EAD UNISANTA

REDES DE COMPUTADORES

Me. Joseffe Barroso de Oliveira

GUIA DA
DISCIPLINA

1. COMUNICAÇÃO DE DADOS - PARTE 01

Objetivo

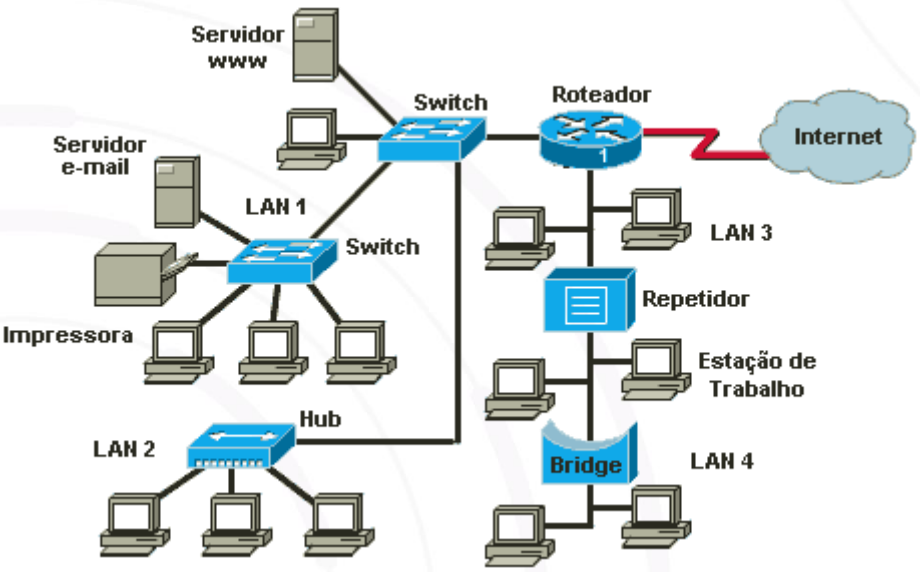
O objetivo deste capítulo é apresentar a primeira parte sobre conceitos e características de diferentes formas de comunicação de dados.

Introdução

Uma rede de computadores é composta por diversos equipamentos que permitem a comunicação entre os computadores. Esses equipamentos possuem características diferentes entre si e devem ser utilizados conforme a necessidade de cada ambiente. Dessa forma, vamos conhecer cada um deles e seu papel ideal dentro de uma rede.

1.1. Conceito

Uma rede de computador moderna pode ser caracterizada por haver uma máquina chamada cliente, uma máquina chamada servidor conectadas por um meio de comunicação. Porém a matéria de redes não se limita apenas os PCs (Personal Computers). Por mais que quando se fala em redes pensamos em conexão na via internet, outros meios também podem ser considerados redes de computadores, como por exemplo, uma conexão bluetooth a conexão de cabo entre o mouse e seu computador, uma conexão de rádio frequência e um drone por exemplo.



Também conhecido como computação distribuída ou bancos de dados distribuídos, ele depende de pontos centrais diferentes para se comunicar e sincronizar em uma rede comum. Esses pontos centrais costumam representar dispositivos de hardware físicos diferentes, mas também podem representar processos de software diferentes ou outros sistemas encapsulados recursivos. Os sistemas distribuídos visam remover gargalos ou pontos centrais de falha de um sistema.

1.2. Componentes básicos de uma rede de computadores

Uma rede de computador comum é composta pelos seguintes itens:

- Um roteador, hub ou switch
- Um equipamento com placa de rede, essa podendo ser com fio ou sem. Este equipamento é chamado de cliente.
- Um banda de comunicação - Neste caso o provedor de internet.
- Uma topologia
- Um gateway

Além dos itens acima, é necessário também um IP para o seu computador funcionar em uma rede de computadores. Um IP representa o endereço daquele computador dentro da rede e com isso ele pode ser identificado para envio e recebimento de informações.

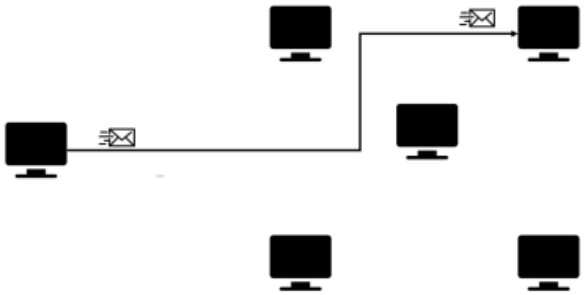
Tudo o que é enviado e recebido através de redes de computadores são um conjunto de 0 e 1, esse conjunto recebe o nome de bit um acrônimo para BInary DigiT. O conjunto desses bits formam uma mensagem e essa mensagem recebe o nome de pacote dentro do mundo das redes. E dessa forma enviamos e recebemos pacotes que nos trazem informação de um lado para o outro em redes.

1.3. Transmissão de pacotes

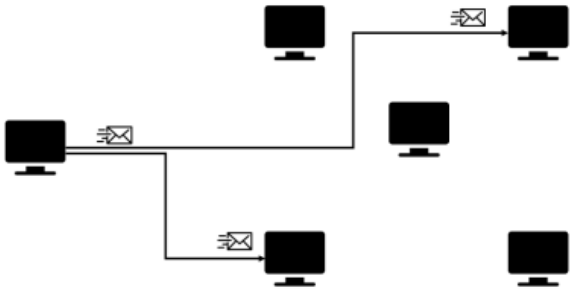
Quando se fala de transmissão de pacotes em redes de computadores, é preciso levar em conta de qual maneira essa informação será transmitida, pois esses pacotes respeitam três meios de comunicação.

Eles são o UNICAST, MULTICAST e o BROADCAST.

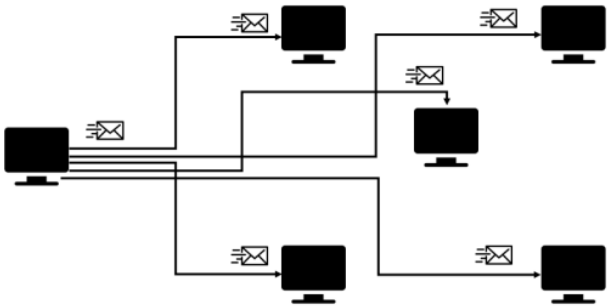
• UNICAST - Meio de transmissão no qual o pacote é enviado diretamente de um destino para uma origem ignorando quaisquer outras máquinas que estejam conectadas a rede de computadores.Também conhecida como transmissão ponto a ponto.O Unicast é o sistema de roteamento mais comum usado na internet, com cada nó atribuído à um endereço IP exclusivo. Os roteadores identificam a origem e destino dos dados e determinam o caminho mais curto (ou o mais viável) para o envio dos pacotes de dados. Os dados são entregues entre roteadores até que ele chegue ao seu destino final.



• MULTICAST - Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes. Os clientes da transmissão multicast devem ser membros de um grupo multicast lógico para receber as informações. Um exemplo de transmissão multicast é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede. Ao invés de ser enviado para um único destino (endereço IP específico), o tráfego de multicast, permite o envio de informações para um determinado grupo de clientes, cada um com um endereço IP diferente, ao mesmo tempo. O Multicast não é normalmente usado pelos roteadores de Internet, é comum sua utilização em ambientes de redes corporativas, afim de entregar o tráfego sem o uso de uma enorme quantidade de largura de banda.

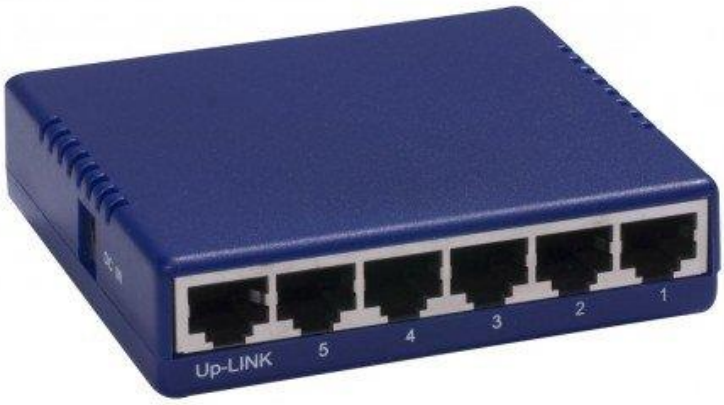


• BROADCAST - Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. A transmissão de broadcast é essencial durante o envio da mesma mensagem para todos os dispositivos na rede local. Um exemplo de transmissão de broadcast é a consulta de resolução de endereços que o Protocolo de Resolução de Endereços (ARP, Address Resolution Protocol) envia para todos os computadores em uma rede local. Uma maneira de ser possível sempre identificar o meio de transmissão Broadcast é lembrar de filmes que mostram os jornais americanos neles sempre há a informação de "Broadcasting News"o que significa que a informação deve ser disseminada para o maior número possível de pessoas.

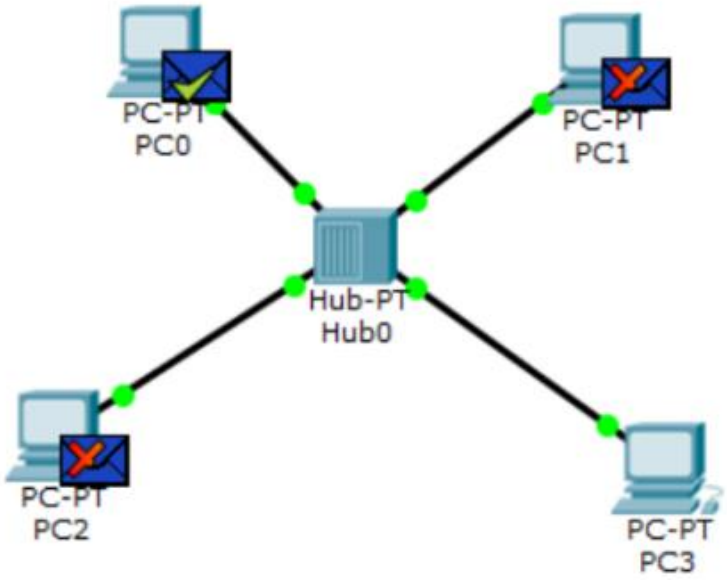


1.4. Hub

Um HUB é uma peça física (hardware) que realiza conexão de computadores de uma rede e possibilita a transmissão de informações entre essas máquinas. Ele recebe o nome de concentrador "burro" ou não gerenciável justamente pela sua falta de capacidade de distribuir pacotes paralelos, ou ao menos lidar com eles.



Porém o HUB possui algumas desvantagens em relação aos demais componentes, o HUB não é capaz de lidar com múltiplos pacotes ao mesmo tempo, o que significa que ao receber dois pacotes em um mesmo intervalo de tempo ele simplesmente irá destruir os dois pacotes e eles não serão entregues. Outra desvantagem é referente a questão da segurança, que ao enviar um pacote para um destinatário ele encaminha o pacote a todos os outros equipamentos da rede e espera que eles neguem a informação e que somente o responsável o aceite. De forma geral é isso que acontece, entretanto ao entregar o pacote a uma máquina que não era o destino você abre uma brecha para que essa informação seja lida, existem muitas técnicas de ataque que são capazes de ler esses pacotes entre elas podemos destacar o Man in the Middle ou MITM, ataque este que lê os pacotes nas redes.



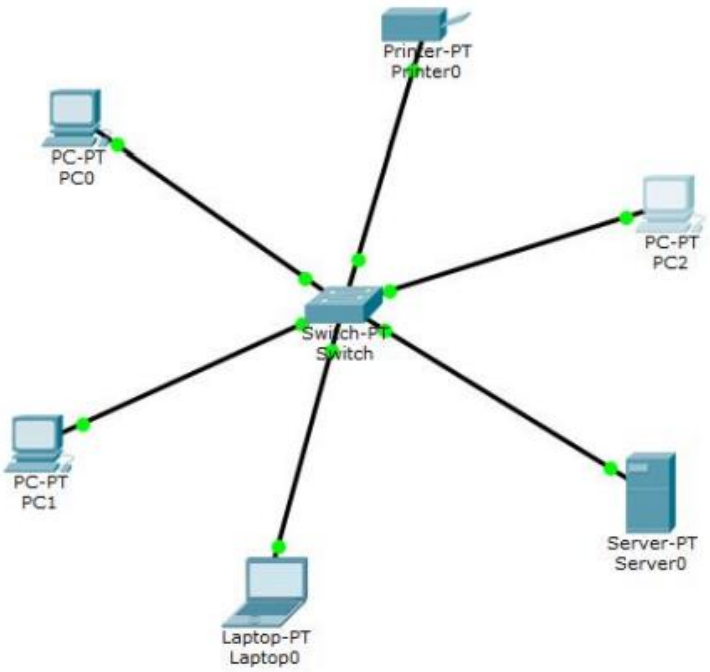
O fato de não ser um equipamento seguro o coloca como uma das opções menos viáveis para as empresas de grande porte que geralmente possuem dados sigilosos e sensíveis e que tal acesso não pode ser aberto. Mas algumas empresas quando colocam o funcionário sobre investigação costumam usar o HUB para que seja possível identificar os pacotes e ver o que está sendo enviado.

1.5. Switch

Switches, são equipamentos de redes, assim como os HUBs, eles são considerados concentradores e distribuem os pacotes para os computadores neles conectados, possuem

normalmente de 4 a 255 portas para conexão de internet, conforme mais portas mais elevado é o valor. Ao contrário do hub, o switch é capaz de lidar com múltiplos pacotes paralelamente, ou seja, caso o concentrador receba mais de um pacote ele consegue manejar e distribuí-lo na rede sem que haja perda de dados. Uma outra vantagem em relação ao HUB é que as informações são entregues diretamente ao destinatário, o que significa que o pacote não passa por todos os equipamentos na rede antes de ser entregue, o que garante um aumento de confiabilidade na rede. Se um pacote demora a ser transmitido, não interfere tanto no desempenho da rede, visto que muitos outros pacotes estão sendo transmitidos em paralelo. Em redes empresariais onde há um grande tráfego de dados, a utilização de um switch ao invés de um hub é altamente recomendável.

Mas existem algumas desvantagens que valem a pena mencionar, tais como a rota de entrega, todo pacote tem uma rota de entrega, vamos fazer uma analogia a um carteiro, um carteiro novo que começou a pouco tempo não conhece as casas que normalmente ele entrega a informação, e normalmente ele não utiliza a rota mais otimizada partindo apenas para rota que pode ser a mais longa. No switch é a mesma coisa o pacote irá passar por algumas rotas pré-definidas, aqui entende-se como rota por quais switches ou roteadores o pacote irá passar e toda troca de um roteador para o outro é chamado de HOP ou salto em português, e essas rotas podem levar mais tempo. Por mais que a tecnologia esteja já disseminada, não podemos considerar o SWITCH como um equipamento barato, conforme maior o número de portas e opções de gerenciabilidade, maior será o valor, podendo chegar na casa dos milhares de reais. Podendo, inclusive, haver equipamentos não disponíveis no Brasil dependendo de uma importação, o que gera um custo ainda mais elevado.



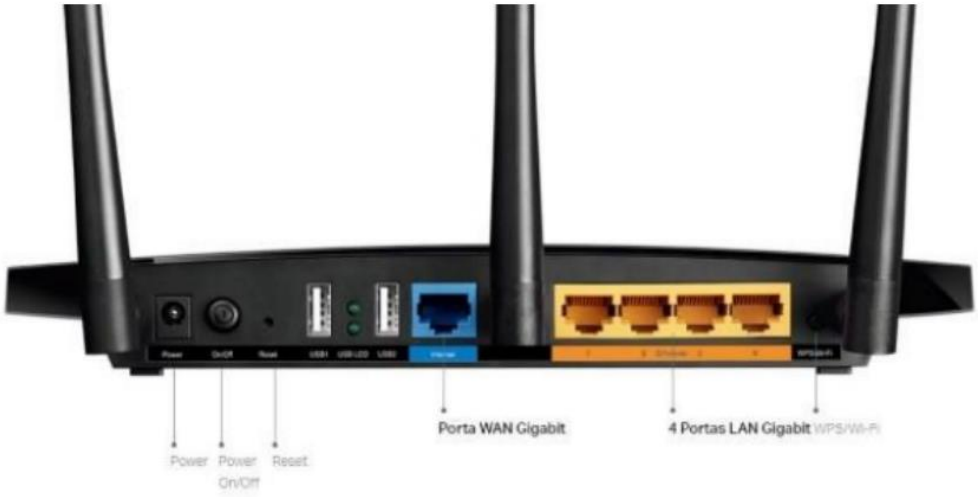
No geral os concentradores gerenciáveis são utilizados de forma conjunta com os roteadores, no qual o roteador fica responsável por toda a parte de rota e saltos e o switch fica responsável apenas pela entrega dos pacotes.

1.6. Roteador

Roteador, pode ser considerado o equipamento mais inteligente de uma rede doméstica, após o computador, pois dentro do roteador existem algoritmos – códigos programados – que são capazes de tratar os pacotes de informações recebidos, lembrando que são vários pacotes ao mesmo tempo.

Cada pacote de informação recebido pelo roteador tem um endereço IP e uma porta destino. O roteador recebe cada pacote e encaminha para o IP de destino, de acordo com regras pré-definidas. Isto é chamado de redirecionamento de portas. Além disso, muitos roteadores possuem firewall internos aumentando significativamente a segurança da rede e também a complexidade e configuração. O Roteador de longe é o melhor equipamento para uma rede, tanto doméstica quanto empresarial obviamente um roteador dedicado a empresas será mais caro e haverá muito mais opções de configuração mas não é raro em empresas de pequeno e médio porte haver roteadores domésticos, uma vez que eles cumprem bem o papel.

