Estratégia Concursos

Aula 00

CGM Fortaleza - Passo Estratégico de Noções de Informática - 2024 (Pós-Edital)

Autor:
Thiago Rodrigues Cavalcanti

21 de Outubro de 2024

1. Conceito de internet e intranet. 2. Conceitos e modos de utilização de tecnologias, ferramentas, aplicativos e procedimentos associados à internet/intranet

Sumário

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

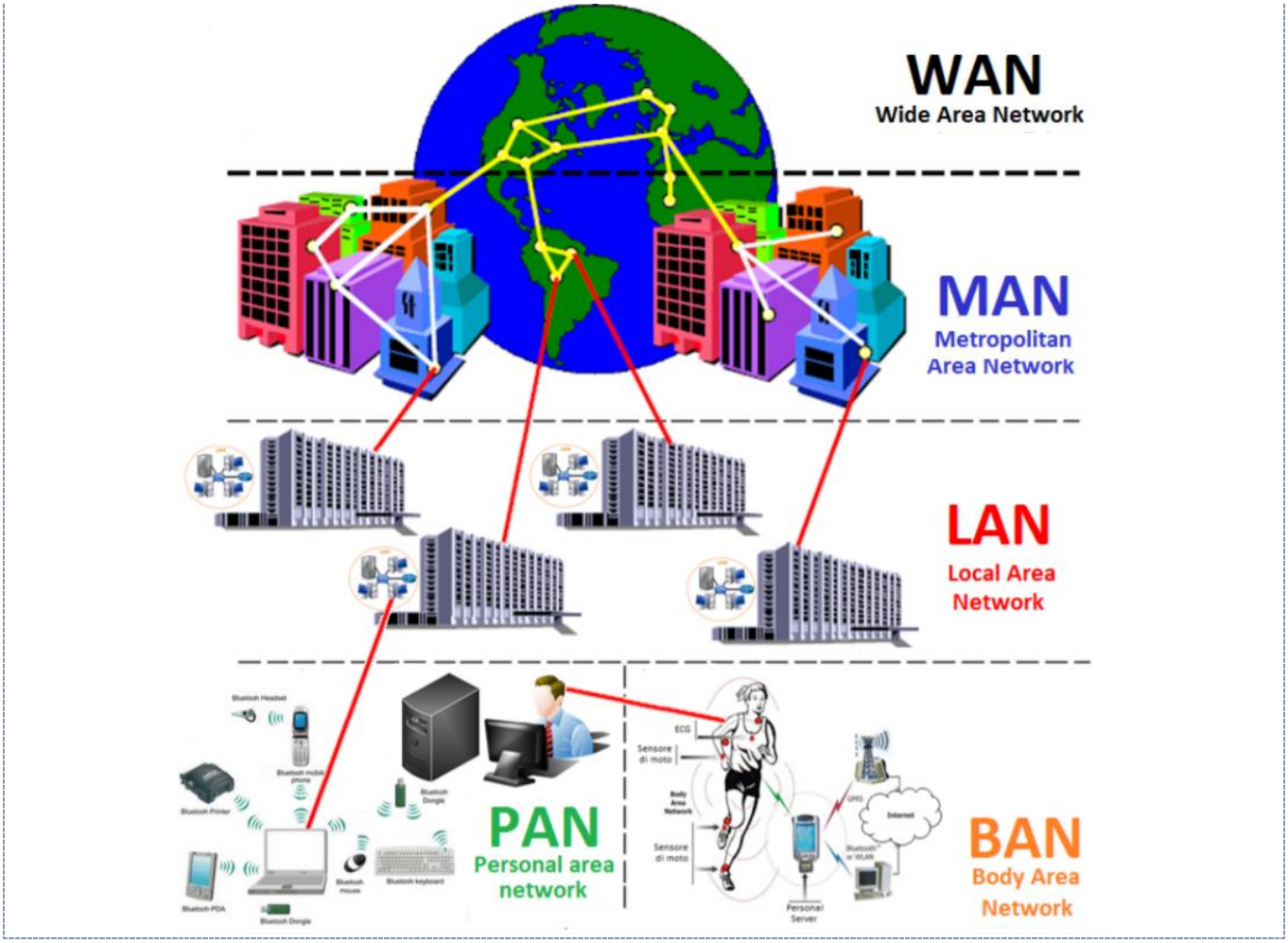
É importante entendermos que as redes de comunicação atualmente envolvem tanto telecomunicação quanto computação, e possuem como principal finalidade suprir a necessidade humana de **se comunicar à distância**. Essa necessidade surgiu desde os primórdios da humanidade e passou por diversos modelos de 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.

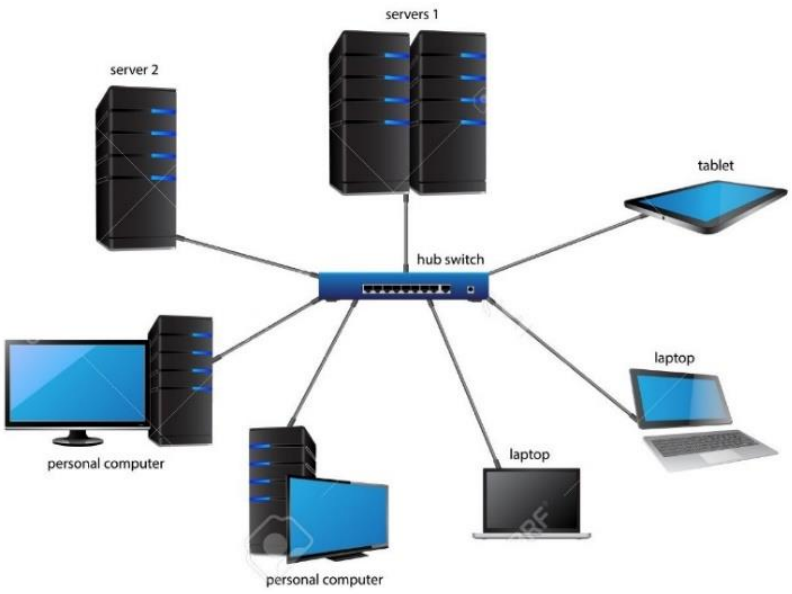
Com a crescente demanda e uso de computadores em universidades e laboratórios de pesquisa no final da década de 1960, houve a necessidade de fornecer interconexões de alta velocidade entre sistemas de computadores. No final da década de 1970 foram formadas as primeiras LANs, que eram usadas para criar 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

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

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 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.

