o usuário pode impedir que os cookies sejam armazenados em seu computador.

Comentários

Cookies são arquivos criados a partir da troca de informações entre os sites visitados e o navegador com o intuito de armazenar informações de navegação, como preferências, hábitos e/ou informações do perfil. É possível desabilitar em cada navegador o armazenamento destas informações. Portanto, assertiva correta.

Gabarito: certo.

---

8. (CESPE / TCE-PA – 2016)

A respeito dos conceitos básicos de Internet e intranet, protocolos, ferramentas e aplicativos, julgue os itens seguintes.

Diferentemente do HTTP, o protocolo de transferência de arquivos (FTP) utiliza duas conexões paralelas em portas distintas com o servidor: uma porta para a conexão de controle e outra para a conexão que viabiliza a transferência de dados.

Comentários

O protocolo FTP utiliza duas portas para estabelecer a comunicação. A porta 20 para transferência de dados e a porta 21 para conexão e controle. Portanto, a assertiva está correta.

As portas dos protocolos funcionam como portas de casas ou apartamentos, onde apenas pessoas autorizadas podem ter acesso. Como na Internet trafegam incontáveis dados, cada dado enviado possui uma "marca" com o tipo de protocolo e a porta para onde ele deve ser direcionado/enviado. Assim, cada dado é enviado especificamente pela porta onde ele tem acesso/autorização.

Gabarito: certo.

---

9. (CESPE / INSS – 2016)

O próximo item, que abordam procedimentos de informática e conceitos de Internet e intranet, apresenta uma situação hipotética, seguida de uma assertiva a ser julgada.

A área administrativa do INSS informou a todos os servidores públicos lotados nesse órgão que o acesso a determinado sistema de consulta de dados cadastrais seria disponibilizado por meio da Internet, em substituição ao acesso realizado somente por meio da intranet do órgão. Nessa situação, não haverá similaridade entre os sistemas de consulta, porque sistemas voltados para intranet, diferentemente dos voltados para Internet, não são compatíveis com o ambiente Web.

Comentários

Vimos na aula que a intranet utiliza os mesmos protocolos que a Internet e é baseada em protocolos TCP/IP. Portanto, a assertiva está incorreta. ***Intranet*** é uma rede **privada**, pertencente a uma empresa (ou a uma residência), de **acesso restrito** a seus membros, que utiliza os **mesmos padrões e protocolos da Internet**, tais como *http, tcp, ip, smtp, pop3*, etc. Assim, os mesmos programas utilizados na Internet **podem também** ser aplicados à Intranet, e vice-versa.

Gabarito: errado.

---

10. (CESPE / INSS – 2016)

Com relação a informática, julgue o item que se segue.

Na Internet, os endereços IP (Internet Protocol) constituem recursos que podem ser utilizados para identificação de microcomputadores que acessam a rede.

Comentários

O Endereço de Protocolo da Internet (ou simplesmente Endereço IP), é um rótulo numérico atribuído a cada dispositivo conectado a uma rede. Esse endereço é único e pode identificar um computador conectado à rede. Portanto, a assertiva está correta.

Gabarito: certo.

---

11. (CESPE / Prefeitura de São Paulo – SP – 2016)

Com relação a redes de computadores, assinale a opção correta.

a) Computadores que utilizam o Linux não acessam computadores que usam o Windows, pois, em uma rede de computadores, não é possível a conexão entre sistemas operacionais diferentes.

b) Para a implantação de uma rede de computadores, são necessários, no mínimo, um computador servidor e quatro computadores clientes.

c) Access point é um dispositivo usado para a conexão de computadores em uma rede sem fio.

d) Para garantir o acesso de um computador a uma rede local, é suficiente conectar a placa de rede, dispensando-se qualquer tipo de configuração do usuário e do administrador de rede.

e) LAN (local area network) é uma rede que conecta computadores localizados a, no máximo, dez metros de distância do servidor e fisicamente próximos uns aos outros.

Comentários

Vamos analisar todas as alternativas.

a) Não existe impedimento para sistemas operacionais diferentes acessarem a mesma rede e inclusive compartilharem arquivos. Isso é possível graças ao protocolo TCP/IP. Errada.

b) Para implantar uma rede basta existir dois equipamentos, que não necessariamente precisam ser um computador servidor e um computador cliente. Pode ser uma rede WiFi onde existe o roteador ou *access point* e qualquer dispositivo que faça conexão com esta rede (notebook, celular, tablet). Errada.

c) Como explicamos na alternativa anterior e vimos na aula, um Access Point é um dispositivo que cria uma rede sem fio onde os computadores podem se conectar. Correta.

d) É necessária a instalação dos drivers (software) da placa para que ela funcione corretamente. Errada.

e) Apesar de serem redes locais, as LANs podem ter um alcance de mais de 10 metros. Errada.

Gabarito: alternativa C.