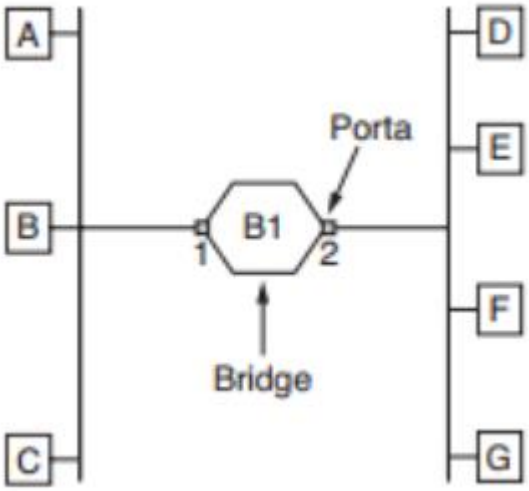
O roteador geralmente não possui além de quatro ou cinco portas uma vez que ele trabalha nativamente com switch, podendo assim ampliar sua capacidade. É possível também ligar roteador dentro de roteador o que gera o chamado Cascateamento de Roteadores, assim como acontece quando trabalha com switch é necessário adicionar uma permissão de master-slave onde o roteador instrui pacotes ao outro roteador



Além de ser responsável por fazer a rota mais curta, o roteador também faz a rota mais segura, ou seja, se durante a transmissão de algum pacote de informação algum outro roteador ficar em modo off-line o roteador anterior poderá remanejar a rota em sacrifício do tempo.

1.7. Bridge

Bridge, nada mais são do que os switches que falamos anteriormente, ou melhor, é um nome moderno para as Bridges. São exatamente a mesma coisa que um switch a única diferença é que a bridge possui apenas três entradas que servem para conectar duas redes, que podem estar separadas. Possuem as mesmas vantagens e desvantagens e são utilizados da mesma maneira.



Podemos concluir que bridge (ponte do inglês) como um equipamento de hardware que une duas redes com protocolos distintos , uma rede Linux com uma rede Windows, assim permitindo que elas troquem pacotes de informação e compartilhem recursos. É exatamente a mesma coisa que um switch, na realidade, definimos uma bridge como um switch com menos portas.

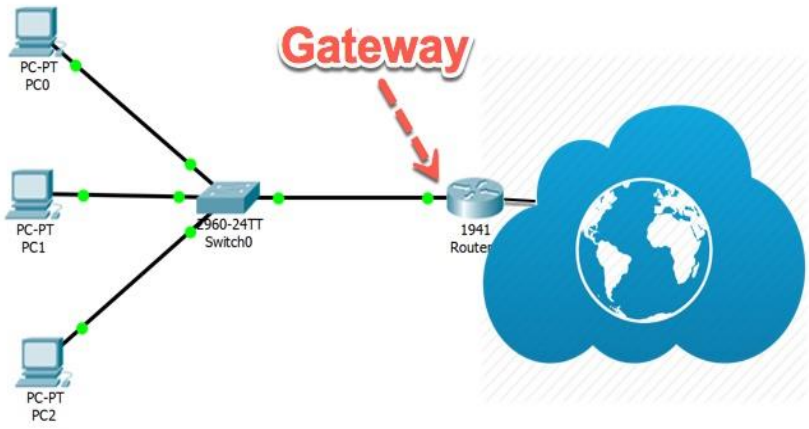
1.8. Repetidor

O sinal de internet, tanto o sem fio quando com fio devido a distância e fatores externos, como campos magnéticos ou obstrução das ondas de rádio pode e com toda certeza irá sofrer degradação, o que vai proporcionar uma baixa qualidade de sinal, um mau desempenho ou até mesmo a ausência de conexão.

Para isso os repetidores permitem aumentar o sinal entre dispositivos de uma rede com o propósito de aumentar a distância entre os equipamentos, seja ela cabeada ou sem fio. O repetidor é capaz de amplificar as ondas eletromagnéticas oriundas de uma rede sem fio ou ligar dois segmentos de redes distintas, por exemplo, um segmento que utiliza um cabo de cobre e um segmento que utiliza um cabo de fibra óptica.

1.9. Gateway

Um gateway de rede é um dispositivo que permite a comunicação entre redes. De um modo genérico podemos classificar os gateways em dois tipos: os gateways conversores de meio e os tradutores de protocolos. Como funções básicas estão: receber um pacote do nível inferior, tratá-lo (ler cabeçalho, descobrir roteamento, construir um novo pacote inter-redes) e enviá-lo ao destino.



2. Comunicação de Dados - Parte 02

Objetivo

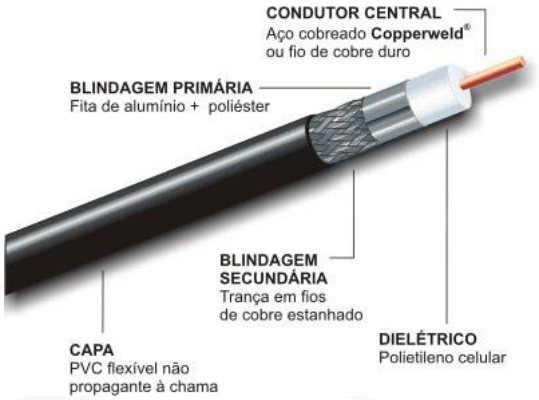
O objetivo deste capítulo é apresentar a segunda parte sobre conceitos e características de diferentes formas de comunicação de dados.

Introdução

Uma rede de computadores é composta por diversos equipamentos que permitem a comunicação entre os computadores. Além dos equipamentos existem os meios de transmissão, que incluem cabos, dispositivos sem fio, entre outros. Vamos conhecer cada um deles e suas diferenças.

2.1. Cabo coaxial

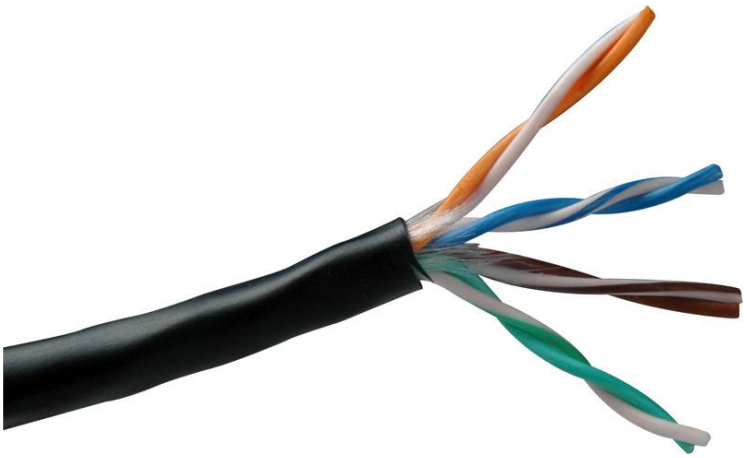
Utilizados em redes de computadores antigas e ainda hoje em cabos de antenas para redes wireless e cable modem, mas que possuíam uma série de limitações como: mal contato, conectores caros, cabos pouco maleáveis e um limite de velocidade de 10 Mbits/s.



O cabo coaxial foi por certo tempo utilizado como cabeamento responsável pela interligação de computadores em uma rede. Um cabo coaxial é basicamente composto por quatro elementos (da parte interna para a externa): um fio de cobre (responsável por transmitir sinais elétricos), um material isolante, com o intuito de minimizar interferências eletromagnéticas produzidas pelo cobre (condutor de energia), um condutor externo de malha e uma camada plástica protetora do cabo. Estes quatro elementos combinados, formam o cabo coaxial (SILVA, 2010).

2.2. Cabo par trançado

Os cabos de par trançado são, atualmente, os mais utilizados em uma rede local de computadores. Composto por pares de fios de cobre, trançados entre si, possuem diferentes tipos, categorias e padrões. Cabos de par trançado fazem uso de material condutor (cobre) para transmitir sinais elétricos. Associado a isso temos basicamente a frequência que este sinal é transmitido e a quantidade de bits que podem ser transferidos por segundo. Por tratar-se de material condutor de sinais elétricos, os cabos de par trançado estão sujeitos a interferências eletromagnéticas externas de diferentes naturezas. Uma das maiores vantagens em se utilizar cabos de par trançado para implantar uma rede de computadores é o fato de possuírem baixo custo e flexibilidade em prestar manutenção, corrigir eventuais problemas ou até mesmo expandir o número de computadores ligados a esta rede.



2.2.1. Categorias de cabo par trançado

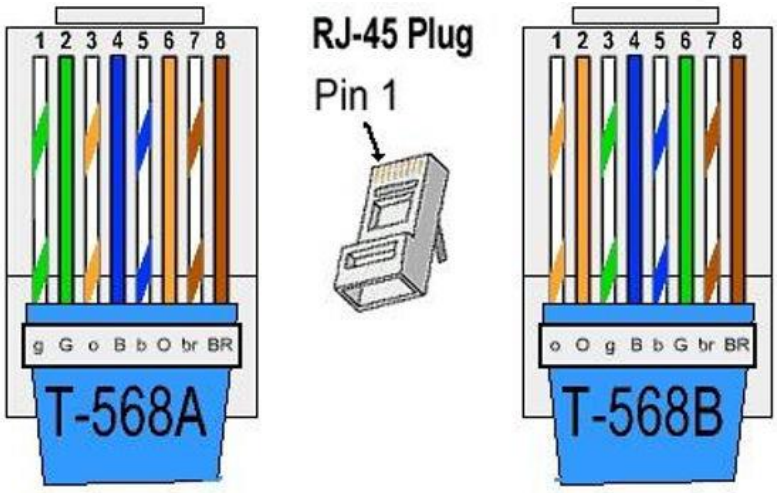
Os cabos de par trançado são divididos em categorias como uma espécie de classificação e características do mesmo (frequência, velocidade de transmissão, etc.). As categorias dos cabos de par trançado vão de 1 a 7. Para todas estas categorias a distância máxima permitida entre um ponto e outro onde o cabo é utilizado é de 100 metros. Fatores que influenciam no comprimento máximo do cabo já foram citados anteriormente, como frequência, taxa de transferência de dados e interferência eletromagnética. No Quadro é possível visualizar um comparativo entre as categorias existentes, taxa de transferência possível e frequência.

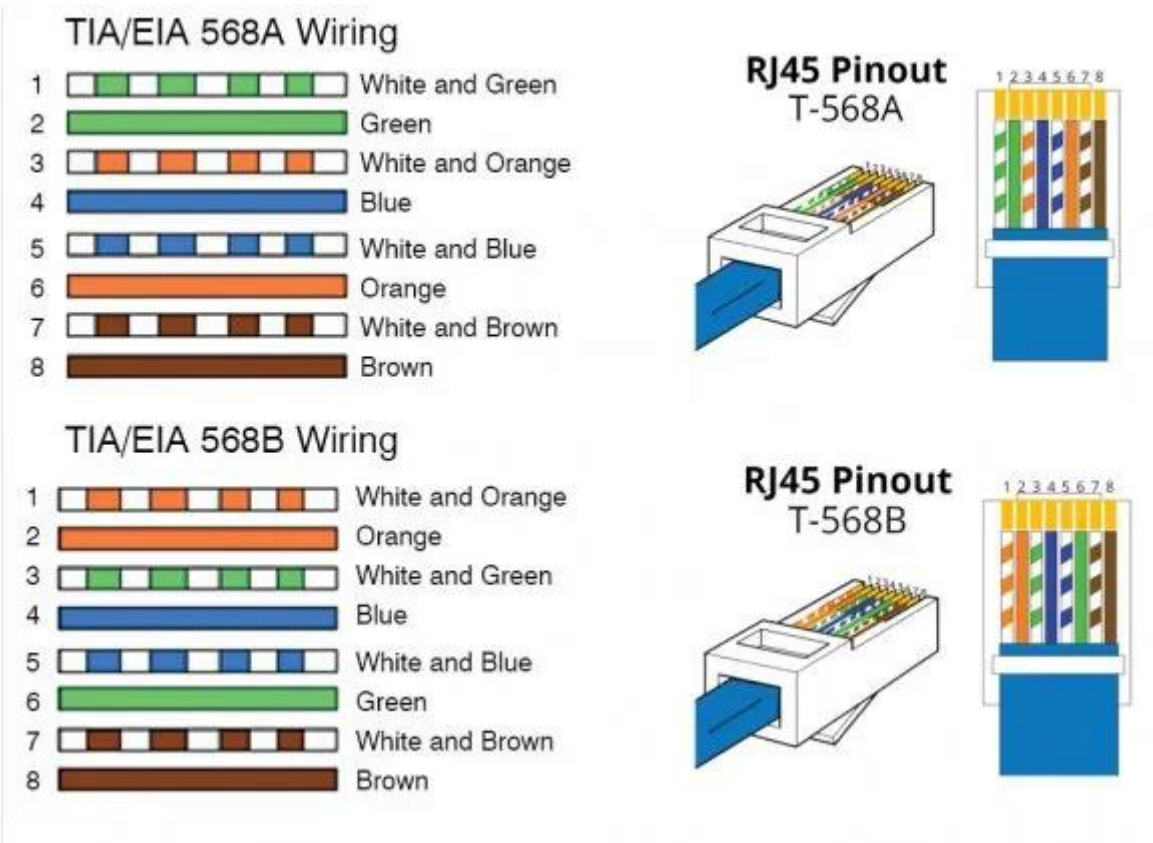
Categoria do cabo	Taxa de transferência máxima	Frequência
Cat 1	Até 01 Mbps	Até 01 MHz
Cat 2	Até 04 Mbps	Até 16 MHz
Cat 3	Até 10 Mbps	Até 16 MHz
Cat 4	Até 20 Mbps	Até 20 MHz
Cat 5	Até 100 Mbps	Até 100 MHz
Cat 5e	Até 1000 Mbps	Até 125 MHz
Cat 6	Até 1000 Mbps	Até 250 MHz
Cat 6a	Até 10 Gbps	Até 500 MHz
Cat 7	Até 10 Gbps	Até 700 MHz

2.2.2. Padrões de conexão e montagem de ponta do cabo

Um cabo de par trançado dispõe em seu interior de oito fios dispostos em pares, sendo que destes quatro pares somente dois pares são efetivamente utilizados (sendo um para transmitir e outro para receber dados). Os oito fios presentes no cabo possuem cores diferentes, como forma de simplificar a identificação dos mesmos e a crimpagem (ato de conectar o cabo ao conector RJ-45).

Para que seja mantido um padrão quanto a ordem de cores deste cabo junto ao conector, tem-se dois padrões bastante utilizados: os padrões EIA 568A e o padrão EIA 568B, sendo que o padrão EIA 568A é o mais comum a ser utilizado:





Os dois padrões possuem grande semelhança, o que ocorre de diferente é a troca de posições entre os cabos laranja e verde. Ao fazer as conexões dos conectores RJ-45 aos cabos de rede (crimpagem) devemos seguir sempre um dos padrões citados acima (568A ou 568B) nas duas extremidades do cabo, isto serve para ligação de um computador a um switch, de um computador a um roteador, enfim, para dispositivos diferentes. Caso exista a necessidade de ligar dispositivos diretamente, como no caso um computador ligado diretamente a outro por um único cabo de rede (chamado neste caso de cabo crossover), neste caso é necessário que uma das pontas do cabo seja conectada usando o padrão 568A e a outra ponta o padrão 568B. É importante salientar a regra a seguir:

- -Dispositivos diferentes: (ligação de cabo par trançado entre computador/ switch ou computador/roteador, etc.) cabos com padrões iguais nas duas pontas (568A nas duas pontas ou 568B nas duas pontas).

- -Dispositivos iguais: (cabo entre computador/computador ou switch/switch, etc.) existe a necessidade de uma ponta de conexão ser diferente da outra (uma ponta 568A e a outra ponta 568B). Com esta regra fica mais fácil a utilização de cada um levando em consideração a necessidade dos mesmos.

Além disso, para confecção do cabo de rede par trançado com o conector RJ-45, é necessário realizar o processo de crimpagem. Para isso, é necessário utilizar um decapador (ferramenta amarela), um alicate crimpador (ferramenta preta e verde) e um testador de cabo (ferramenta branca e verde) para verificar se realmente a crimpagem do cabo com o conector está 100% funcional. Todas essas ferramentas podemos ver abaixo:

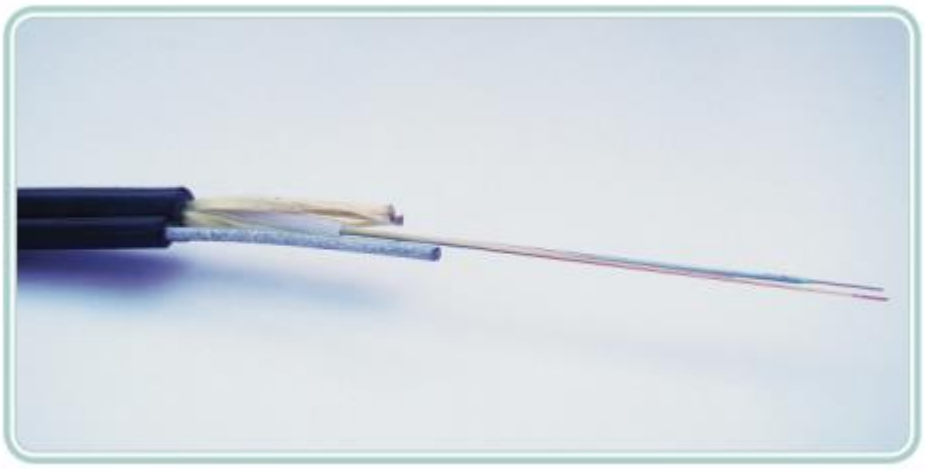
2.3. Fibra óptica

Os cabos de fibra óptica popularizaram-se e hoje têm um papel fundamental nas telecomunicações, principalmente em ambientes que necessitam de uma alta largura de banda, como é o caso da telefonia, televisão a cabo, entre outros. A redução do preço da fibra, o alcance e quantidade de dados que é possível trafegar nela são alguns dos motivos da aceitação e utilização das fibras ópticas em longas distâncias, bem como, gradativamente nas redes locais de computadores. Uma fibra óptica nada mais é do que uma pequena haste de vidro, revestida por materiais protetores, que utiliza-se da refração interna total, para poder transmitir feixes de luz ao longo da fibra por grandes distâncias.