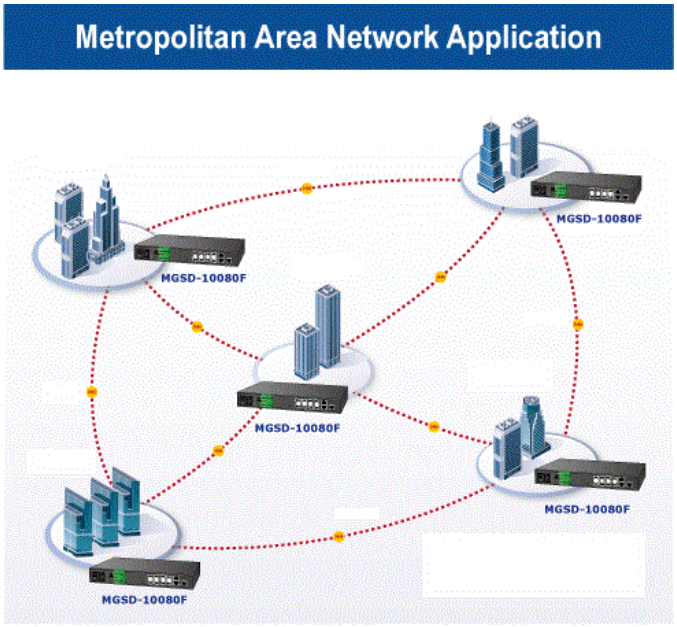
Estações são os clientes da rede que se conectam aos servidores para obter os serviços e as funções mencionadas acima. Geralmente são os computadores, notebooks, tablets e celulares.

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].

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

WAN

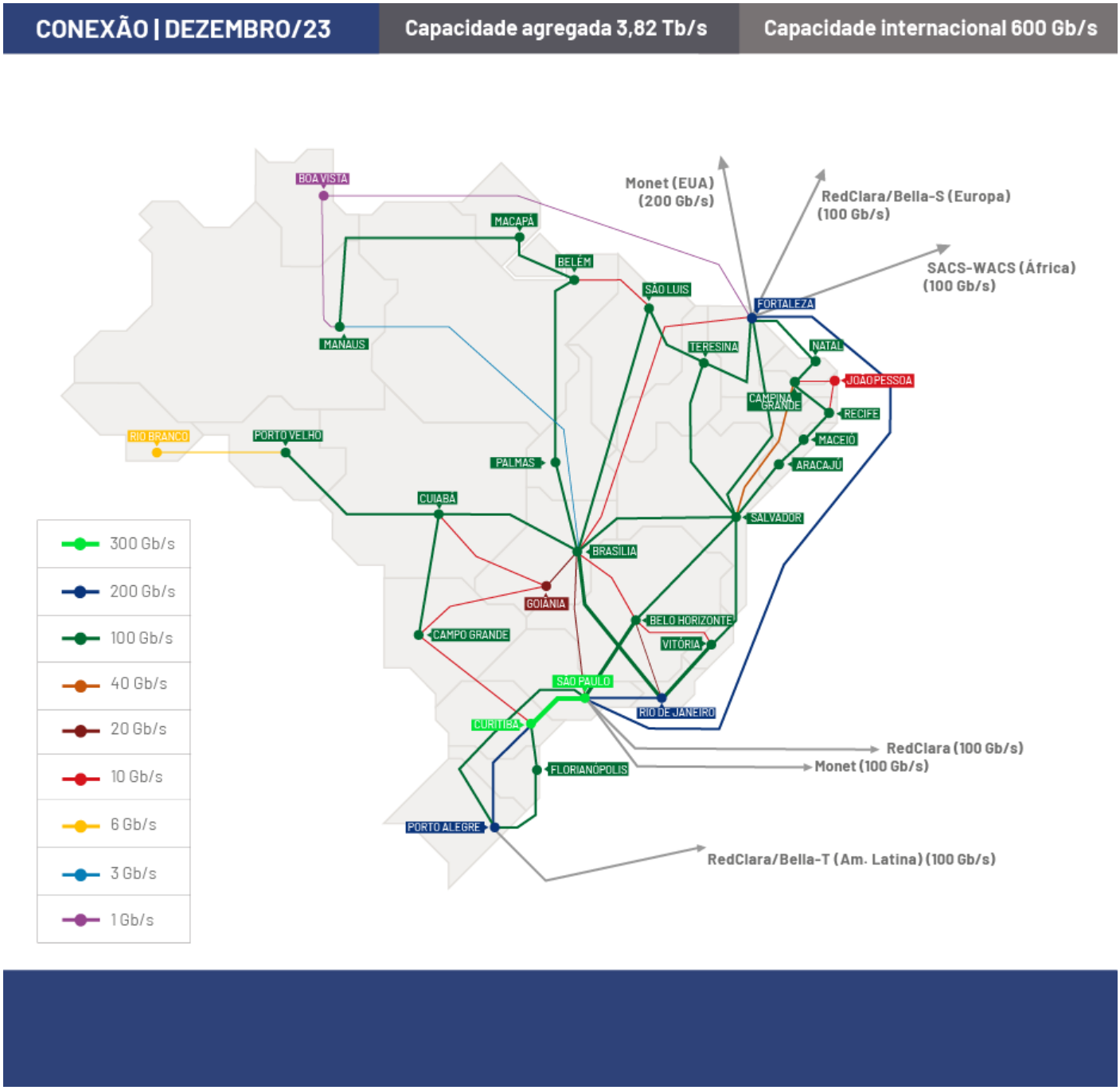
O último destaque na classificação das redes, são as redes de longas distâncias que permitem a interligação de redes locais em países ou até continentes diferentes, numa grande área geográfica. A Internet é classificada como uma WAN.