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

1) **Como as redes de computadores são classificadas? E quais as principais características de cada classificação?**

2) **O que são e quais os modelos de arquitetura?**

3) **Qual a diferença entre internet e intranet?**

4) **O que é um firewall?**

5) **Qual a diferença entre um Roteador e um Switch?**

6) **O que é um protocolo?**

7) **Quais os principais protocolos da internet?**

8) **O que seria WEP, WPA e WPA2? Qual deles é o mais seguro?**

Perguntas com respostas

1) Como as redes de computadores são classificadas? E quais as principais características de cada classificação?

De modo geral, as redes são classificadas em Rede Local (LAN), Rede Metropolitana (MAN) e Rede de Longa Distância (WAN). Dentro dessas classificações surgem alguns ramos direcionados para as redes sem fio. Além disso, duas outras classificações também são muito cobradas em concursos públicos, a Rede de Área de Armazenamento (SAN) por conta do Cloud Storage e a Rede de Área Pessoal (PAN) por conta da Internet das Coisas (do inglês, Internet of Things, IoT) e das conexões de pequenas distâncias para compartilhar e controlar dispositivos.

2) O que são e quais os modelos de arquitetura?

A arquitetura das redes de computador é formada por níveis, interfaces e protocolos. Cada nível oferece um conjunto de serviços através de uma interface ao nível superior, usando funções realizadas no próprio nível e serviços disponíveis nos níveis inferiores. Os modelos são TCP/IP e OSI.

3) Qual a diferença entre internet e intranet?

A definição de Internet é um conglomerado de redes locais (de computadores), espalhadas pelo mundo, que torna possível a interligação entre os computadores. Ou de forma mais simples é a rede mundial de computadores. Já intranet é uma rede privada, pertencente a uma empresa, de acesso restrito a seus membros, que utiliza os mesmos padrões e protocolos da Internet.

4) O que é um firewall?

Firewall (em português: parede de fogo) é uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet, através de uma política de segurança. Seu objetivo é permitir que somente dados autorizados sejam transmitidos e/ou recebidos.

5) Qual a diferença entre um Roteador e um Switch?

Roteador é o equipamento que interliga diferentes redes de computadores, encaminhando os dados entre as elas. Quando um pacote de dados chega, em uma de suas linhas, o roteador lê a informação de endereço para determinar o seu destino final. Em seguida, usando essa informação na tabela de roteamento ou encaminhamento, ele direciona o pacote para a rede seguinte até o destino final. Já o switch tem como função conectar diversos computadores em uma rede. Além de computadores é possível ligar roteadores, impressoras e qualquer outro dispositivo com as mesmas características técnicas de comunicação (com porta de rede). O switch cria uma série de canais exclusivos em que os dados do dispositivo de origem são recebidos somente pelo dispositivo de destino.

6) O que é um protocolo?

Protocolo é o conjunto de regras que definem o modo como se dará a comunicação entre dispositivos conectados em uma rede.

7) Quais os principais protocolos da internet?

HTTP (acessar páginas Web), FTP (transferir arquivos), SMTP (enviar e-mails), POP3 (receber e-mails), IMAP4 (receber e-mails).

8) O que seria WEP, WPA e WPA2? Qual deles é o mais seguro?

São algoritmos de segurança para as redes WiFi. WEP - é a sigla de Wired Equivalent Privacy, que foi o algoritmo de segurança mais usado do mundo, criado em 1999 e que é compatível com praticamente todos os dispositivos Wi-Fi disponíveis no mercado. Por conta da sua popularidade, logo foram descobertas falhas de segurança e por isso acabou se tornando um algoritmo inseguro. Oficialmente, o WEP não é considerado um padrão desde 2004, quando a Wi-Fi Alliance — associação que certifica produtos sem fio e promove a tecnologia — encerrou o suporte a ele. WPA - é a sigla para Wi-Fi Protected Access. Foi o algoritmo que substituiu o WEP tornando-se o protocolo-padrão da indústria, a partir de 2003. Como ele foi criado de forma a não tornar os dispositivos WEP obsoletos, uma série de elementos do protocolo antigo foi reaproveitada e, com ela, diversos dos problemas do antecessor também acabaram presentes na nova versão. Por este motivo, foi criada uma versão mais segura, a WPA2. WPA2 - É a sigla para a mais nova versão do WPA e também é o sistema-padrão atual, implementado pela Wi-Fi Alliance em 2006. A grande diferença está na maneira como o sistema processa as senhas e os algoritmos de criptografia. Entre eles o mais seguro é o WPA2.

...

Forte abraço e bons estudos!

"Hoje, o 'Eu não sei', se tornou o 'Eu ainda não sei'"

(Bill Gates)

Thiago Cavalcanti

Face: www.facebook.com/profthiagocavalcanti
Insta: www.instagram.com/prof.thiago.cavalcanti

YouTube: youtube.com/profthiagocavalcanti

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.