Junta-se a capacidade de transmissão da fibra com o fato da perda ser mínima em grande parte dos casos.

Um cabo de fibra óptica é composto por diferentes materiais, conforme pode ser descrito a seguir, da parte interna para a externa da fibra (SILVA, 2010):

- Núcleo – geralmente produzido de vidro, possui em média 125 mícrons (um décimo de um milímetro aproximadamente), por onde passa a luz emitida e refletida por toda a fibra.
-
- Casca – geralmente de plástico serve para revestir a fibra. • Capa – feita de plástico tem o objetivo de proteger tanto a casca como a fibra.
-
- Fibras de resistência mecânica – servem para preservar o cabo evitando que o mesmo seja danificado.
-
- Revestimento externo – camada de plástico externa que protege os cabos de fibra óptica internos. Os cabos de fibra óptica variam quanto a quantidade de fios existentes em seu interior, podendo ter um ou vários, dependendo do tipo e onde será utilizado.



De modo geral, os cabos utilizados para interligação em uma rede de computadores local, geralmente possui um único cabo. Já, os cabos de fibra destinados a interligação de grandes distâncias e links de comunicação possuem diversos fios. Existe uma série de

vantagens em se utilizar cabos de fibra óptica no lugar dos cabos de par trançado citados anteriormente, algumas destas vantagens são:

- Como os cabos de fibra óptica são bastante finos, conforme tamanho mencionado anteriormente é possível incluir uma grande quantidade de fios em um cabo.

- A quantidade de transmissão de dados possível em uma fibra é muito maior do que a capacidade alcançada através de cabos de par trançado.

- Além disso, como as fibras possuem um longo alcance, necessitam de menos repetidores ou equipamentos para expansão do sinal.

- No caso de grandes distâncias a serem interligadas, acaba saindo mais barato o uso de fibras ópticas.

- Por usar refração de luz em seu núcleo a fibra é imune a interferências eletromagnéticas, podendo ser utilizada em diferentes ambientes e situações.

As fibras ópticas fazem uso de luz infravermelha para transmissão de sinais, com um comprimento de onda de 850 a 1550 nanômetros. O uso de LED's era bastante comum nos transmissores, porém, foi sendo gradativamente substituído pelos lasers devido a demanda de velocidade dos novos padrões (01 Gbps e 10 Gbps).

2.3.1. Tipos de fibra

As fibras ópticas dividem-se em fibras de monomodo, também conhecidas como SMF (Single Mode Fibre) e as fibras de multimodo ou MMF (Multi Mode Fibre).

As fibras monomodo, têm as seguintes características:

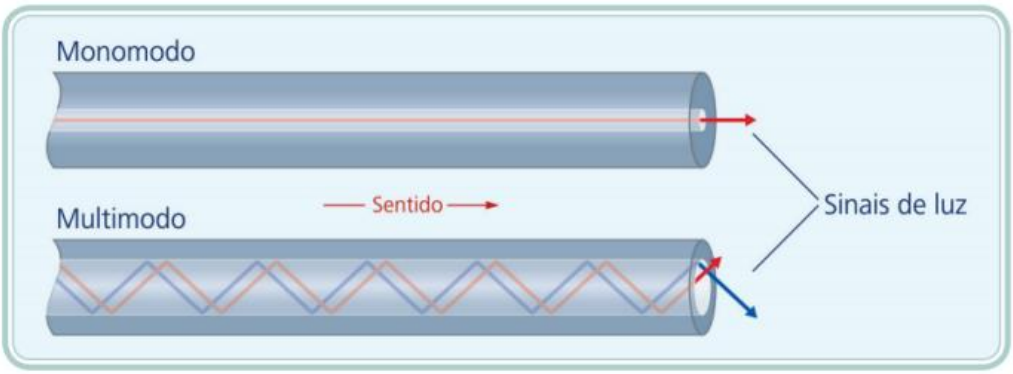
- Possuem um núcleo de 08 à 10 mícrons de diâmetro.
- Inicialmente eram bem mais caras do que as fibras multimodo.
- A atenuação do sinal é menor do que nas fibras multimodo.

- São capazes de atingir distâncias de até 50 km sem a necessidade de retransmissores.

Já as fibras ópticas multimodo, possuem como características:

- Núcleos no tamanho de 62,5 mícrons de diâmetro.
- Inicialmente eram mais baratas que as fibras monomodo.
- Possuem uma atenuação do sinal luminoso maior que as fibras monomodo.
- Podem interligar pontos até 2,5km sem necessidade de retransmissores.

A diferença entre uma fibra monomodo e uma multimodo é basicamente a forma de propagação do sinal luminoso que cada uma faz. Nas fibras monomodo, por exemplo, dado o núcleo da fibra ser menor, isso faz com que a luz trafegue na fibra mantendo uma constância do sinal, tendo desta forma um número menor de reflexões dentro da fibra, o que torna a mesma menos suscetível a perdas ou atenuação do sinal. Porém, nas fibras multimodo, acontece o inverso, ou seja, devido ao núcleo da fibra ter uma maior espessura, o sinal luminoso ricocheteia dentro da fibra em diferentes direções, fazendo com que o sinal luminoso tenha maior atenuação e maior perda durante a transmissão.



Abaixo podemos ver as características das fibras ópticas monomodo e multimodo.

Tipo de Fibra	Velocidade	Distancia
Multimodo	100 Mbit/s	2 Km
Multimodo	1000 Mbit/s	200 ~ 500 m
Multimodo	10 Gbit/s	300m
Monomodo	1000 Mbit/s	2 Km
Monomodo	10 Gbit/s	10 Km

Os conectores para as fibras ópticas tem um papel importante, no que diz respeito a permitir a passagem da luz, sem que ocorra um alto nível de perda, neste processo. Existem diferentes tipos de conectores que podem ser utilizados para este fim, entre os mais usuais estão os conectores: ST, SC, LC e MT-RJ.

2.4. Wi-fi (Conexão sem fio)

O termo Wi-Fi (Wireless Fidelity), refere-se a um padrão (IEEE 802.11) para redes sem-fio. Através da tecnologia Wi-Fi é possível realizar a interligação de dispositivos compatíveis como notebooks, impressoras, tablets, smartphones, entre outros. Assim como outras tecnologias sem fio, o Wi-Fi utiliza-se da radiofrequência para transmissão de dados. Esta flexibilidade e facilidade de construir redes utilizando este padrão fez com que o Wi-Fi se tornasse popular, sendo hoje utilizado em diferentes locais como hotéis, bares, restaurantes, hospitais, aeroportos, etc. A tecnologia Wi-Fi é baseada no padrão 802.11,

conforme citado anteriormente, que estabelece regras (normas) para criação e uso das redes sem-fio O alcance das redes Wi-Fi variam conforme os equipamentos utilizados, mas em geral cobrem áreas de centenas de metros. As redes Wi-Fi, são subdivididas em categorias ou padrões, como forma de organização e normatização da tecnologia, conforme descrito a seguir.

Padrão 802.11: Criada originalmente em 1997, opera com frequências definidas pelo IEEE (Institute of Electrical and Electronic Engineers) de 2,4 GHz à 2,48 GHz, possuindo uma taxa de transmissão de dados de 1 Mbps à 2 Mbps. Quanto às formas que o padrão 802.11 utiliza para transmissão do sinal de radiofrequência, tem-se: o DSSS (Direct Sequence Spread Spectrum) e o FHSS (Frequency Hopping Spread Spectrum). O DSSS faz o uso de vários canais de envio simultâneo, enquanto o FHSS transmite a informação utilizando diferentes frequências.

Padrão 802.11b: Este padrão (802.11b) é uma atualização do padrão 802.11 original. Como característica principal apresenta diferentes velocidades de transmissão, que são: 01 Mbps, 02 Mbps, 5,5 Mbps e 10 Mbps. A taxa de frequência é igual ao padrão anterior (2,4 GHz à 2,48 GHz) sendo que a distância máxima de comunicação neste padrão pode chegar a 400 metros, para ambientes abertos e 50 metros para ambientes fechados (salas, escritórios, etc.).

Padrão 802.11a: Disponível em 1999, esta tecnologia possui as seguintes características:

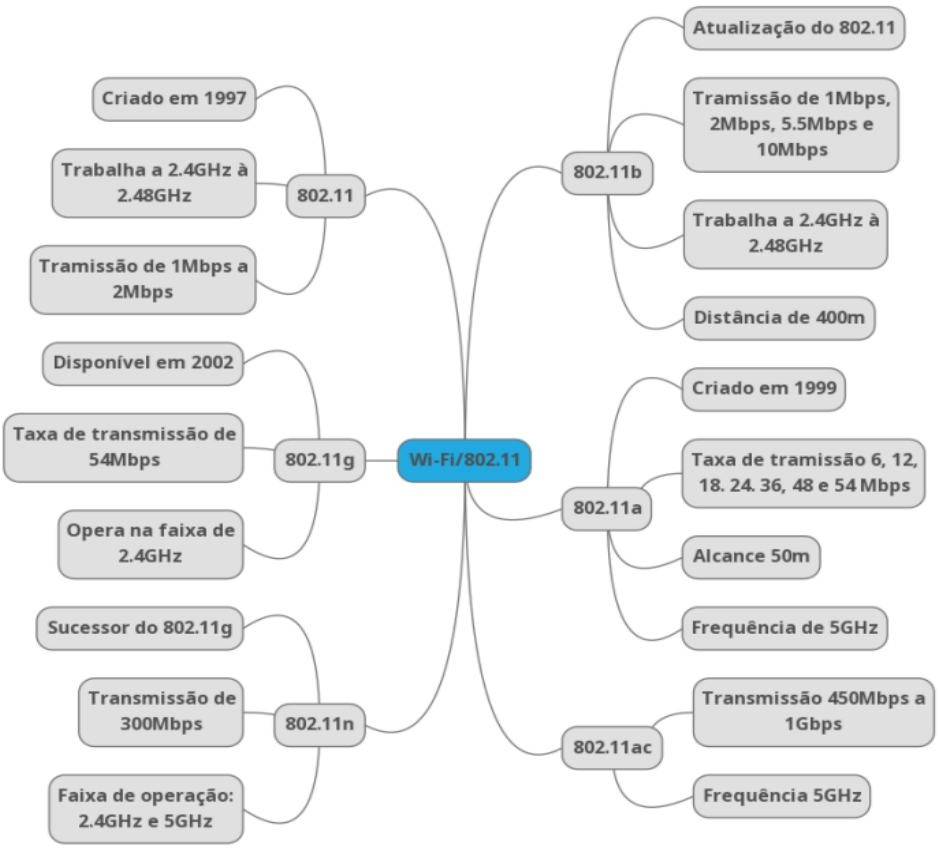
- Taxa de transmissão de dados: 06, 09, 12, 18, 24, 36, 48 e 54 Mbps
- Alcance máximo de 50 metros
- Frequência de operação de 05 GHz
- Utiliza a técnica de transmissão denominada OFDM (Orthogonal Frequency Division Multiplexing), que permite a informação ser trafegada e dividida em pequenos segmentos transmitidos simultaneamente em diferentes frequências

Padrão 802.11g: Disponível desde 2002, este padrão veio a substituir o padrão 802.11b. Como características este padrão possui:

- Taxas de transmissão de até 54 Mbps.
- Frequências na faixa de 2,4 GHz.
- Técnica de transmissão OFDM

Padrão 802.11n: Sucessor do padrão 802.11g, o padrão 802.11n teve seu início a partir de 2007. Sua principal característica está no fato de conseguir transmitir utilizando várias vias de transmissão (antenas) em um padrão chamado MIMO (Multiple-Input Multiple-Output), propiciando com isso taxas de transmissões na faixa de 300 Mbps. Com relação a frequência de operação, o padrão 802.11n pode operar tanto na faixa de 2,4 GHz como na faixa de 5 GHz, tornando-se compatível com padrões anteriores. Quanto a abrangência é possível chegar a 400 metros.

Padrão 802.11ac: O padrão 802.11ac, sucessor do padrão 802.11g, faz parte de uma nova geração de padrões de alta velocidade das redes sem-fio. Sua principal vantagem está na velocidade da transmissão de dados entre dispositivos do mesmo padrão: de 450 Mbps à 1 Gbps. Preparada para trabalhar na frequência de 5 GHz, contará com um sistema avançado de modulação chamado MU-MIMO (Multi User – Multiple Input Multiple Output) (ALECRIM, 2008a).



2.5. Bluetooth

O Bluetooth é uma tecnologia de transmissão de dados sem-fio, que permite a comunicação entre computadores, notebooks, smartphones, mouse, teclado,impressoras, entre outros dispositivos de forma simples e com um baixo custo, bastando que estes dispositivos estejam em uma mesma área de cobertura.

A tecnologia Bluetooth (padronizada pela IEEE 802.15) possui características como: baixo consumo de energia para seu funcionamento e um padrão de comunicação sem-fio para dispositivos que façam uso desta tecnologia. Dessa forma, a comunicação entre estes dispositivos ocorre através de radiofrequência, independente da posição deste dispositivo, desde que o mesmo se encontre dentro de uma mesma área de abrangência dos demais dispositivos que queiram comunicar-se. A área de cobertura do Bluetooth abrange três tipos de classes diferentes, conforme abaixo:

Classe	Potência (máxima)	Alcance (máximo)
1	100 mW	100 metros
2	2,5 mW	10 metros
3	1 mW	1 metro

A velocidade de transmissão em uma rede Bluetooth varia conforme a versão da tecnologia, neste caso temos:

- Versão 1.2, com taxa de transmissão de 1 Mbps (taxa máxima).
- Versão 2.0, com taxa de transmissão de 3 Mbps (taxa máxima).
- Versão 3.0, com taxa de transmissão de 24 Mbps (taxa máxima).

Quanto à frequência e operação do Bluetooth, o mesmo opera na frequência de 2,45 GHz, padrão de rádio aberta utilizável em qualquer lugar do mundo. A faixa de operação chamada ISM (Industrial Scientific Medical), possui variações de 2,4 à 2,5 GHz.

2.6. Placa de rede

As placas de rede ou interfaces de rede, também denominadas de NIC (Network Interface Card) são a comunicação inicial entre um computador ou notebook, por exemplo, e os demais dispositivos da rede (switch, hub, ponto de acesso, etc.), permitindo que este dispositivo conecte-se a outro na rede. As placas de rede podem ser on-board, neste caso já vem integradas ao computador em questão, ou off-board, neste caso são placas vendidas separadamente que são encaixadas na placa mãe do computador (slots). Basicamente o que uma placa de rede faz é transmitir e receber dados através da rede. Entre suas principais funções estão: gerar sinais que são captados na rede e controlar o fluxo de dados.

Placa de rede wi-fi

Placa de rede para cabo par trançado

Placa de rede para cabo coaxial (esq.) e cabo par trançado (dir.)

Placa de rede wi-fi e bluetooth para notebook

3. TOPOLOGIA E CARACTERÍSTICAS FÍSICAS DAS REDES DE COMPUTADORES

Objetivo

O objetivo deste capítulo é apresentar topologias e classificações das redes de computadores.

Introdução

Redes de computadores são formadas por uma série de conexões realizadas entre diversos dispositivos que têm a função de trocar recursos e dados, conectando-se entre si. O que nós conhecemos como internet é, justamente, um tipo de rede de computador: o único que abrange o mundo inteiro. Esse tipo de conexão permite, justamente, as trocas de dados entre diversos dispositivos.

3.1. Classificação das redes

3.1.1. PAN

A rede PAN é bastante restrita, normalmente, às áreas domésticas de uma residência. É a sigla para Personal Area Network. Nesse caso, conecta-se uma série de dispositivos que operam segundo o tipo de conexão estabelecido (Bluetooth, USB etc).

Contudo, a diferença está no centro do número de pessoas envolvidas. **A rede PAN, normalmente, trata-se de uma única pessoa utilizando os diversos dispositivos da rede**, enquanto na LAN doméstica, temos um maior número de usuários envolvidos.

3.1.2. LAN

LAN é a sigla para Local Area Network, ou seja, é uma rede formada por dispositivos que estejam dentro da mesma área física. **Normalmente, é muito utilizada em espaços pequenos e que não tenham demandas altas de contato externo**. Assim, é a opção mais comum para escolas, escritórios pequenos, residências, entre outros.

3.1.3. MAN

MAN é a sigla para Metropolitan Area Network, ou seja, é uma rede formada por **dispositivos que estão na mesma área de abrangência, mas dentro de um espaço maior, ou seja, em uma região metropolitana**. É muito utilizada, principalmente, para oferecer conexões entre unidades que estão localizadas em uma mesma cidade.

Normalmente, é adotada em **escritórios que tenham mais de uma unidade na mesma cidade,** mas que não se encontram no mesmo edifício, fazendo a interligação entre eles. Além disso, também atende a escolas de uma rede da mesma localidade ou, ainda, para a conexão entre órgãos públicos na mesma rede, que estejam em edifícios diferentes.

3.1.4. WAN

WAN é a sigla para a Wide Area Network e se trata de uma rede maior e, portanto, **pode abranger um país e, até mesmo, um continente inteiro ou mais.**

3.1.5. WLAN

A WLAN é a sigla para Wireless-LAN, ou seja, trata-se de uma rede local na qual os dispositivos estão conectados sem a necessidade de cabos para esse fim. **É uma opção à rede LAN** e pode realizar uma divisão da conexão física em diversas conexões LAN virtuais.