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.



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.

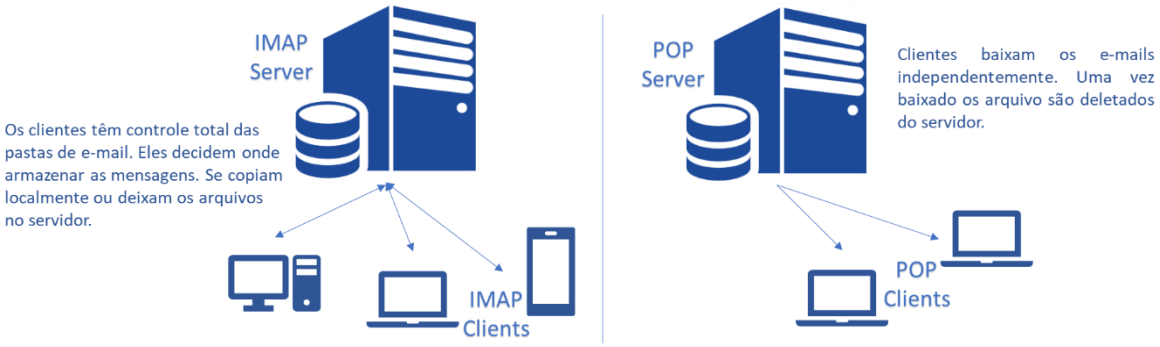
Download: Download (em português: descarregamento) significa obter (baixar) um conteúdo (um ou mais arquivos) de um servidor remoto para um computador local. Para isso são utilizados aplicativos específicos que se comunicam com o servidor através de protocolos pré-definidos. Por exemplo: os navegadores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

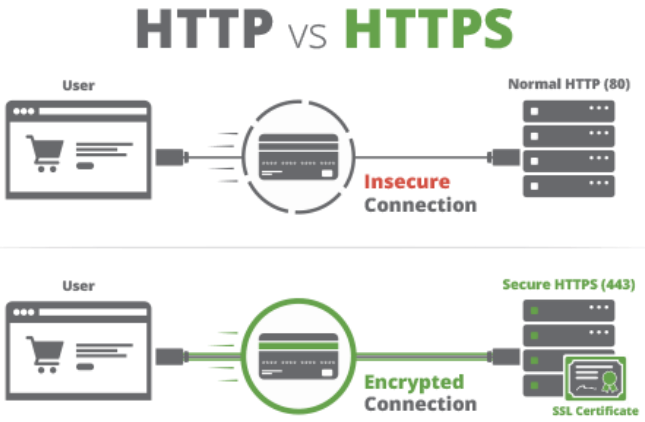
Portal: Um portal é um site da Internet projetado para aglomerar e distribuir conteúdo de diferentes fontes de maneira uniforme, sendo um ponto de acesso para uma série de outros sites pertencentes ou não ao mesmo domínio. Um exemplo de portal é o g1.globo.com. A partir dele você pode acessar os sites 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

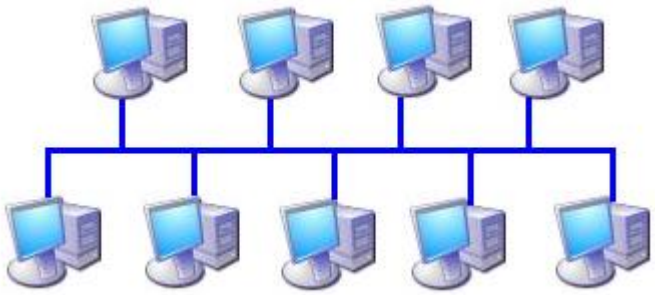
O termo topologia ou mais especificamente topologia da rede, diz respeito ao layout físico da rede, ou seja, como os computadores, cabos e outros componentes estão ligados na rede. Topologia é o termo padrão que muitos profissionais usam quando se referem ao design básico da rede.

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.



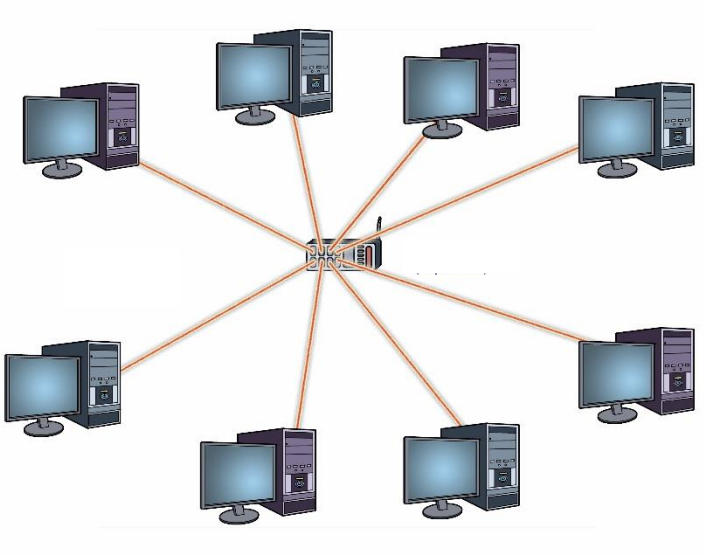
Os computadores em uma rede de topologia de barramento comunicam-se endereçando os dados a um computador em particular e inserindo estes dados no cabo sob a forma de sinais eletrônicos. Os computadores se comunicam em um barramento, segundo três conceitos: envio do sinal, repercussão do sinal e terminador.

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.