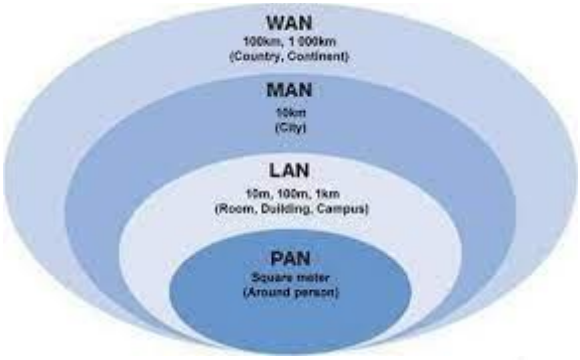
3.1.6. WMAN

Em paralelo, a WMAN é a sigla para Wireless-MAN, ou seja, **são redes metropolitanas que são interligadas sem a necessidade de cabos.** Utiliza torres de

celulares para realizar essa conexão sem fio, unindo empresas, universidades, órgãos governamentais, entre outros.

3.1.7. WWAN

Temos, em outra analogia, a WWAN, ou seja, Wireless-WAN. **São redes maiores e utilizadas, principalmente, com conexões móveis (3G, 4G e 5G),** permitindo a integração de diversos usuários no modelo Wi-Fi, ao mesmo tempo.



3.2. Topologia das redes

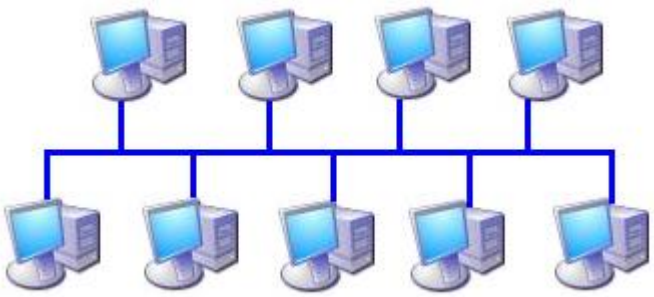
Uma topologia de rede tem o objetivo de descrever como é estruturada uma rede de computadores, tanto fisicamente como logicamente. A topologia física demonstra como os computadores estão dispersos na rede (aparência física da rede). Já a topologia lógica demonstra como os dados trafegam na rede (fluxo de dados entre os computadores que compõem a rede). A topologia de uma rede pode ter diferentes classificações.

As principais são:

- Barramento
- Anel
- Estrela
- Malha
- Árvore
- Híbrida

3.2.1. Barramento

Na topologia em barramento todos os computadores trocam informações entre si através do mesmo cabo, sendo este utilizado para a transmissão de dados entre os computadores. Este tipo de topologia é utilizado na comunicação ponto-a-ponto.



De acordo com Silva (2010), as vantagens da topologia em barramento são:

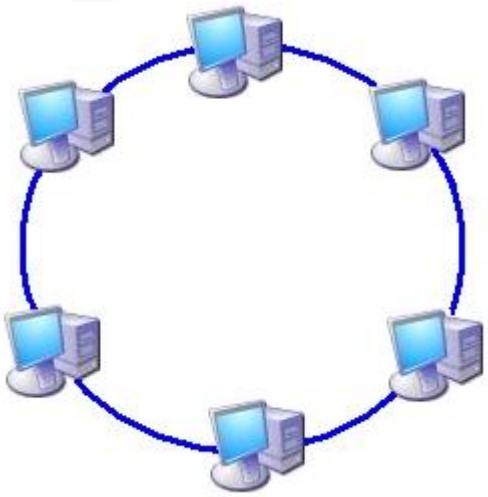
- Estações de trabalho compartilham do mesmo cabo.
- São de fácil instalação.
- Utilizam pouca quantidade de cabo.
- Possui baixo custo e grande facilidade de ser implementada em lugares pequenos.

Como desvantagens deste tipo de topologia, está o fato de que somente um computador pode transmitir informações por vez. Caso mais de uma estação tente transmitir informações ao mesmo tempo, temos uma colisão de pacotes. Cada vez que uma colisão acontece na rede é necessário que o computador reenvie o pacote. Esta tentativa de reenvio do pacote acontece várias vezes, até que o barramento esteja disponível para a transmissão e os dados cheguem até o computador receptor.

3.2.2. Anel

Uma rede em anel corresponde ao formato que a rede possui. Neste caso, recebem esta denominação pois os dispositivos conectados na rede formam um circuito fechado, no formato de um anel (ou círculo). Neste tipo de topologia os dados são transmitidos unidirecional mente, ou seja, em uma única direção, até chegar ao computador destino. Desta forma, o sinal emitido pelo computador origem passa por diversos outros computadores, que retransmitem este sinal até que o mesmo chegue ao computador

destino. Vale lembrar aqui que cada computador possui seu endereço que é identificado por cada estação que compõe a rede em anel.



Como vantagens esta topologia estão:

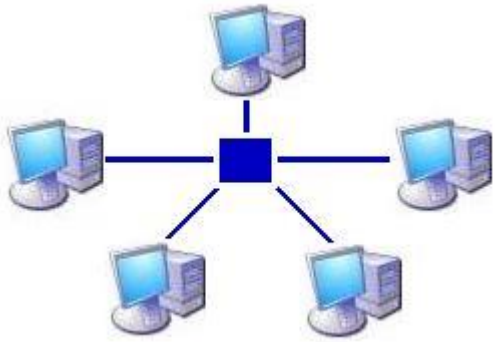
- Inexistência de perda do sinal, uma vez que ele é retransmitido ao passar por um computador da rede.
- Identificação de falhas no cabo é realizada de forma mais rápida que na topologia em barramento.

Como desvantagens desta topologia estão:

- Atraso no processamento de dados, conforme estes dados passam por estações diferentes do computador destino.
- Confiabilidade diminui conforme aumenta o numero de computadores na rede.

3.2.3. Estrela

Uma rede em estrela possui esta denominação, pois faz uso de um concentrador na rede. Um concentrador nada mais é do que um dispositivo (hub, switch ou roteador) que faz a comunicação entre os computadores que fazem parte desta rede. Dessa forma, qualquer computador que queira trocar dados com outro computador da mesma rede, deve enviar esta informação ao concentrador para que o mesmo faça a entrega dos dados.



A topologia em estrela apresenta algumas vantagens, as quais são:

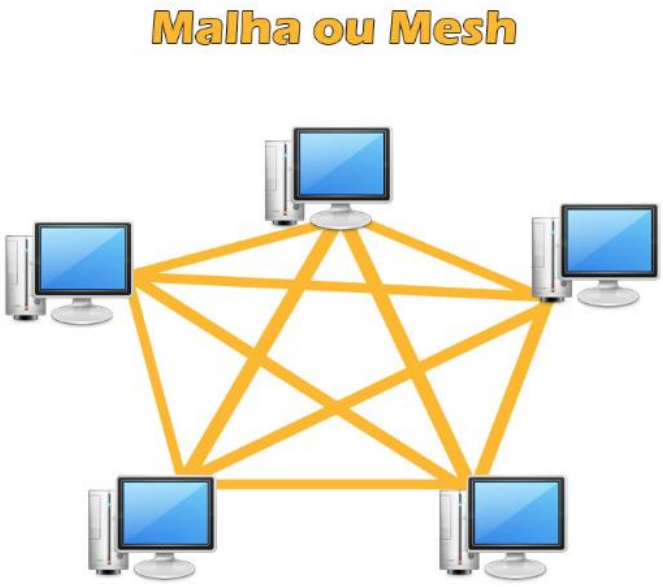
- Fácil identificação de falhas em cabos.
- Instalação de novos computadores ligados a rede, ocorre de forma mais simples que em outras topologias.
- Origem de uma falha (cabo, porta do concentrador ou cabo) é mais simples de ser identificada e corrigida.
- Ocorrência de falhas de um computador da rede não afeta as demais estações ligadas ao concentrador.

Como desvantagens ligadas a esta topologia, estão:

- Custo de instalação aumenta proporcionalmente a distância do computador ao concentrador da rede.
- Caso de falha no concentrador afeta toda a rede conectada a ele.

3.2.4. Malha ou Mesh

A topologia em malha refere-se a uma rede de computadores onde cada estação de trabalho está ligada a todas as demais diretamente. Dessa forma, é possível que todos os computadores da rede, possam trocar informações diretamente com todos os demais, sendo que a informação pode ser transmitida da origem ao destino por diversos caminhos.



Como vantagens deste tipo de rede, podemos citar:

- Tempo de espera reduzido (devido a quantidade de canais de comunicação).
- Problemas na rede não interferem no funcionamento dos demais computadores

Desvantagem:

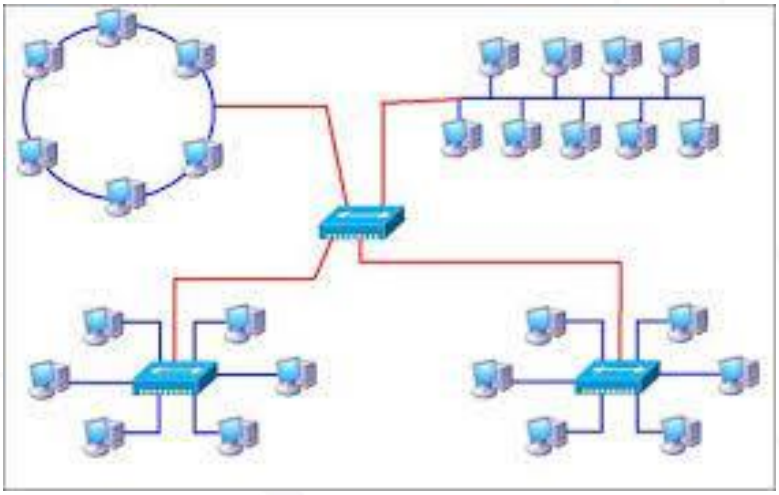
- Alto custo financeiro

3.2.5. Árvore ou Hierárquica

Neste tipo de topologia um concentrador interliga todos os computadores de uma rede local, enquanto outro concentrador interliga as demais redes, fazendo com que um conjunto de redes locais (LAN) sejam interligadas e dispostas no formato de árvore.

3.2.6. Híbrida

Este tipo de topologia é aplicada em redes maiores que uma LAN. É chamada de topologia híbrida pois pode ser formada por diferentes tipos de topologia, ou seja, é formada pela união, por exemplo de uma rede em barramento e uma rede em estrela, entre outras.



4. INTERNET E PROTOCOLOS ASSOCIADOS - PARTE 01

Objetivo

O objetivo deste capítulo é apresentar a primeira parte dos principais protocolos de rede utilizados em conjunto com a internet.

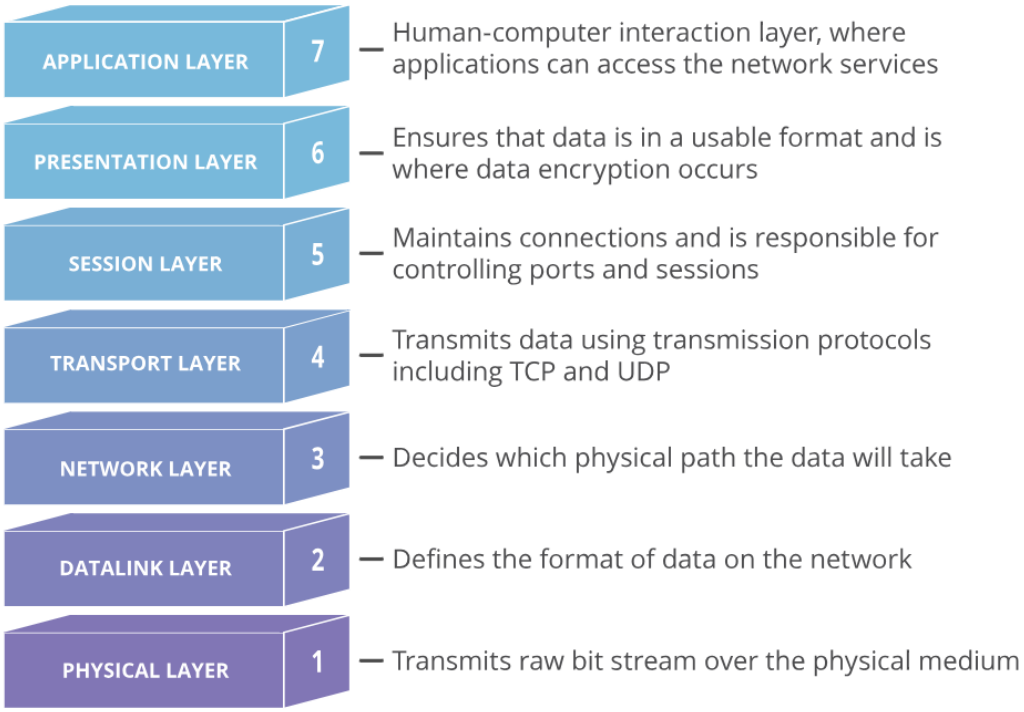
Introdução

No que se refere às redes, um protocolo é um conjunto de regras para formatação e processamento de dados. Os protocolos de rede são como uma linguagem em comum para computadores. Os computadores dentro de uma rede podem usar softwares e hardwares muito diferentes; entretanto, o uso de protocolos permite que eles se comuniquem uns com os outros independentemente dessas diferenças.

4.1. Modelo OSI

O modelo de interconexão de sistemas abertos (OSI) é um modelo conceitual criado pela Organização Internacional de Normalização que permite que diversos sistemas de comunicação se comuniquem usando protocolos padronizados. Em poucas palavras, o OSI fornece um padrão para que diferentes sistemas de computadores possam se comunicar.

O modelo OSI pode ser considerado a linguagem universal da rede de computadores. Ele se baseia no conceito de dividir um sistema de comunicação em sete camadas abstratas, empilhadas umas sobre as outras.



Para que a comunicação entre computadores seja realizada corretamente, é necessário que ambos os computadores estejam configurados segundo os mesmos parâmetros e obedeçam aos mesmos padrões de comunicação.

A rede é dividida em camadas, cada uma com uma função específica. Os diversos tipos de protocolos de rede variam de acordo com o tipo de serviço utilizado e a camada correspondente. Conheça a seguir as principais camadas e seus tipos de protocolos principais:

Camada de aplicação: WWW, HTTP, SMTP, Telnet, FTP, SSH, NNTP, RDP, IRC, SNMP, POP3, IMAP, SIP, DNS, PING;

Camada de transporte: TCP, UDP, RTP, DCCP, SCTP;

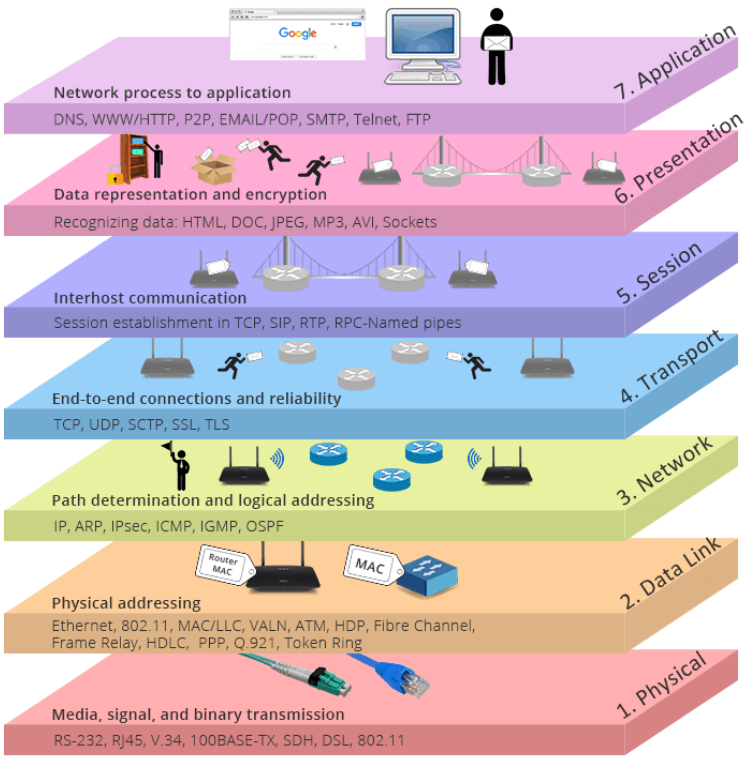
Camada de rede: IPv4, IPv6, IPsec, ICMP;

Camada de ligação física: Ethernet, Modem, PPP, FDDi.

Abaixo podemos ver a função de cada camada e os respectivos protocolos que atuam em cada camada:

Camada Modelo OSI	Função da Camada	Protocolos da Camada
7 - Aplicação	Camada em que estão os serviços e protocolos que compõem os aplicativos.	Http, https, ssh, telnet, pop, snmp, smtp, ftp.
6 - Apresentação	Formata os dados para serem apresentados à camada de aplicação.	ASCII, jpg, tls
5 - Sessão	Responsável por iniciar e encerrar as conexões de rede.	Rpc, sql, nfs,
4 - Transporte	Proporciona comunicação fim-a-fim entre os dispositivos finais	Tcp, udp, sctp, dccp
3 - Redes	Fornece o roteamento dos pacotes entre o dispositivo de origem e o destino	Ipv4, arp, ipv6, icmp, arp
2 - Enlace de Dados	Responsável por controlar como os dados vão acessar o meio físico.	Ethernet, 802.11, hdlc, frame relay, ppp
1 - Física	Responsável pelos meios de conexão(interfaces) utilizados para trafegar os dados pelas redes de computadores.	Modem, 1000base-TX, hub, RS-232, Rj45

Na prática temos a seguinte representação do modelo OSI:



4.2. IP

O protocolo IP, do termo em inglês Internet Protocol (Protocolo de Internet) faz parte da camada de internet e é um dos protocolos mais importantes da web. Ele permite a elaboração e transporte dos pacotes de dados, porém sem assegurar a sua entrega.