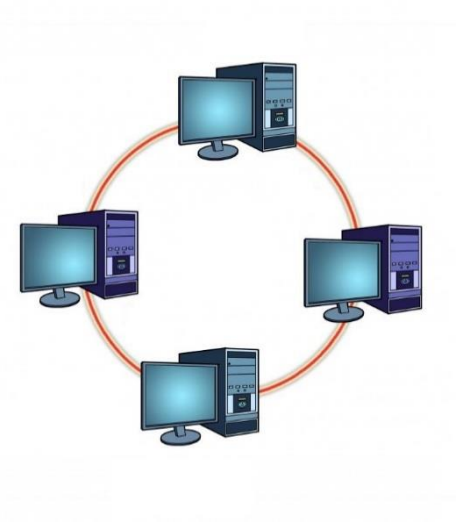
Estrela



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.

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.

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.

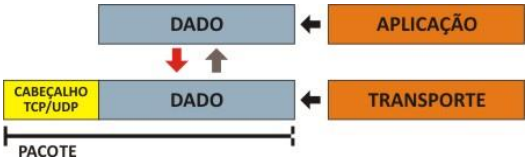
Os protocolos da camada de transporte também podem assegurar uma comunicação confiável entre os hosts, realizando controle de fluxo (taxa de transmissão de dados) e detecção de erros, além de permitir o reenvio de dados quando são perdidos ou descartados.

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.

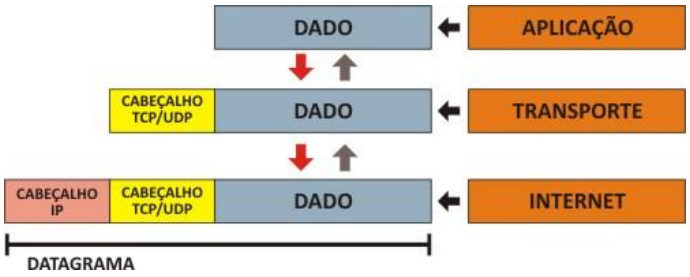


Camada de Internet / Rede

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).**

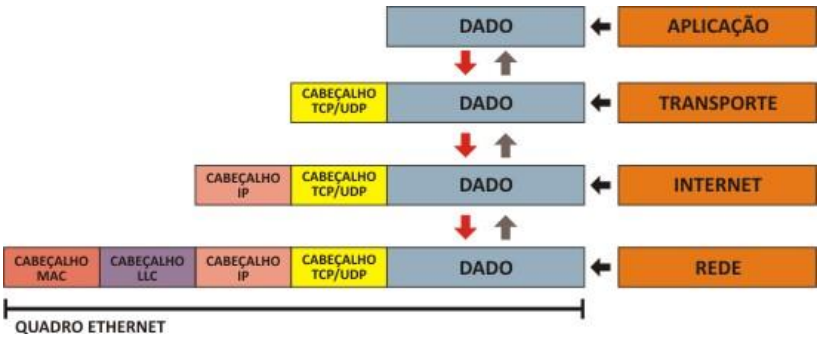


Camada de Interface com a Rede

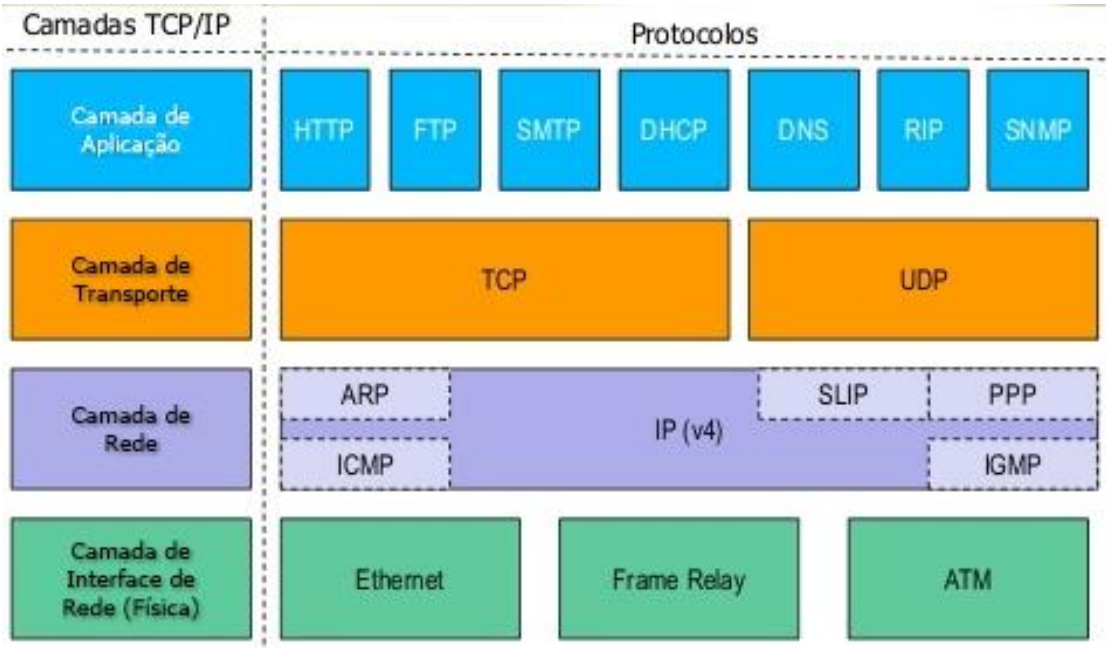
Os datagramas gerados na camada Internet são enviados para a camada Interface com a Rede, durante a transmissão de dados, ou a camada de Interface com a Rede pegará os dados da rede e os enviará para a camada de Internet, na recepção dos dados.

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.

TOME NOTA!

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.

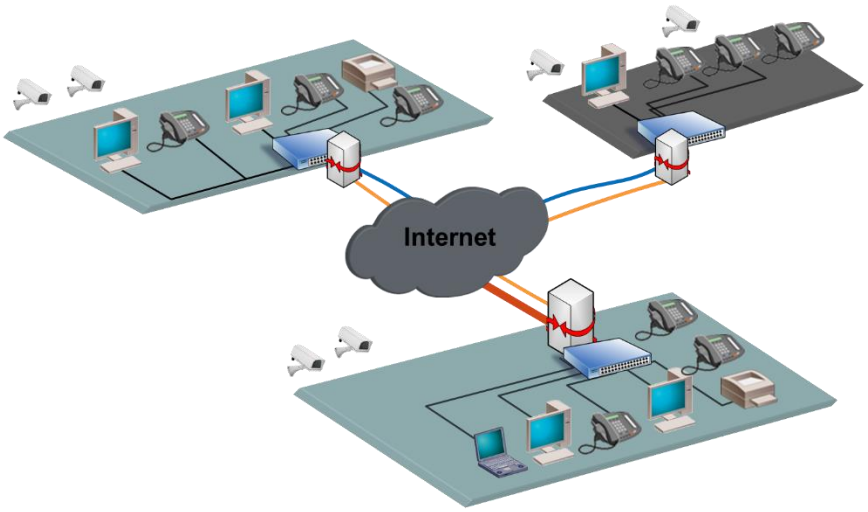
Internet

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.

Uma rede de computadores é formada a partir de 2 (dois) ou mais computadores interligados com a finalidade de compartilhar informações. Ao definir a Internet como “rede mundial de computadores”, significa que diversas redes de computadores estão interconectadas e espalhadas por todo o mundo.

Infraestrutura e Funcionamento

Nesse modelo é importante você saber que através da Internet não somente computadores, mas também diferentes dispositivos podem se comunicar. Estes dispositivos, também chamados hosts, podem estar conectados em redes diferentes que inicialmente não teriam comunicação entre si. Para poder se comunicar, cada host recebe um endereço único, parecido com os números de telefone. Assim, como qualquer telefone no mundo todo é único (considerando o código do país e o DDD), cada dispositivo ligado a Internet possui um número único, que é chamado de endereço IP ou número IP.



Na figura podemos observar o papel da Internet fazendo a interligação entre diferentes redes, com diferentes dispositivos (hosts), localizados em qualquer parte do mundo. Para realizar estas conexões existem diversos equipamentos distribuídos em todo o mundo. Vamos destacar alguns destes equipamentos:

- **Roteador**

O 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. Na Internet existem vários tipos de roteadores para fazer a rede funcionar da forma mais eficiente.

- **Hub e Switch**

Estes equipamentos têm 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). A principal diferença entre eles está na forma como transmitem os dados entre os computadores. Enquanto os hubs reúnem o tráfego em somente uma via, o switch cria uma série de canais exclusivos em que os dados do dispositivo de origem são recebidos somente pelo dispositivo de destino.

- **Modem**

A palavra Modem origina-se da junção de duas palavras, modulador e demodulador. É um dispositivo eletrônico que modula um sinal digital em uma onda analógica, para ser transmitido através da linha telefônica, e que na extremidade de destino demodula o sinal analógico convertendo para o formato digital original.

A técnica utilizada por estes equipamentos listados é conhecida como comutação de pacotes, em contraste com a comutação de circuitos que é utilizada nos sistemas telefônicos. Na comutação de pacotes, as mensagens que serão transmitidas são fragmentadas em pacotes menores, que viajam na Internet de forma independente uns dos outros. Ao chegar ao destino as informações são reagrupadas formando a mensagem original.

Caminhos da internet

Já sabemos que a Internet é a rede mundial de computadores. Contudo, precisamos entender que os dados trafegam por alguns pontos distintos e importantes na estrutura antes de chegar à nossa casa.

- **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.

- **Provedor de Acesso**

A partir dos *backbones*, o sinal da Internet passa aos **provedores de acesso**, que são as empresas que contratam o sinal de *backbones* para distribuir aos seus usuários. Em geral, são empresas ligadas ao setor de telecomunicações, ou são as próprias companhias telefônicas que fornecem acesso à Internet através de planos acordados com seus usuários.

- **Provedor de Serviço**

Os dados de Internet que irão trafegar na rede precisam de um meio para seu transporte até os usuários, e são as empresas provedoras de serviço as responsáveis por este papel. Estas empresas recebem os dados do provedor de acesso e distribuem aos usuários por variados meios (via rádio, fibra ótica, etc.). São empresas que devem ser regulamentadas pela Anatel (Agência Nacional de Telecomunicação) e podem ser prestadores de serviço de rede, companhias telefônicas e empresas de telecomunicação.

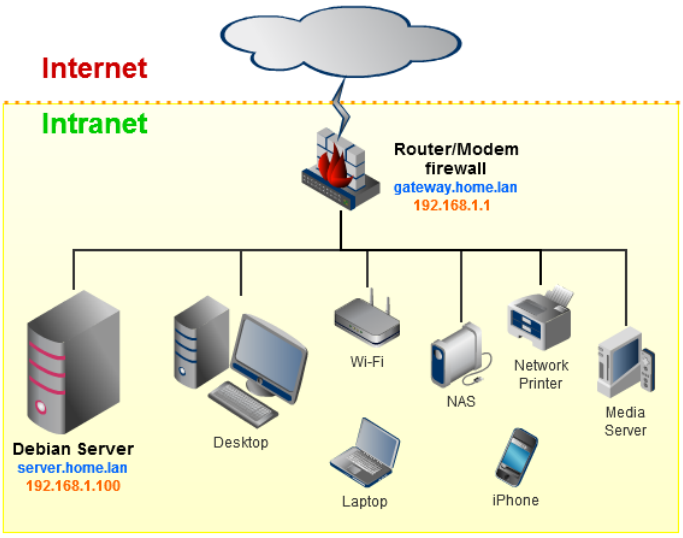
Agora sim, vamos entender qual o caminho que a Internet faz até chegar na sua casa. Este caminho passa por quatro passos principais, sempre identificados por um endereço de IP: o Backbone, o provedor de acesso, o provedor de serviço e o usuário final. Veja a figura abaixo.