O destinatário da mensagem é determinado por meio dos campos de endereço IP (endereço do computador), máscara de sub rede (determina parte do endereço que se refere à rede) e o campo gateway estreita por padrão (permite saber qual o computador de destino, caso não esteja localizado na rede local).

4.3. TCP/IP

Trata-se do acrônimo de dois protocolos combinados. São eles o TCP (Transmission Control Protocol — Protocolo de Controle de Transmissão) e IP (Internet Protocol — Protocolo de Internet). Juntos, são os responsáveis pela base de envio e recebimento de dados por toda a internet. Essa pilha de protocolos é dividida em 4 camadas:

Aplicação: usada para enviar e receber dados de outros programas pela internet. Nessa camada estão os protocolos HTTP, FTP e SMTP;

Transporte: responsável por transportar os arquivos dos pacotes recebidos da camada de aplicação. Eles são organizados e transformados em outros menores, que serão enviados à rede;

Rede: os arquivos empacotados na camada de transporte são recebidos e anexados ao IP da máquina que envia e recebe os dados. Em seguida, eles são enviados pela internet;

Interface: é a camada que executa o recebimento ou o envio de arquivos na web.

4.4. FTP

Significa Protocolo de Transferência de Arquivos (do inglês File Transfer Protocol). É a forma mais simples para transferir dados entre dois computadores utilizando a rede.

O protocolo FTP funciona com dois tipos de conexão: a do cliente (computador que faz o pedido de conexão) e do servidor (computador que recebe o pedido de conexão e fornece o arquivo ou documento solicitado pelo cliente).

O FTP é útil caso o usuário perca o acesso ao painel de controle do seu site. Assim sendo,essa ferramenta pode ser usada para realizar ajustes página, adicionar ou excluir arquivos, ou ainda solucionar qualquer outra questão no site.

4.5. SFTP

Simple Transfer Protocol (Protocolo de Transferência Simples de Arquivos) consiste no protocolo FTP acrescido de uma camada de proteção para arquivos transferidos.

Nele, a troca de informações é feita por meio de pacotes com a tecnologia SSH (Secure Shell – Bloqueio de Segurança), que autenticam e protegem a conexão entre cliente e servidor. O usuário define quantos arquivos serão transmitidos simultaneamente e define um sistema de senhas para reforçar a segurança.

4.6. SSH

SSH (Secure Shell) é um dos protocolos específicos de segurança de troca de arquivos entre cliente e servidor. Funciona a partir de uma chave pública. Ela verifica e autentica se o servidor que o cliente deseja acessar é realmente legítimo.

O usuário define um sistema de proteção para o site sem comprometer o seu desempenho. Ele fortifica a segurança do projeto e garante maior confiança e estabilidade na transferência de arquivos.

4.7. SSL

O protocolo SSL (Secure Sockets Layer — Camada de Portas de Segurança) permite a comunicação segura entre os lados cliente e servidor de uma aplicação web, por meio de uma confirmação da identidade de um servidor e a verificação do seu nível de confiança.

Ele age como uma subcamada nos protocolos de comunicação na internet (TCP/IP). Funciona com a autenticação das partes envolvidas na troca de informações.

A conexão SSL é sempre iniciada pelo cliente, que solicita conexão com um site seguro. O browser, então, solicita o envio do Certificado Digital e verifica se ele é confiável, válido, e se está relacionado ao site que fez o envio. Após a confirmação das informações, a chave pública é enviada e as mensagens podem ser trocadas.

5. INTERNET E PROTOCOLOS ASSOCIADOS - PARTE 02

Objetivo

O objetivo deste capítulo é apresentar a segunda parte dos principais protocolos de rede utilizados em conjunto com a internet.

Introdução

No que se refere às redes, um protocolo é um conjunto de regras para formatação e processamento de dados. Os protocolos de rede são como uma linguagem em comum para computadores. Os computadores dentro de uma rede podem usar softwares e hardwares muito diferentes; entretanto, o uso de protocolos permite que eles se comuniquem uns com os outros independentemente dessas diferenças.

5.1. HTTP

HTTP é a sigla para Hypertext Transfer Protocol, que significa Protocolo de Transferência de Hipertexto. Ele é o mais básico e usado para navegação em sites da internet.

O protocolo HTTP funciona também como uma conexão entre o cliente e o servidor. Neste caso, o cliente é o navegador que você usa para acessar a internet. E o servidor é aquele em que um site ou domínio está hospedado na rede.

O navegador envia um pedido de acesso a uma página. Essa requisição acontece quando colocamos o endereço de algum site no campo de buscas no navegador. É assim que se acessa qualquer site na rede.

Enquanto isso, o servidor manda uma resposta de permissão de acesso. Com ela, vêm os arquivos que formam a página que o usuário que acessar. Além, também, das informações de hipertexto que fazem outras requisições para levar o leitor a outras páginas através de links.

Se a solicitação vier com algum problema, como o Erro 500, o usuário não consegue acessar o site.

5.2. HTTPS

HTTPS é a sigla para Hyper Text Transfer Secure, que significa Protocolo de Transferência de Hipertexto Seguro.

O protocolo HTTPS é e funciona de forma exatamente igual ao HTTP. A diferença da letra “S” na sigla é uma camada extra de proteção, indicando que sites e domínios que possuem esse protocolo são seguros para o usuário acessar.

O protocolo HTTPS é muito usado por sites com sistemas de pagamentos que dependem proteção para assegurar dados, informações de conta e cartão de crédito dos usuários.

Essa proteção é feita por certificação digital, que cria uma criptografia para impedir que ameaças e ataques na internet tenham acesso indevido às informações dos usuários.

O HTTPS aparece em um navegador quando o site acessado possui um Certificado SSL instalado. O SSL cria um canal de proteção entre o cliente e o servidor, adicionando a letra “S” ao HTTP e reforçando uma camada extra de segurança.

5.3. ICMP

Sigla para Internet Control Message Protocol (Protocolo de Mensagens de Controle da Internet). Esse protocolo autoriza a criação de mensagens relativas ao IP, mensagens de erro e pacotes de teste.

Ele permite gerenciar as informações relativas a erros nas máquinas conectadas. O protocolo IP não corrige esses erros, mas os mostra para os protocolos das camadas vizinhas. Por isso, o protocolo ICMP é usado pelos roteadores para assinalar um erro, chamado de Delivery Problem (Problema de Entrega).

5.4. SMTP

Protocolo para transferência de e-mail simples (Simple Mail Transfer Protocol) é comumente utilizado para transferir e-mails de um servidor para outro, em conexão ponto a ponto.

As mensagens são capturadas e enviadas ao protocolo SMTP, que as encaminha aos destinatários finais em um processo automatizado e quase instantâneo. O usuário não tem autorização para realizar o download das mensagens no servidor.

5.5. TELNET

Protocolo de acesso remoto. É um protocolo padrão da Internet que permite obter uma interface de terminais e aplicações pela web. Fornece regras básicas para ligar um cliente a um intérprete de comando.

Ele tem como base uma conexão TCP para enviar dados em formato ASCII codificados em 8 bits, entre os quais se intercalam sequências de controle Telnet. Assim, fornece um sistema orientado para a comunicação bidirecional e fácil de aplicar.

5.6. POP3

Acrônimo para Post Office Protocol 3 (Protocolo de Correios 3). É um protocolo utilizado para troca de mensagens eletrônicas. Funciona da seguinte forma: um servidor de email recebe e armazena mensagens. O cliente se autentica ao servidor da caixa postal para poder acessar e ler as mensagens.

Assim, as mensagens armazenadas no servidor são transferidas em sequência para o computador do cliente. Quando, a conexão é encerrada as mensagens ainda são acessadas no modo offline.

5.7. DHCP

DHCP é o acrônimo para Dynamic Host Configuration Protocol, que significa, em português adaptado, Protocolo de Configuração Dinâmica de Endereços de Rede. Ele permite que os computadores consigam um endereço de IP automaticamente.

Por meio de um servidor, o protocolo DHCP é capaz de obter, sem a necessidade de configuração manual, endereços de IPs para cada um dos computadores (ou dispositivos móveis) ligados a uma rede de internet.

Uma vez que uma máquina obtém um endereço de IP, ele fica indisponível para uso naquele momento. Quando ela é desligada ou desconectada da internet, o endereço de IP, antes volta a ficar disponível para ser usado por qualquer nova máquina ligada na conexão.

O protocolo DHCP funciona de três maneiras diferentes. São elas:

Automática: Um IP é definido automaticamente para uma máquina que se conecta na. Neste caso, uma quantidade de IPs é delimitada para ser usada dentro de uma rede de internet. Qualquer computador que se ligar a ela recebe, automaticamente, um, destes IPs definidos.

Dinâmica: Como o termo sugere, uma máquina que se conecta à rede de internet recebe um IP dinâmico pelo período em que continuar conectado. Se a máquina for desligada ou se desconectar da rede, ela perde este IP usado e usa um novo assim que a conexão for restabelecida.

Manual: O protocolo DHCP define um IP para uma máquina de acordo com o valor de MAC (Medium Access Control) da placa de rede em que ela está conectada. Este IP é único e estático, sendo que este recurso é usado quando é preciso que um computador tenha um IP fixo.

6. COMPUTAÇÃO EM NUVEM - PARTE 01

Objetivo

O objetivo deste capítulo é apresentar a primeira parte dos conceitos de computação em nuvem.

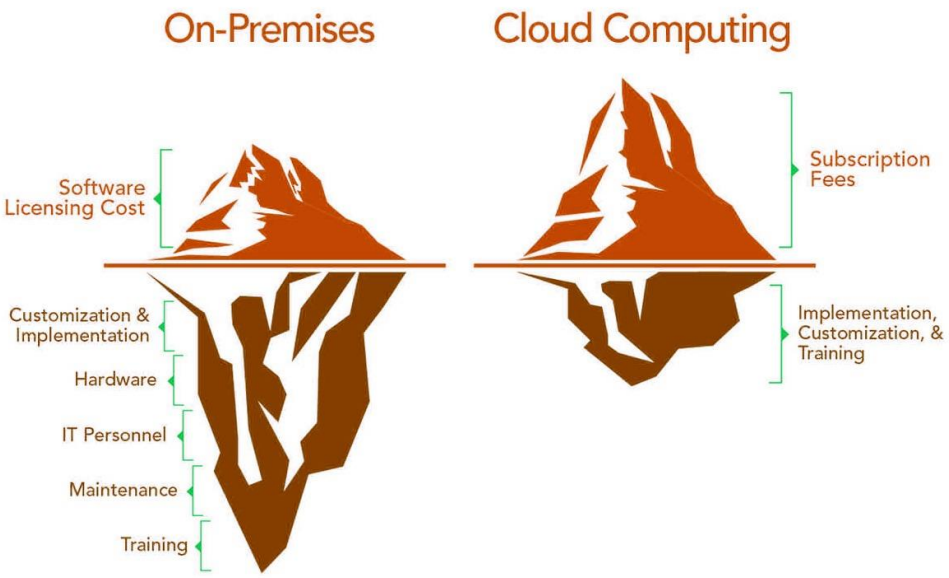
Introdução

Com tantas diferenças entre as organizações e as novas tecnologias trazidas pela transformação digital, definitivamente não existe uma solução única para todos. A chave é, em vez disso, procurar uma solução que ajude sua empresa a economizar custos e aumentar a eficiência. A ampla adoção da cloud computing levou muitos fornecedores a mudar o foco dos modelos de entrega local para a nuvem, com a tecnologia cloud revolucionando os recursos de computação on-premise de trabalho. No entanto, para empresas que ainda não mudaram suas aplicações ou armazenamento de dados para a nuvem, a pergunta “Qual é a melhor solução para o meu negócio?” Pode ter vindo à mente uma ou duas vezes. Dito isso, existem empresas que ainda preferem manter uma infraestrutura de armazenamento de dados on-premise em vez de utilizar a cloud computing. Ambas as abordagens oferecem suas próprias vantagens, mas pode não ser fácil distinguir qual seria a melhor para certos tipos de organizações sem a devida consideração.

6.1. Infraestrutura On-premise vs Infraestrutura Cloud computing

Não é nenhuma surpresa que a cloud computing tenha crescido em popularidade, principalmente pela oferta de flexibilidade, economia de tempo e dinheiro até o aumento de agilidade e escalabilidade.

Por outro lado, o modelo on-premise - onde os servidores ficam localizados na própria empresa - foi a única opção para as organizações por um longo tempo. E até pode continuar a atender adequadamente às suas necessidades de negócios. Além disso, o armazenamento local é confiável, seguro e permite que as empresas mantenham um nível de controle que a nuvem geralmente não possibilita.



6.1.1. On-premise

Quer a empresa coloque suas aplicações na nuvem ou decida mantê-los on-premise, a segurança dos dados sempre será primordial. Mas, para as empresas em setores altamente regulamentados, geralmente a decisão é manter tudo 'dentro de casa'. Saber que seus dados estão localizados em seus servidores internos e infraestrutura de TI também pode fornecer mais tranquilidade de qualquer maneira.

A desvantagem do on-premise é que os custos associados ao gerenciamento e manutenção de toda a infraestrutura podem ser exponencialmente mais altos do que um ambiente de cloud computing.

Uma configuração local requer **hardware de servidor interno, licenças de software, recursos de integração e colaboradores de TI disponíveis** para oferecer suporte e gerenciar possíveis problemas que possam surgir. Isso nem mesmo leva em consideração a quantidade de manutenção pela qual uma empresa é responsável quando algo quebra ou não funciona.

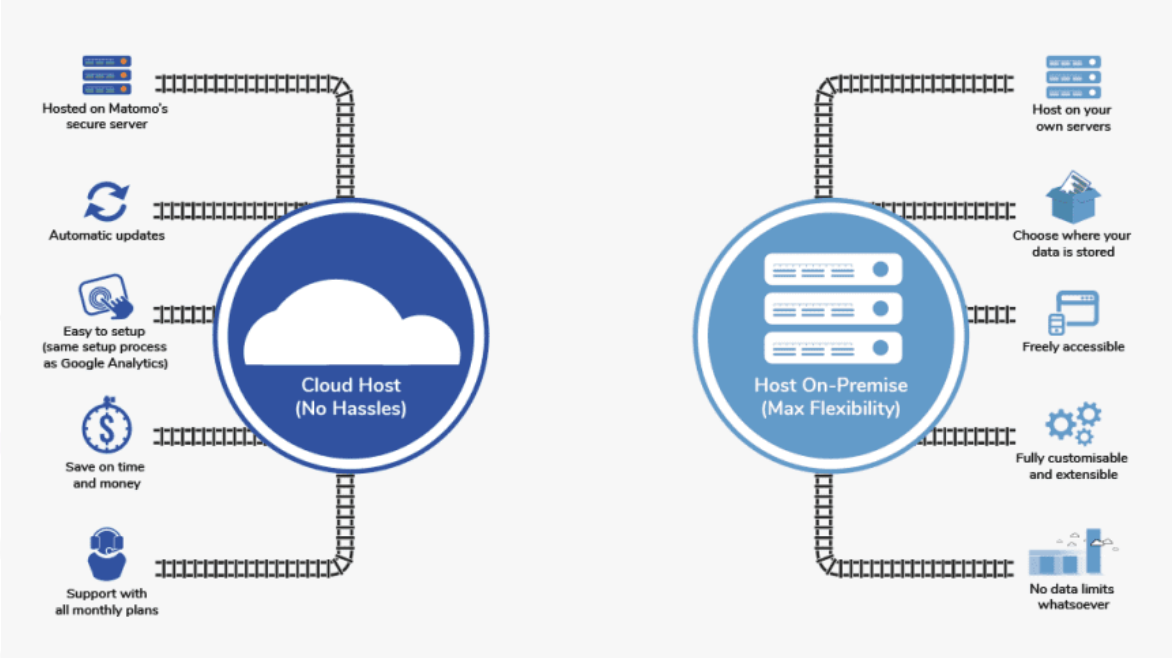
6.1.2. Cloud computing

A cloud computing difere do modelo on-premise de uma maneira crítica. Uma empresa hospeda tudo internamente em um ambiente local, enquanto em um ambiente de nuvem um provedor terceirizado hospeda tudo isso para você. **Isso permite que as**

empresas paguem conforme a necessidade e aumentem ou diminuam o armazenamento contratado com eficácia, dependendo do uso, dos requisitos do usuário e do crescimento da empresa.

Um servidor baseado em nuvem utiliza tecnologia virtual para hospedar as aplicações da empresa externamente. **Não há despesas com manutenção de hardware, é possível fazer backup dos dados regularmente e as empresas só precisam pagar pelos recursos que usam.** Para as organizações que planejam uma expansão agressiva, a nuvem tem um apelo ainda maior porque permite que você se conecte com clientes, parceiros e outras empresas em qualquer lugar com o mínimo de esforço.

Além disso, **a cloud computing oferece provisionamento quase instantâneo porque tudo já está configurado**. Assim, qualquer novo software integrado ao seu ambiente está pronto para ser usado imediatamente após a assinatura. Com o provisionamento instantâneo, qualquer tempo gasto na instalação e configuração é eliminado e os usuários podem acessar o aplicativo imediatamente.