Intranet

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 também é baseada em protocolos TCP/IP (HTTP, HTTPS, FTP, SMTP, POP3, IMAP e outros), possibilitando o compartilhamento de informações e reduzindo os custos.

A Intranet muitas vezes confunde-se com a Internet. Embora existam muitas semelhanças entre elas, na realidade são dois conceitos diferentes. Simplificando, a Internet é a rede mundial de computadores, enquanto a Intranet é uma Internet privada que opera dentro de uma organização. Seguindo a classificação das redes de computadores, podemos entender que a Intranet é uma LAN (*Local Area Network*).

O principal objetivo da Intranet é **compartilhar informações sobre a organização e recursos de computação** (sistemas, e-mails e a própria Internet) entre os utilizadores.



Na figura acima podemos visualizar um exemplo de Intranet. A linha preta é a conexão da rede com a Internet, porém todos os dispositivos que estão apresentados após o equipamento denominado modem, fazem parte da Intranet.

Para você ficar bom nesse assunto, observe a tabela abaixo onde podemos ver um comparativo entre o que a Internet e a Intranet podem disponibilizar.

RECURSO	INTERNET	INTRANET
Acesso restrito		✓
Comunicação instantânea	✓	✓
Comunicação externa	✓	
Compartilhamento de impressoras		✓
Compartilhamento de dados	✓	✓
Rede local (LAN)		✓

É importante destacar que é possível que a Intranet de uma organização esteja conectada à Internet. Inclusive, esta é a regra geral, embora existam Intranets desconectadas da Internet. Normalmente, as organizações impõem uma política restritiva de comunicação entre a Intranet e a Extranet, permitindo o acesso à Internet pelos computadores da Intranet, mas protegendo os serviços da Intranet, para que não sejam acessados por terceiros na Internet. Quem já trabalhou em uma Intranet certamente se viu em uma máquina com acesso à Internet.

IP (Internet Protocol)

Internet Protocol ou Protocolo de Internet é a junção de dois termos: Inter que significa entre e net que significa rede. Sendo assim, Internet significa entre redes. O IP é um protocolo para comunicação entre redes.

Fazendo uma analogia com os Correios, o IP seria como o motorista de entregas. Ele é aquele cara que já dirigiu pelo Brasil inteiro e conhece as melhores rodovias e rotas para entregar os pacotes aos seus destinatários. Porém, ele não garante a entrega dos pacotes, porque ele pode pegar um congestionamento na estrada, pode ser assaltado, entre outras situações.

Seguindo com nossa analogia, para enviar uma carta pelos Correios era necessário pegar um papel, escrever o conteúdo e colocar dentro de um envelope, com endereço de origem e endereço de destino. Na Internet, as informações que transmitidas são encapsuladas dentro de um "envelope" chamado Pacote IP que contém necessariamente um endereço IP de origem e um endereço IP de destino.

O endereço IP define de forma única e universal a conexão de um dispositivo. Eles são exclusivos no sentido em que cada endereço define uma única conexão com a Internet – dois dispositivos jamais podem ter o mesmo endereço ao mesmo tempo. Além disso, eles são universais, onde o sistema de endereçamento tem de ser aceito por qualquer host que queira se conectar à Internet.

Agora vamos falar um pouquinho sobre endereçamento e versões. Da mesma forma que um carteiro precisa saber o CEP de uma casa, o protocolo IP precisa saber o endereço IP de um host para entregar os dados destinados a ele.

Endereçamento

Existem duas notações predominantes de endereço IP: Octetos Binários ou Decimal Pontuada. Basicamente ele possui 32 bits de comprimento (Versão 4). Esses 32 bits geralmente são divididos em 4 octetos. Um octeto é um conjunto de 8 bits ou 1 byte.

Endereço IP com notação de Octetos Binários			
10101010	01010101	11100111	10111101

Endereço IP com notação Decimal Pontuada						
170	.	85	.	231	.	189

Na Internet, você pode ter dois tipos de endereço IP: estático ou dinâmico. O primeiro, também chamado de fixo, é um endereço que não muda – ele é bem pouco utilizado, sendo mais comuns em máquinas servidoras do que em máquinas clientes (Ex.: IP do Google). Já o segundo é um endereço que é modificado a cada conexão – ele é bem mais utilizado, principalmente em redes domésticas como em uma casa ou em um escritório.

Além disso, é importante entender que esses endereços não são aleatórios – existem diversas regras que devem ser obedecidas para cada endereço. Uma delas é o endereçamento com classes. Nós já vimos quem um endereço IP (Versão 4) possui 32 bits e já sabemos que um bit só pode ter dois valores (0 ou 1). 232 ou 4.294.967.296 possibilidades.

Diante de tantos números, foram criadas diversas regras para realizar o endereçamento de um IP. Uma delas busca dividir o espaço de endereços possíveis em cinco classes: A, B, C, D e E. Logo, todo e qualquer IP do universo pode ser classificado em uma dessas cinco classes. Essa é uma ação extremamente simples: basta analisar o primeiro número (na notação decimal pontuada). Eles seguem a seguinte tabela:

Primeiro Octeto	*Classe*	*Utilização*
1 A 126	A	Inicialmente destinado a grandes organizações.
128 A 191	B	Inicialmente destinado a organizações de médio porte.
192 A 223	C	Inicialmente destinado a pequenas organizações.
224 A 239	D	Inicialmente destinado a reservado para multicast.
240 A 255	E	Inicialmente destinado a reservado para testes.

Interpretar essa tabela é muito simples. Se o primeiro número de um endereço IP for de 1 a 126, ele será da Classe A – geralmente utilizado por grandes organizações; se for de 128 a 191, ele será da Classe B – geralmente utilizado por organizações de médio porte; se for e 192 a 223, ele será da Classe C – geralmente utilizado por pequenas organizações; se for de 224 a 239, será da Classe D – reservado para multicast; e se for de 240 a 254, será da Classe E – reservado para testes.