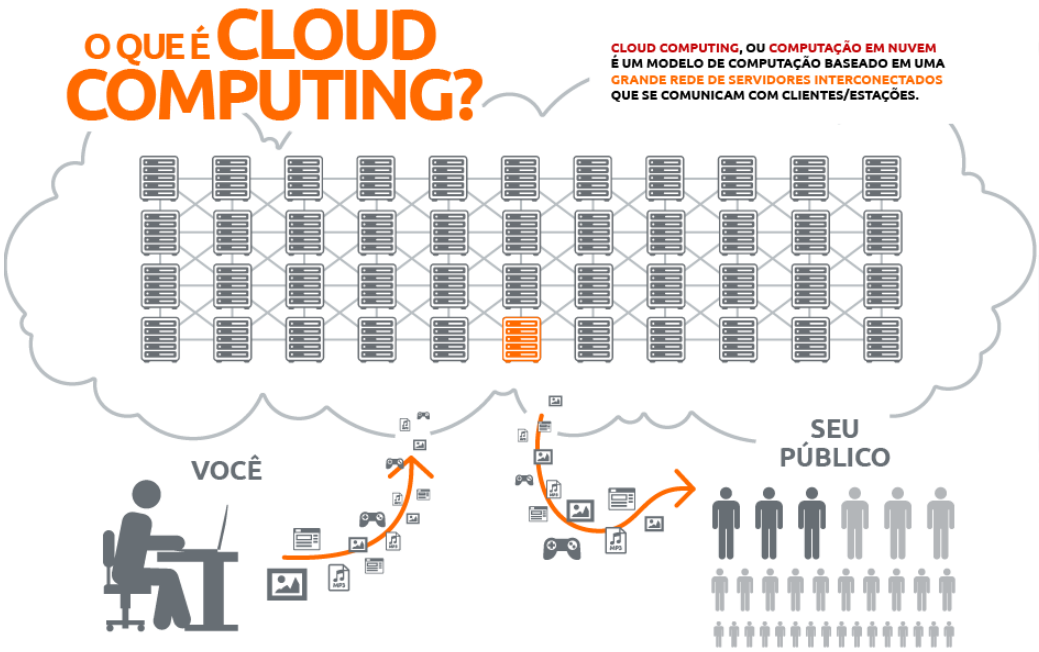


6.2. Como funciona a cloud?

A computação em nuvem funciona de maneira diferente dos modelos convencionais de tecnologia da informação. Em vez de ter equipamentos próprios, a nuvem é composta

por uma série de servidores interligados que oferecem vasto armazenamento e processamento de dados.

Com a cloud, você pode ajustar os recursos destes servidores de acordo com suas necessidades, alocando capacidade de processamento, espaço em disco, memória e largura de banda. Isso é feito de forma fácil e rápida, sem precisar reinstalar nada. Além disso, a nuvem permite que você ajuste esses recursos a qualquer momento, conforme suas necessidades mudam.



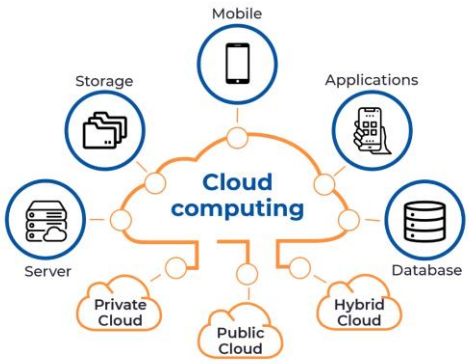
6.3. Para que serve a cloud?

Usando a computação em nuvem, as organizações podem usar recursos compartilhados de computação e armazenamento, em vez de criar, operar e melhorar a infraestrutura por conta própria.

É um modelo que permite os seguintes recursos:

- Os usuários podem provisionar e liberar recursos sob demanda.
- Os recursos podem ser redimensionados para cima ou para baixo automaticamente, dependendo da carga.

- Os recursos são acessíveis em uma rede com segurança adequada.
- Os provedores de serviços em nuvem podem ativar um modelo de pagamento conforme o uso, em que os clientes são cobrados com base no tipo de recursos e por uso.



6.4. Quais as vantagens da cloud?

Aqui está uma lista de algumas das vantagens mais importantes que a cloud computing oferece:

Economia de custo: Construir nossos próprios servidores e ferramentas é demorado e caro, pois precisamos solicitar, pagar, instalar e configurar hardware caro, muito antes de precisarmos dele. No entanto, usando a cloud, pagamos apenas pelo valor que usamos e quando usamos os recursos de computação. Dessa maneira, a computação em nuvem é econômica.

Escalabilidade: Uma das grandes vantagens é a elasticidade, onde você pode aumentar e diminuir a capacidade da sua máquina de forma simples com apenas alguns cliques. A cloud computing então se tornou atrativa. Ela não nasceu para resolver o problema da sazonalidade de acessos ou picos de acessos, mas encaixou de ser essa a maior atratividade.

Agilidade e Inovação: Possibilita a inovação com mais agilidade, você pode disponibilizar recursos de TI de form rápida e conforme a necessidade com baixo custo, implantando vários servidores em alguns instantes.

Confiabilidade: Fornece muito mais serviços gerenciados, confiáveis e consistentes do que uma infraestrutura de TI interna (on premises). Garante 24x7 e 365 dias de serviço. Se algum servidor falhar, os aplicativos e serviços hospedados poderão ser facilmente transferidos para qualquer um dos servidores disponíveis.

Armazenamento ilimitado: Fornece capacidade de armazenamento quase ilimitada, ou seja, não precisa se preocupar em ficar sem espaço de armazenamento ou aumentar a disponibilidade atual de espaço de armazenamento.

Backup e recuperação: Armazenar dados na nuvem, fazer backup e restaurar os mesmos é relativamente mais fácil do que armazená-los em um dispositivo físico. Os provedores de serviços cloud também possuem tecnologia suficiente para recuperação de dados, portanto, há a conveniência de recuperar os dados a qualquer momento.

Acesso fácil às informações: Depois de migrar para a nuvem, você pode ter acesso de qualquer lugar do mundo, desde que haja conexão com a Internet. Existem vários recursos de armazenamento e segurança que variam de acordo com o tipo de nuvem escolhida.

6.5. Tipos de cloud computing

Nuvem pública: Na nuvem pública (public cloud), os provedores de serviços terceirizados disponibilizam recursos e serviços para seus clientes via internet. Os dados do cliente e a segurança relacionada estão na infraestrutura de propriedade dos provedores de serviços. No momento, os principais provedores de nuvem são Amazon AWS, Microsoft Azure e Google Cloud Platform.

Nuvem privada: Uma nuvem privada (private cloud) também fornece recursos quase semelhantes aos da nuvem pública, mas os dados e serviços são gerenciados pela organização ou por terceiros apenas para a organização do cliente. Nesse tipo de nuvem, o controle principal é sobre a infraestrutura, minimizando os problemas relacionados à segurança.

Nuvem híbrida: Uma nuvem híbrida (hybrid cloud) é a combinação de nuvem pública e privada, mas não necessariamente de fornecedores diferentes. A decisão de executar em nuvem pública ou privada geralmente depende de vários parâmetros, como sensibilidade de dados e aplicativos, certificações do setor e padrões, regulamentos, etc.

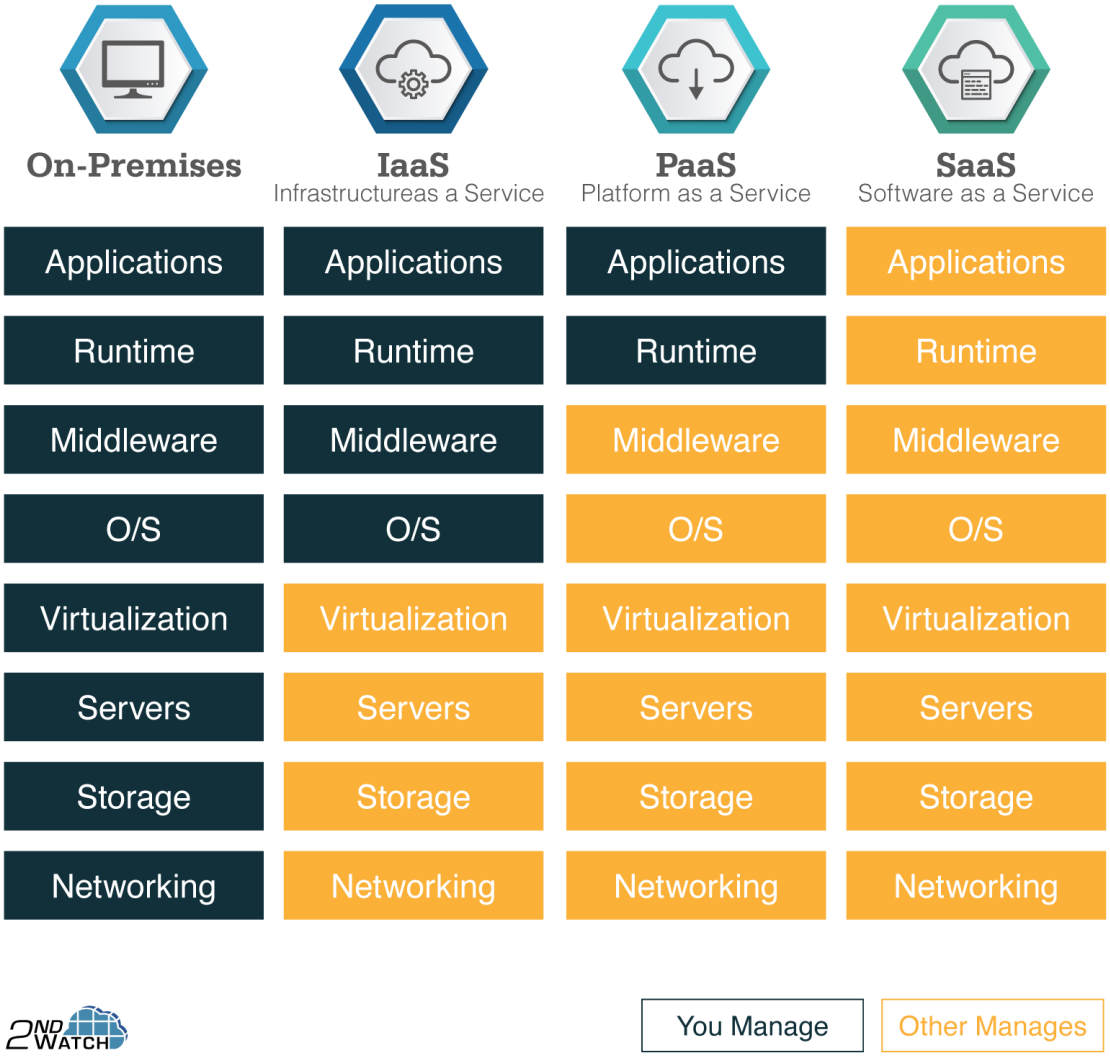
6.6. Modelos de serviço em cloud

IaaS - Infrastructure as a Service: IaaS significa Infraestrutura como Serviço. Ele fornece aos usuários a capacidade de provisionar processamento, armazenamento e conectividade de rede sob demanda. Usando esse modelo de serviço, os clientes podem desenvolver seus próprios aplicativos nesses recursos.

Os principais provedores de IaaS no mundo são: Amazon Web Services; Microsoft; Alibaba e Google.

PaaS - Platform as a Service: PaaS significa Plataforma como Serviço. Aqui, o provedor de serviços fornece vários serviços, como bancos de dados, filas, mecanismos de fluxo de trabalho, e-mails etc. aos seus clientes. O cliente pode usar esses componentes para criar seus próprios aplicativos. Os serviços, a disponibilidade de recursos e o backup de dados são gerenciados pelo provedor de serviços, ajudando os clientes a se concentrarem mais na funcionalidade de seus aplicativos.

Exemplos deste tipo de serviço: Google App Engine; Heroku; RedHat OpenShift; Microsoft Azure Cloud Services; Tsuru e etc.



SaaS - Software as a Service: SaaS significa Software como Serviço. Como o nome sugere, aqui os fornecedores terceirizados fornecem aplicativos de usuário final a seus clientes com alguns recursos administrativos no nível do aplicativo, como a capacidade de criar e gerenciar seus usuários. Também é possível algum nível de personalização, como os clientes podem usar seus próprios logotipos corporativos, cores etc.

Exemplos deste tipo de serviço: ERP; CRM; Google Docs; LinkedIn; Skype; Facebook e etc.

Multicloud: Multicloud é o uso de mais de um provedor de serviços cloud em um ambiente de TI, em vez de depender de um único fornecedor desses serviços (lock-in). O ambiente multicloud normalmente usa dois ou mais fornecedores de nuvem pública (AWS, Azure, Google entre outros), também podem incluir uma nuvem privada, que inclui tecnologia cloud no data center de uma empresa.

A transformação digital do negócio requer a disponibilidade de arquiteturas de TI flexíveis, escaláveis e confiáveis, capazes de suportar os aplicativos mais inovadores e com as melhores relações custo-benefício. É por isso que mais e mais empresas estão decidindo utilizar estratégias de multicloud.

6.7. Porque a nuvem é o (presente) futuro da computação?

Um estudo da consultoria Gartner, aponta que 85% das empresas em todo o mundo irão adotar a nuvem pública até 2025. O relatório indica que investir em cloud é o caminho viável para tornar os serviços digitais ainda mais presentes e relevantes no nosso dia a dia.

Já a pesquisa Futuro da computação em nuvem, realizada pelo Google, ouviu especialistas e líderes de TI. Ela mostra que 87% dos empresários acreditam que investir em soluções de cloud computing será crucial para aumentar os lucros das empresas até 2029.

Talvez esse seja o grande potencial dessa tecnologia: baratear os custos de infraestrutura de TI, permitindo que todos os tipos de clientes usufruam de seus benefícios, garantindo uma maior disponibilidade dos serviços — que sempre podem ser facilmente acessados pela Internet.

Além disso, o estudo da Gartner aponta outro dado interessante: até 2025, a estimativa é de que mais de 95% das novas cargas de trabalhos digitais sejam implementadas em plataformas nativas na nuvem. Em 2021, o volume era de 30%.

Com tantas empresas migrando para a cloud computing, um relatório do Fórum Econômico Mundial de 2020 revela que a expectativa é que, até 2025, o gasto mundial com soluções em cloud deve chegar a 623 bilhões de dólares — em 2021, o gasto estimado era

de US$ 408 bilhões. Isso representa um aumento de mais de 50% em um curto período de tempo.

7. COMPUTAÇÃO EM NUVEM - PARTE 02

Objetivo

O objetivo deste capítulo é apresentar a segunda parte dos conceitos de computação em nuvem.

Introdução

Mesmo com o conceito tendo surgido na década de 60, a primeira vez que "computação em nuvem" foi usado foi em 1997. Hoje, é uma realidade sólida e faz cada vez mais parte da rotina de trabalho e armazenamento de arquivos pessoais. Os três maiores nomes do mercado, a Google Cloud, a Windows Azure e a AWS têm investido em plataformas cada vez melhor desenvolvidas para oferecer a seus usuários maior agilidade e menor custo. A migração de empresas para o cenário Cloud cresce vertiginosamente e compele os provedores de tecnologia nuvem a oferecerem vantagens como escalabilidade, segurança, economia de custos e outros fatores primordiais, o que acelera a competição entre gigantes.

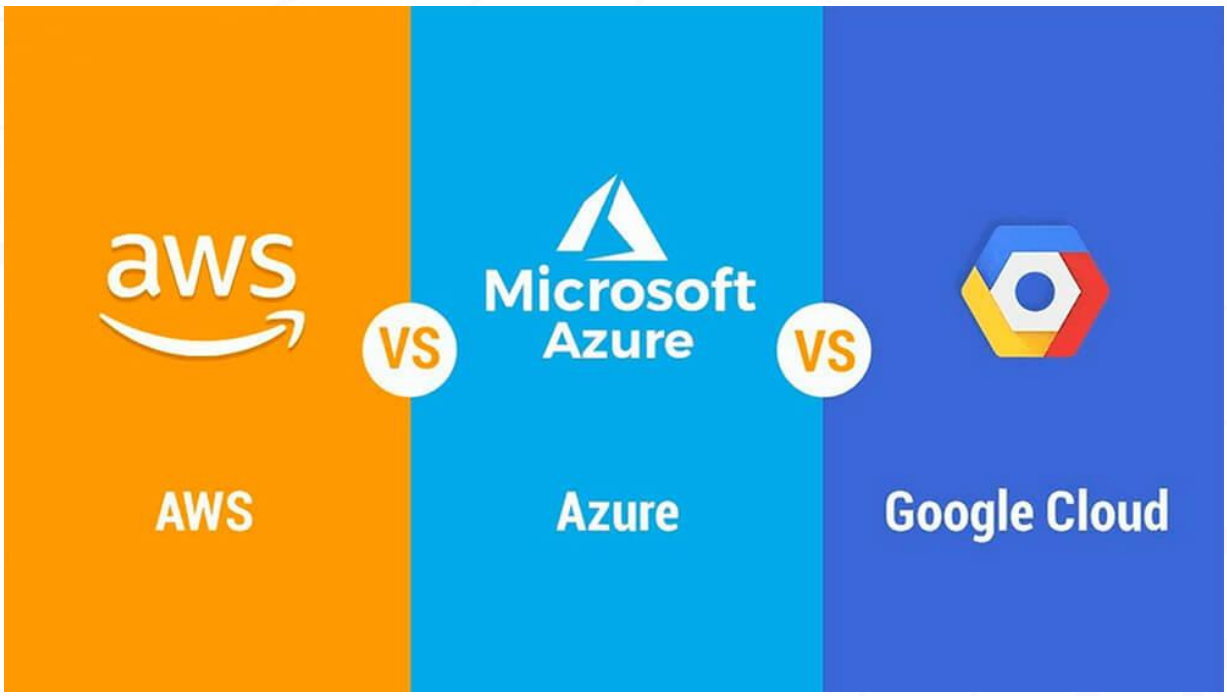
7.1. Panorama do mercado de IaaS (Infraestrutura como Serviço)

Na descrição da Microsoft, desenvolvedora da Azure, IaaS é "um tipo de serviço de computação em nuvem que oferece recursos fundamentais de computação, armazenamento e rede sob demanda e pagos conforme o uso".