Apesar de todas as soluções de curto prazo (Ex.: DHCP, NAT, etc.), o esgotamento de endereços ainda é um problema de longo prazo para a Internet. Esse e outros problemas no protocolo IP em si – como a falta de tratamento específico para transmissão de áudio e vídeo em tempo real e a criptografia/autenticação de dados para algumas aplicações – têm sido a motivação para o surgimento do IPv6 (IP Versão 6).

A nova versão possui 128 Bits, logo temos até 2128 possíveis endereços ou 340 undecilhões de endereços ou 340.282.366.920.938.000.000.000.000.000. 000.000.000 de endereços!

No IPv4, decidiu-se utilizar uma representação decimal de 32 bits para facilitar a configuração! Ainda que fizéssemos isso com o IPv6, teríamos uma quantidade imensa de números. Dessa forma, optou-se por utilizar uma representação com hexadecimal, que necessita de todos os números e mais algumas letras: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Dividem-se 128 Bits em 8 grupos de 16 Bits (seção de 4 hexadecimais), separados por dois-pontos.

O IPv6 não possui o conceito de classes e nem endereço de broadcast. Além disso, como o endereço ainda fica grande com o hexadecimal, há algumas formas de abreviar: zeros não significativos de uma seção (quatro dígitos entre dois-pontos) podem ser omitidos, sendo que apenas os zeros não significativos podem ser omitidos e, não, os zeros significativos. Na tabela abaixo, temos um exemplo:

Endereço original
FDEC:0074:0000:0000:0000:B0FF:0000:FFF0
Endereço abreviado
FDEC:74:0:0:0:B0FF:0:FFF0
Endereço mais abreviado
FDEC:74::B0FF:0:FFF0

Usando essa forma de abreviação, 0074 pode ser escrito como 74, 000F como F e 0000 como 0.

Observe que se tivéssemos o número 3210, por exemplo, não poderia ser abreviado. Outras formas de abreviações são possíveis se existirem seções consecutivas formadas somente por zeros. Podemos eliminar todos os zeros e substituí-los por um dois-pontos duplo. Note que esse tipo de abreviação é permitido apenas uma vez por endereço (Ex: não pode 2001:C00::5400::9).

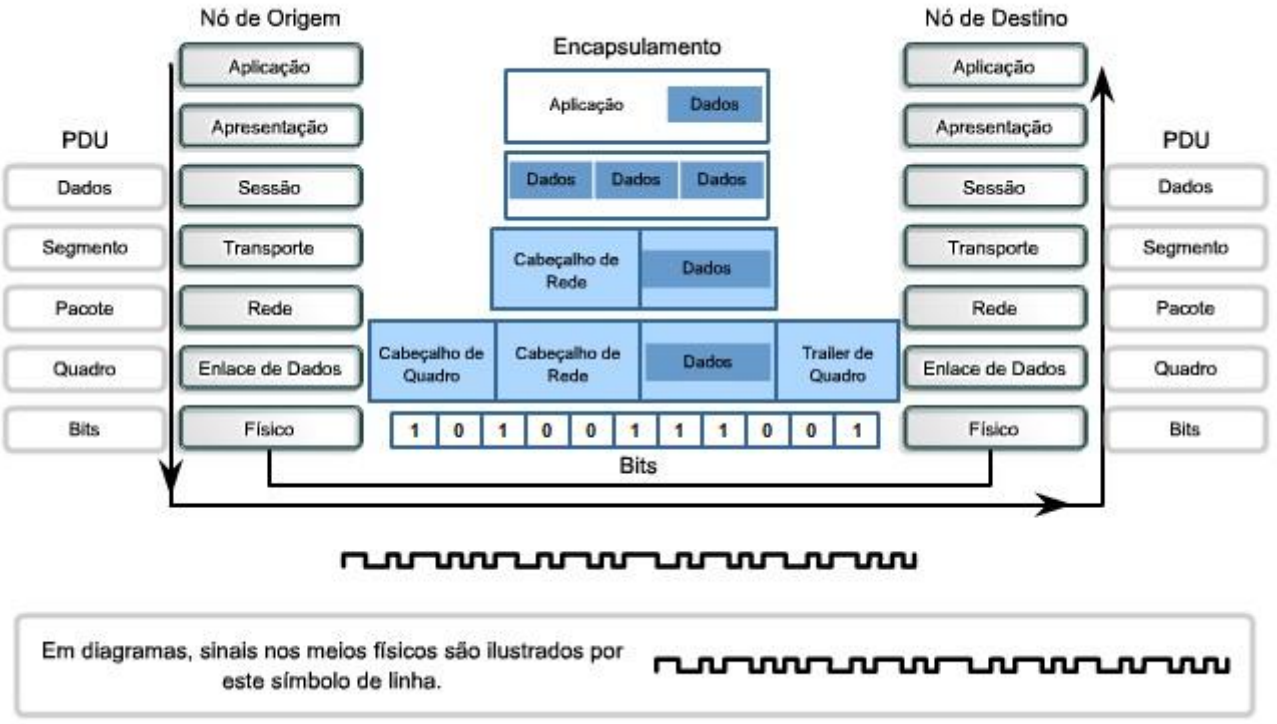
Se existirem duas ocorrências de seções de zeros, apenas uma delas pode ser abreviada. A re-expansão do endereço abreviado é muito simples: devemos alinhar as partes não abreviadas e inserir zeros para obter o endereço original expandido. É interessante notar também que o IPv6 permite também o endereçamento local, isto é, endereços usados em redes privadas. Por fim, o IPv6 pode se comunicar com o IPv4.

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.