Partindo dessa ideia (e da que IaaS é somente um dos quatro tipos de serviços de nuvem, que também contam com o SaaS [software como serviço], o PaaS [plataforma como serviço] e a tecnologia sem servidor), podemos estabelecer que, em panorama de mercado de IaaS:

A AWS (Amazon Web Services) é ainda a grande líder, mandando no mercado por uma vantagem muito expressiva.

A Microsoft com o seu produto Azure tem maior força na modalidade SaaS e a Google Cloud vem crescendo agressivamente e colocou seu nome junto das grandes.



Juntas, ainda que com a AWS isoladamente mandando no mercado, elas comandam mais de 60% do mercado e rendem quase US$ 100 bilhões por ano, conforme o Synergy Research Group em relatório divulgado em junho de 2021.

Somadas com empresas que oferecem o serviço com menor expressividade, chegam a marca de US$ 150 bilhões anuais.

7.2. O que avaliar em um fornecedor de cloud computing?

Escolher entre AWS x Azure x Google pode gerar dúvidas. Afinal, avaliar um fornecedor de cloud computing é uma tarefa complexa – e dizemos porquê. O fator central a ser considerado, em primeiro momento, depende total e completamente das necessidades, da demanda e dos desejos de cada cliente individualmente. Itens como a carga de trabalho executada, por exemplo, devem ser levados em consideração na hora de escolher uma das opções disponíveis no mercado.

Isso porque muitas vezes, são usados vários provedores em diferentes partes de operações para diferentes casos de uso – o que se pode chamar de abordagem de várias nuvens. No entanto, há uma variedade de fatores importantes de diferenciação que afastam as três titãs do mercado, auxiliando a direcionar o interesse dos usuários finais àquela que atende melhor suas exigências.

De forma geral, alguns aspectos centrais são analisados primariamente.

Computação (VMs) e Armazenamento:

As VMs, sigla que designa máquinas virtuais, e a capacidade de armazenamento de dados são aspectos importantes na hora de analisar a melhor plataforma para você. A principal oferta da AWS são as instâncias EC2, que podem ser personalizadas com um grande número de opções.

Enquanto isso, a Azure oferece bastante força em duas Máquinas Virtuais (VMs), com outras ferramentas, como seu serviço de escalonamento automático, por exemplo..

Os VMs da Google, chamados Compute Engine são rápidos, vêm com armazenamento em disco permanente, prometem desempenho consistente e são altamente personalizáveis dependendo das necessidades do cliente.

Infraestruturas de Rede:

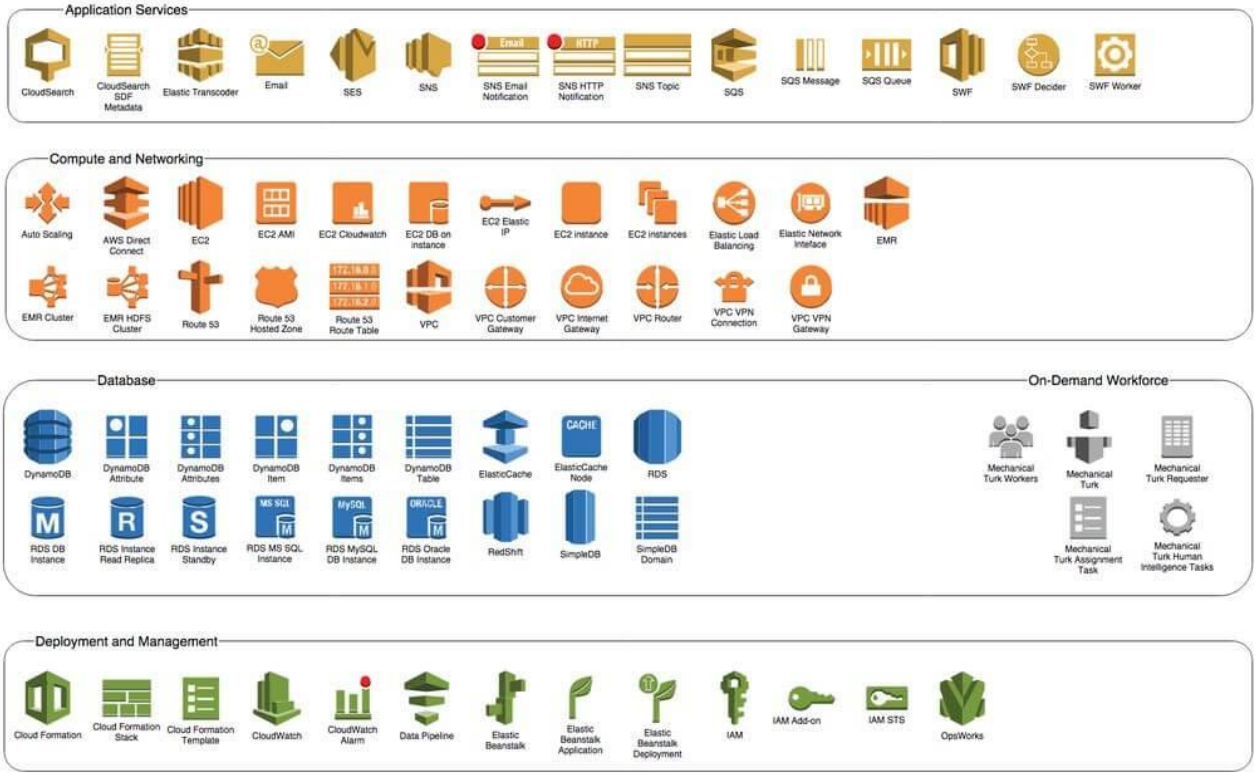
Sobre infraestrutura de rede, as três empresas oferecem recursos sensacionais, com balanceamento de carga de servidor automatizado e conectividade com sistemas locais.

Suporte e Uptime:

Os três provedores oferecem suporte a bancos de dados relacionais. O Microsoft Azure usa banco de dados SQL, a AWS usa o Amazon Relational Database Service, Redshift e a Google Cloud Plataform usa o SQL.

7.3. AWS

A Amazon Web Services tem seu foco voltado a ser um provedor amplo de serviços de TI, abrangendo nativos da nuvem e borda até ERP e cargas de trabalho essenciais. A empresa possui operações geograficamente diversificadas e atende clientes de todas as demandas, desde startups em seu estágio inicial até grandes empresas consolidadas no mercado.



7.3.1. Prós e Contras da AWS

A maior força da Amazon é o domínio do mercado de nuvem pública. Em seu Quadrante Mágico de Infraestrutura de Nuvem como Serviço, em todo o mundo, o Gartner observou: “A AWS é líder em participação de mercado em IaaS na nuvem há mais de 10 anos”.

Parte da razão de sua popularidade é, sem dúvida, o enorme escopo de suas operações. A AWS possui uma enorme e crescente variedade de serviços disponíveis, bem como a rede mais abrangente de data centers em todo o mundo.

O relatório do Gartner resumiu, dizendo: “A AWS é o provedor mais maduro e pronto para empresas, com os recursos mais profundos para administrar um grande número de usuários e recursos”. A grande fraqueza da Amazon está relacionada ao custo. Muitas empresas acham difícil entender a estrutura de custos da empresa e gerenciar esses custos efetivamente ao executar um alto volume de cargas de trabalho no serviço.

7.3.2. Quando escolher AWS

A AWS é uma ótima opção para cargas de trabalho analíticas e web, até migrações de data center em grande escala, a AWS fornece uma série de serviços. Quando se trata de computação, a AWS fornece a maior variedade de tipos de VM. Atualmente, a AWS também possui as mais altas opções de computação e armazenamento disponíveis no mercado.

Sua ampla variedade de tipos de VM (136 tipos de VM e mais de 26 famílias de VM) permite que os clientes executem tudo, desde pequenas cargas de trabalho na web até as maiores cargas de trabalho. Para aprendizado de máquina e cargas de trabalho de IA, a AWS também fornece as configurações mais altas dos tipos de VM habilitados para GPU.

Para cargas de trabalho que exigem locação única por motivos de conformidade e regulamentação, a AWS agora também fornece Bare-Metal-as-a-Service. O armazenamento em bloco vem com uma variedade de opções, como redimensionamento dinâmico, diferentes tipos de disco (magnético e SSD).

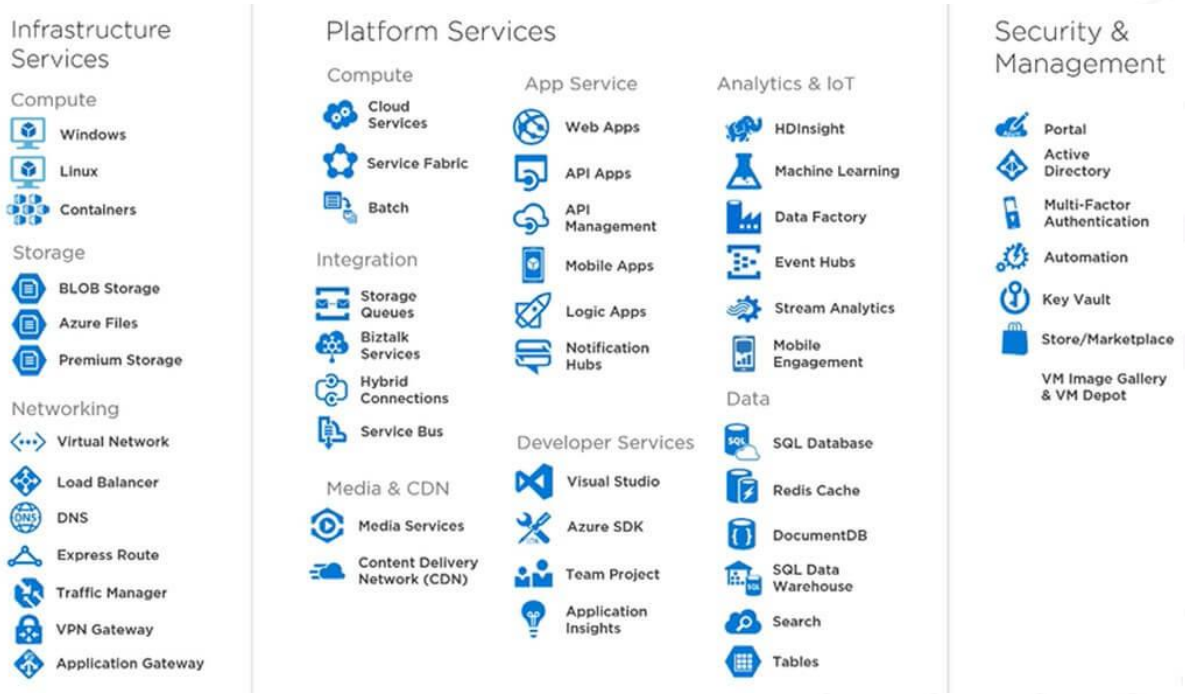
Ao contrário de outros CSPs, a AWS não restringe IOPS por tamanho de volume. Você pode provisionar IOPS por um custo extra até para discos pequenos. Na frente do banco de dados relacional gerenciado, a AWS oferece suporte a bancos de dados gerenciados para MySQL, PostgreSQL, MariaDB, Oracle (SE e EE) e MS SQL (edições Web e Enterprise).

Além disso, eles têm seu próprio banco de dados compatível com MySQL e PostgreSQL, que oferece desempenho semelhante ao Oracle por um investimento baixo. Para bancos de dados NoSQL, a AWS disponibiliza seu produto DynamoDB há mais de meia década. A AWS é um defensor e fornece uma variedade de bancos de dados NoSQL criados para esse fim. Isso inclui DynamoDB, Neptune e Elasticache.

Para segurança de rede, a AWS lançou serviços gerenciados para proteção contra DDoS (AWS Shield) e Web Application Firewall (WAF), juntamente com o AWS Inspector, o AWS Config e o CloudTrail para gerenciamento e auditoria de inventário e políticas. O GuardDuty fornece detecção de ameaças. A AWS atende a cargas de trabalho do governo dos EUA em regiões separadas do GovCloud nos EUA (CIA e FBI).

7.4. Microsoft Azure

O Microsoft Azure é forte em todos os casos de uso, que incluem a computação estendida em nuvem e de borda. Sua capacidade excepcional garante ao cliente corporativo, principalmente, uma experiência sólida como só a Microsoft poderia – inclusive o suporte Windows.



Com foco de investimento em melhorias na plataforma, fornecendo um grande leque de serviços, suas operações são geograficamente diversificadas e seus clientes tendem a ser empresas de médio e grande porte.

A Azure é a concorrente que mais conseguiu se aproximar da líder AWS. Em 2021, enquanto a AWS comandava 33% do nicho no mercado, a Azure conseguiu 20% de expressão, o que é uma porcentagem bastante elevada.

7.4.1. Prós e contras do Microsoft Azure

A Microsoft chegou atrasada ao mercado de nuvem, mas deu um passo à frente, adotando essencialmente o software local – Windows Server, Office, SQL Server, Sharepoint, Dynamics Active Directory, .Net e outros – e adaptando-o novamente para a nuvem.

Um grande motivo para o sucesso do Azure é a integração com as aplicações/softwares da Microsoft.

Como o Azure está totalmente integrado a esses outros aplicativos, as empresas que usam muitos softwares da Microsoft geralmente acham que também faz sentido usar o Azure.

7.4.2. Quando escolher o Azure

O Azure é uma plataforma de nuvem de grande importância no mercado com uma variedade de recursos, que pode ser uma plataforma preferida para clientes que já estão usando produtos da Microsoft. Embora o Azure ofereça suporte a vários serviços baseados em produtos de código aberto, o portfólio da Microsoft na nuvem é o que o diferencia dos clientes.

O Azure tem mais de 151 tipos de VMs e 26 famílias que oferecem suporte a tudo, desde pequenas cargas de trabalho até as cargas de trabalho HPC, Oracle e SAP. O Azure possui Windows e vários tipos de Linux (RHEL, CentOS, SUSE, Ubuntu). O Azure tem uma família separada de instâncias para cargas de trabalho de ML/AI.

Se você precisar executar cargas de trabalho de última geração que exijam até 128 vCPU e memória de 3,5 TB, o Azure consegue. Se você possui licenças existentes para Windows OS, MS-SQL e as traz para a nuvem (BYOL) por meio do Microsoft License Mobility Program, o Azure é a opção.

O Azure também foi o primeiro player de nuvem a reconhecer a tendência da nuvem híbrida. O Azure também forneceu suporte para dispositivos de armazenamento híbridos como o StorSimple, que era único no espaço da nuvem pública. Se você possui um data center com cargas de trabalho predominantemente da Microsoft e precisa fazer uma migração em grande escala para a nuvem, aproveitando as ferramentas conhecidas, o Azure fornece ferramentas e serviços, como o Azure Site Recovery.

Quando se trata de bancos de dados SQL e NoSQL, o Azure tem um conjunto de serviços bastante completo. Ele fornece o MS SQL Server e o SQL Datawarehouse Gerenciados. O Azure também fornece bancos de dados gerenciados para MySQL,

PostgreSQL e MariaDB. Ele fornece uma API compatível com MongoDB, Cassandra, Gremlin (Graph) e Armazenamento de Tabela do Azure.

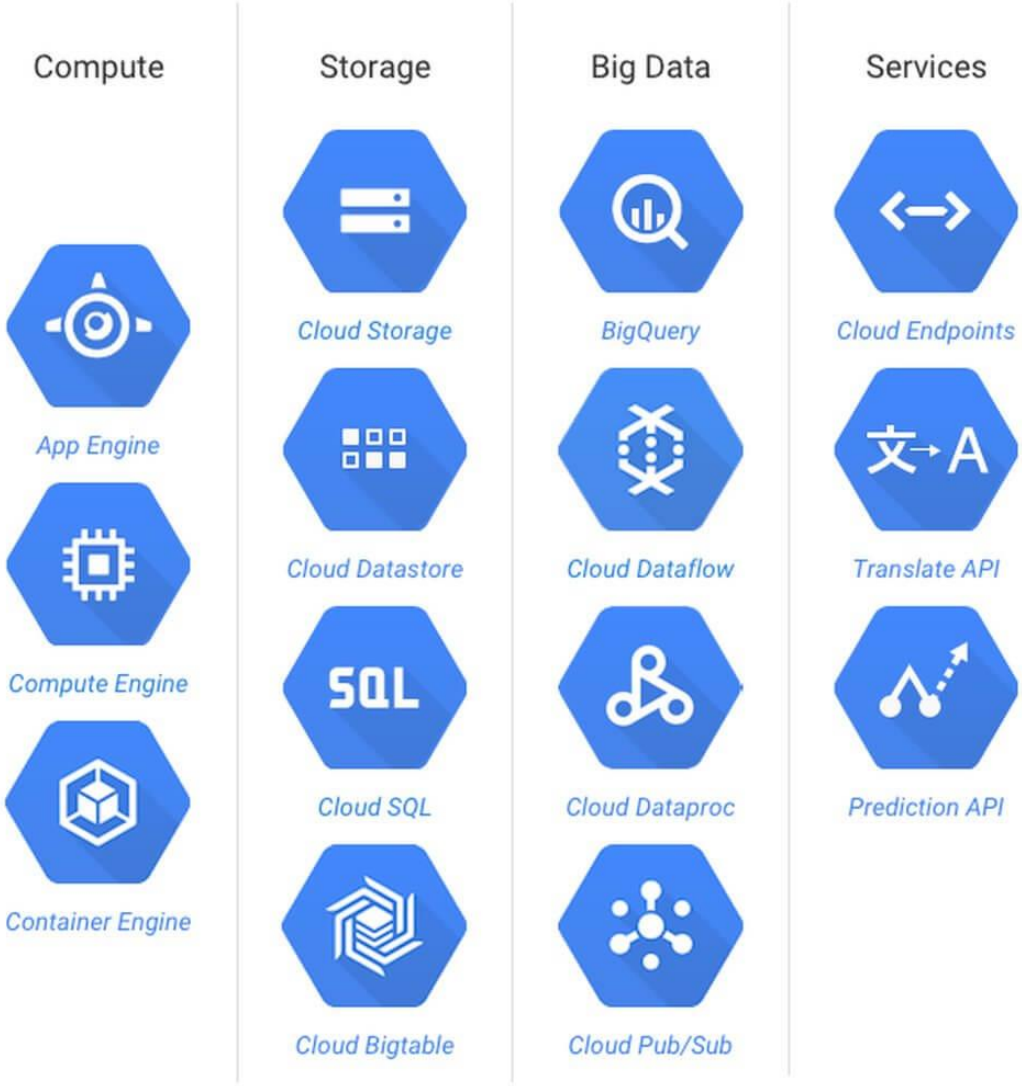
Se você precisar executar vários modelos de dados gerenciados, incluindo modelos de dados de documentos, gráficos, valores-chave, tabelas e famílias de colunas em uma única nuvem, o Cosmos pode ser a melhor opção. O Microsoft Azure Cosmos DB é nomeado líder no relatório Forrester WaveTM: NoSQL Big Data, relatório do 1º trimestre de 2019.