Dentro do assunto “Redes de computadores. Acesso remoto, topologia de redes, equipamentos de interconexão (hubs, switches, roteadores, pontos de acesso wireless), cabeamento estruturado”, no tópico “Redes de Computadores” destacamos as camadas do Modelo OSI onde os protocolos estão distribuídos em 7 níveis. Observe a imagem abaixo que ilustra o caminho percorrido por cada bloco de dados.



Também precisamos destacar no tópico “Internet” algumas definições que são importantes e costumam ser recorrentes nas provas da banca.

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

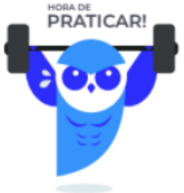
	página, um site, uma pasta etc. Um URL é composto de um protocolo, que pode ser tanto HTTP, que é um protocolo de comunicação, FTP que é uma forma rápida de transferir arquivos na internet, etc. O formato do URL é definido pela norma RFC 1738.
SSL	SSL é a abreviação de Secure Sockets Layer, trata-se 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. IMPARH - 2018 - Professor (Pref Fortaleza)/Substituto/Ciências/Edital 104.2018

O uso do computador e da Internet influenciou significativamente as relações humanas, sobretudo o que se refere à comunicação. O e-mail é uma das principais ferramentas online de troca de informações e conversa entre conhecidos, porém essa ferramenta não é dinâmica

e imediata, e a sua funcionalidade baseia-se no antigo sistema de correspondência em papel. Para resolver esses problemas, surgiu uma nova ferramenta:

A) os websites de busca.

B) as ferramentas de pesquisa.

C) o compartilhamento de arquivos.

D) as redes sociais.

Comentários

Vamos analisar as ferramentas / sistemas mencionados na questão:

E-mail: Embora seja uma importante ferramenta de comunicação, o e-mail não é uma forma dinâmica e instantânea de interação, já que a troca de mensagens pode ter um atraso.

Websites de busca (A) e Ferramentas de pesquisa (B): São importantes para encontrar informações, mas não são ferramentas de comunicação direta.

Compartilhamento de arquivos (C): Está mais relacionado à troca de documentos e mídias, sem substituir diretamente a função de interação contínua.

Redes Sociais (D): Surgiram como uma solução para tornar a comunicação mais imediata, dinâmica e interativa. Plataformas como Facebook, Twitter, e Instagram permitem conversas em tempo real, além de compartilhamento de conteúdo, fotos, vídeos, e outros tipos de interação instantânea, atendendo às demandas modernas de comunicação.

Portanto, a resposta correta é D) as redes sociais, que resolveram as limitações de comunicação do e-mail com uma interação mais imediata e contínua.

Gabarito: alternativa D.

---

2. IMPARH - 2015 - Profissional Temporário de Nível Médio (IPLANFOR)/Auxiliar em Informática/Edital 72.2014

Assinale a alternativa correta quanto ao conceito de Internet e Intranet.

A) A Internet consiste em um conjunto de redes que executam o conjunto de protocolos TCP/IP somente através dos sistemas operacionais Linux/Unix.

B) Intranet é um subconjunto de redes válido na Internet.

C) A Internet é um conglomerado de redes que executam o protocolo IPX/SPX.

D) A Internet é um conglomerado de redes de computadores que utilizam um conjunto comum de protocolos, denominado TCP/IP, para se interligar.

Comentários

Vamos analisar cada uma das alternativas:

A) Errada: A Internet utiliza o conjunto de protocolos TCP/IP em qualquer sistema operacional, não apenas Linux/Unix. O TCP/IP é o padrão para todos os sistemas operacionais modernos, incluindo Windows, macOS, etc.

B) Errada: A Intranet é uma rede privada interna, usada dentro de uma organização, e não faz parte da Internet. Ela usa os mesmos protocolos (TCP/IP) e tecnologias da Internet, mas é restrita a uma rede fechada.

C) Errada: O protocolo IPX/SPX foi utilizado por redes locais (LANs) no passado, mas não é o protocolo usado na Internet. A Internet utiliza o TCP/IP como seu protocolo padrão.

D) Certa: A Internet é de fato um conglomerado de redes interligadas que utilizam o TCP/IP (Transmission Control Protocol/Internet Protocol) como o conjunto de protocolos padrão para comunicação entre sistemas.

Portanto, a resposta correta é D) A Internet é um conglomerado de redes de computadores que utilizam um conjunto comum de protocolos, denominado TCP/IP, para se interligar.

Gabarito: alternativa D.

---

3. IMPARH - 2012 - Administrador (IPMFOR)/Edital 46.2012

A empresa Tecnologics Ltda, recentemente implantou uma intranet em sua empresa. Esse artifício, utilizado em larga escala em várias organizações no Brasil, permitirá aos seus funcionários, entre outras coisas:

A) compartilhar informações com clientes em outras cidades.

B) servir de base para aquisições e fusões com a concorrência.

C) realizar comércio eletrônico a qualquer instante.

D) trocar informações restritas e facilitar a circulação dessas informações entre os funcionários.

Comentários

Intranet: É uma rede privada interna de uma organização que utiliza tecnologias da Internet (como TCP/IP, navegadores, etc.) para compartilhar informações, ferramentas, e recursos entre os funcionários de uma empresa. O principal benefício é o compartilhamento seguro de informações restritas e a melhoria da comunicação e colaboração interna.

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

A) Errada: A Intranet é usada para comunicação interna e não para compartilhamento de informações com clientes externos. Para isso, utiliza-se a Internet ou outras ferramentas externas.

B) Errada: A Intranet não é utilizada como ferramenta específica para fusões ou aquisições com concorrentes.

C) Errada: A Intranet não é voltada para a realização de comércio eletrônico; este tipo de transação é feito através da Internet.

D) Certa: A principal função da Intranet é exatamente facilitar a troca de informações restritas e otimizar a comunicação dentro da empresa, permitindo que funcionários acessem informações importantes de forma segura e eficiente.

Portanto, a resposta correta é D) trocar informações restritas e facilitar a circulação dessas informações entre os funcionários.

Gabarito: alternativa D.

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.