Além do modelo de cobrança pagamento por uso com cartão de crédito e outros modos de faturamento, os clientes com contas corporativas existentes podem comprar pré-assinaturas do Azure como parte de suas renovações anuais. Isso é útil para clientes que desejam orçamentar os gastos anuais da nuvem com antecedência. Evitando a incerteza e as aprovações adicionais de orçamento para o meio do ano.

A mobilidade de licenças na nuvem para produtos da Microsoft também é relativamente fácil para clientes com vários produtos da Microsoft em execução no local.

7.5. Google Cloud Platform (GCP)

O Google Cloud Platform (GCP) está melhorando lentamente seus recursos de borda e tomou dianteira pela terceira maior fatia do mercado. Com contínuo investimento para ser um provedor amplo de IaaS e PaaS e expandindo seus recursos, é um nome forte de mercado que vem se fortalecendo dentro do segmento.



Como as outras, tem posições geograficamente diversificadas e os clientes são variados, desde startups até grandes negócios. No último balanço fornecido pelo Synergy Research Group, o Google Cloud ocupou 10% de todo o montante do segmento em 2021.

7.5.1. Prós e contras do Google Cloud Platform (GCP)

O Google Cloud Platform (GCP), apesar de atrasado no jogo e com a menor participação de mercado dos provedores de nuvem pública, está mostrando um crescimento nos últimos anos. Possui vários recursos que o colocam à frente de seus concorrentes em determinadas áreas.

O GCP também está pegando onda, não apenas com os novos clientes que já fazem parte do ecossistema, mas também os primeiros usuários da nuvem que desejam expandir

seu cenário para o Google como parte de uma estratégia para várias nuvens. O Google também começou com serviços de PaaS, mas vem expandindo constantemente seu portfólio de produtos.

7.5.2. Quando escolher o GCP

Do ponto de vista da computação, o Google tem o menor número de tamanhos de VM (28 tipos de instância em 4 categorias). No entanto, ele tem uma característica que torna esses números um pouco irrelevantes.

O Google permite que os usuários criem seus próprios tamanhos personalizados (CPU, memória) para que os clientes possam combinar o tamanho das cargas de trabalho na nuvem com o tamanho no local. O faturamento também é feito com base na CPU e memória totais usadas, em vez de VMs individuais. Isso reduz o desperdício de capacidade não utilizada.

Outro recurso exclusivo é que o GCP permite que quase todos os tipos de instância conectem GPUs. Isso pode transformar qualquer instância padrão ou personalizada em uma VM pronta para ML. O Google também foi líder em cobrança por segundo, o que forçou outros CSPs a seguir o exemplo.

Comparado à norma usual do faturamento por hora, o faturamento por segundo reduz muito qualquer desperdício de capacidade. Isso resulta em uma economia de até 40% no geral. O Google também vinculou ou comprou ferramentas de migração para a nuvem de terceiros.

Essas ferramentas, como Velostrata e CloudPhysics, ajudam os clientes a avaliar, planejar e migrar ao vivo suas VMs para o GCP. Rede é o destaque do GCP. Eles têm uma rede global de baixa latência. Mesmo da perspectiva do cliente, uma rede VPC abrange todas as suas regiões.

Outros CSPs limitam as redes VPC a uma região. Isso facilita para os clientes do GCP criar aplicativos que atendem aos clientes globalmente, sem criar complexos mecanismos de design de infraestrutura entre regiões e replicação de dados.

Para Bancos NoSQL, o GCP tem um produto chamado BigTable. O BigTable é um banco de dados NoSQL gerenciado em escala de petabytes, usado pelo Google em seus próprios produtos, como o Gmail.

Do ponto de vista de cobrança, o Google oferece descontos automáticos, como descontos de uso sustentado, que reduzem o preço sob demanda se uma VM executar mais de um determinado número de horas em um mês.

Se você deseja o provedor de nuvem mais econômico, o GCP é uma ótima opção.

8. CONCEITOS BÁSICOS DE SEGURANÇA DE REDES - PARTE 01

Objetivo

O objetivo deste capítulo é apresentar a primeira parte dos conceitos básicos de segurança de redes.

Introdução

Segurança de rede é qualquer atividade projetada para proteger o acesso, o uso e a integridade da rede corporativa e dos dados. A segurança da rede combina várias camadas de defesa na borda e na rede. Cada camada de segurança de rede implementa políticas e controles. Usuários autorizados obtêm acesso a recursos de rede, mas agentes mal-intencionados são impedidos de realizar explorações e ameaças.

8.1. Firewall

Firewalls colocam uma barreira entre a rede interna confiável e as redes externas não confiáveis, como a Internet. Eles usam um conjunto de regras definidas para permitir ou bloquear o tráfego. Um firewall pode ser um hardware, software ou ambos.

8.2. Segurança de e-mails

Os gateways de e-mail são os principais vetores de ameaça de uma violação de segurança. Os invasores usam informações pessoais e táticas de engenharia social para criar campanhas de phishing sofisticadas, com o objetivo de enganar destinatários e enviá-los para sites de malware. Um aplicativo de segurança de e-mail bloqueia a entrada de ataques e controla mensagens de saída para impedir a perda de dados confidenciais.

8.3. Software antivírus e antimalware

"Malware", abreviação de "malicious software" (software mal-intencionado), inclui vírus, worms, Trojans, ransomware e spyware. Às vezes, o malware infecta uma rede, mas permanece inativo por dias ou até semanas. Os melhores programas antimalware não apenas analisam o malware na entrada, mas também sempre rastreiam os arquivos posteriormente para encontrar anomalias, remover malware e corrigir danos.

8.4. Segmentação de rede

A segmentação definida por software coloca o tráfego de rede em diferentes classificações e facilita a aplicação de políticas de segurança . De preferência, as classificações são baseadas na identidade do endpoint, não em meros endereços IP. Você pode atribuir direitos de acesso com base na função, local e muito mais, para que o nível certo de acesso seja concedido às pessoas certas, e os dispositivos suspeitos sejam contidos e corrigidos.

8.5. Controle de acesso

Nem todo usuário deve ter acesso à rede. Para impedir possíveis invasores, você precisa reconhecer cada usuário e cada dispositivo. Em seguida, você pode aplicar as políticas de segurança. Você pode bloquear dispositivos de endpoint não compatíveis ou conceder a eles apenas acesso limitado. Esse processo é um controle de acesso à rede (NAC).

8.6. Segurança de aplicações

Qualquer software usado para administrar os negócios precisa ser protegido, independentemente de sua equipe de TI criar ou comprar de terceiros. Infelizmente, qualquer aplicação pode conter falhas ou vulnerabilidades que os invasores usam para se infiltrar na rede. A segurança da aplicação abrange o hardware, software e processos que você usa para corrigir essas falhas.

8.7. Análise do comportamento

Para detectar um comportamento anormal da rede, você deve saber como é o comportamento normal. As ferramentas de análise comportamental distinguem automaticamente as atividades que se desviam da norma. A equipe de segurança pode identificar melhor os indicadores de comprometimento que apresentam um possível problema e remediar rapidamente as ameaças.

8.8. Prevenção contra perda de dados

As empresas devem garantir que a equipe não envie informações confidenciais para fora da rede. As tecnologias de prevenção contra perda de dados, ou DLP, podem impedir as pessoas de enviar, encaminhar ou, até mesmo, imprimir informações importantes de modo não seguro.

8.9. Segurança da web

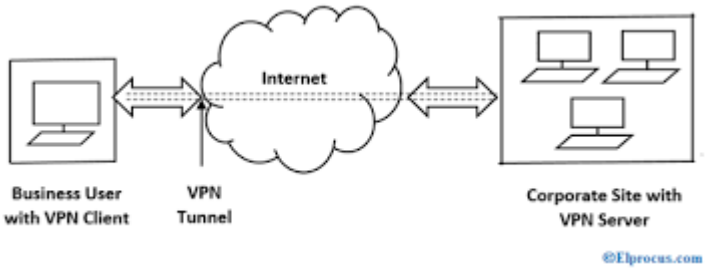
Uma solução de segurança da Web controlará o uso da Web da equipe, bloqueará ameaças baseadas na Web e negará acesso a sites mal-intencionados. Ela protegerá o gateway da Web no local ou na nuvem. "Segurança da Web" também se refere às etapas que você executa para proteger o próprio site.

8.10. VPN

A VPN é a sigla para Virtual Private Network, e se trata de uma conexão entre computadores feita de forma privada. Normalmente, é utilizada para oferecer maior privacidade e segurança de rede nas trocas de dados no dia a dia.

A VPN é bastante utilizada, por exemplo, para:

- Bloquear a navegação;
- Impedir o compartilhamento de dados internos da empresa em redes públicas;
- Realizar uma conexão criptografada;
- Esse tipo de conexão de computador é fundamental para quem deseja evitar que informações privadas possam ser obtidas por meio de cibercriminosos;



9. Conceitos básicos de segurança de redes - Parte 02

Objetivo

O objetivo deste capítulo é apresentar a segunda parte dos conceitos básicos de segurança de redes.

9.1. Tipos de autenticação

As senhas ainda são a autenticação mais comum na maioria dos sistemas. Eles normalmente não são muito seguros, entretanto, porque são fáceis de quebrar.

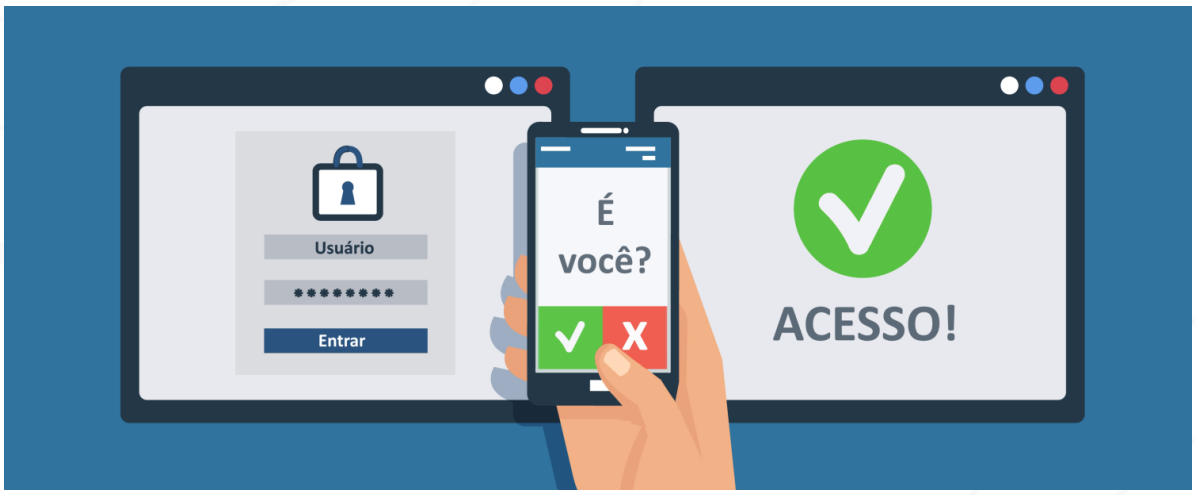
Se a senha for curta o suficiente, o criminoso não terá problemas para descobrir o que é. Os criminosos usam um ataque de adivinhação de senha que envolve força bruta – tentando todas as combinações possíveis. Ou o invasor pode usar um ataque de quebra de senha, que envolve o uso de um programa para recriar senhas com hash para o mesmo valor.

Existem três tipos ou fatores de autenticação em uso hoje. Eles estão:

Algo que você conhece: Uma sequência de caracteres, números ou uma combinação daqueles que estão armazenados em seu cérebro. Hoje eles devem ser armazenados em um gerenciador de senhas.

Algo que você tem: Um dispositivo ou software em um dispositivo que você precisa para autenticar. Isso inclui dispositivos como um token RSA ou o autenticador do Google em um smartphone.

Algo que você é: Um aspecto de sua pessoa. Isso é biométrico, fisiológico, como uma impressão digital, ou comportamental, como uma impressão vocal.



A melhor opção é a autenticação de dois fatores (2FA), às vezes chamada de autenticação multifator (MFA). É altamente recomendável para suas contas pessoais, como Amazon ou Facebook.

Aplicações como o autenticador do Google são de uso gratuito e uma escolha muito melhor do que receber uma mensagem de texto ou de serviço de mensagens curtas (SMS) em seu telefone. O Instituto Nacional de Padrões e Tecnologia (NIST) não recomenda SMS.

9.2. Criptografia

A criptografia é essencial para manter os dados confidenciais e as comunicações longe de olhares indiscretos. A criptografia protege arquivos no disco rígido do seu computador, uma sessão bancária, dados armazenados na nuvem, e-mails confidenciais e uma longa lista de outras aplicações. A criptografia também fornece verificação da integridade dos dados e autenticação da fonte dos dados.

A criptografia se divide em dois tipos básicos de criptografia: simétrica e assimétrica.

A criptografia simétrica tem uma única chave que criptografa e descriptografa. Como resultado, ela deve ser compartilhada com outra pessoa para completar a comunicação criptografada. Os algoritmos comuns incluem o Advanced Encryption Standard (AES), Blowfish, Triple-DES (Data Encryption Standard), e muitos mais.

A criptografia assimétrica tem duas chaves distintas, uma pública e outra privada, que funcionam como um conjunto correspondente. O conjunto de chaves pertence a um

usuário ou um serviço: por exemplo, um servidor web Uma chave é para criptografia e a outra é para descriptografia.

Se a chave pública criptografar os dados, ela os manterá confidenciais. Isso ocorre porque o proprietário da chave privada é o único que pode descriptografá-la.

Se a chave privada criptografar os dados, isso prova a autenticidade da fonte. Quando os dados são descriptografados com sucesso com a chave pública, significa que apenas a chave privada poderia criptografá-los. A chave pública é verdadeiramente pública, acessível a qualquer pessoa.

Um terceiro tópico é hashing. Mesmo que não seja criptografia, ela precisa ser incluída neste ponto nas discussões de segurança. O hash executa um algoritmo em uma mensagem que calcula uma resposta resultante, chamada de hash, que é baseada nos bits dessa mensagem. Os bits podem ser dados, voz ou vídeo. O hash não altera o valor dos dados de forma alguma. Em contraste, a criptografia altera os dados para um estado ilegível.

O hash prova que os bits da mensagem não mudaram. Ele garante que os dados tenham integridade e que estejam em seu formato original. Apenas o hash protege os dados de alterações acidentais.

Se o hash for criptografado com uma chave privada assimétrica, isso prova que um criminoso não adulterou os dados de forma mal-intencionada. Mudanças maliciosas não podem ocorrer a menos que a chave privada seja comprometida.

Se a chave não foi comprometida, você sabe que a pessoa que possui a chave privada deve ser a pessoa que calculou o hash. Essa chave pode ser uma chave simétrica, que às vezes é chamada de chave privada ou a chave privada assimétrica.

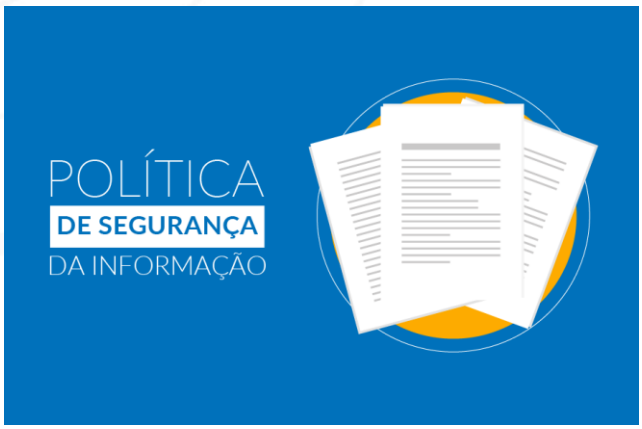
9.3. O que levar em consideração para segurança da informação das empresas

Abaixo reunimos algumas das melhores práticas que devem ser implementadas para garantir a segurança da informação e consequentemente da rede da empresa.

9.3.1. Elabore uma Política de Segurança da Informação (PSI)

Vale lembrar que toda melhor prática começa com a gestão da organização. Nessa perspectiva, é essencial que seja criada uma Política de Segurança da Informação (PSI). Esse documento deve conter todas as diretrizes a serem seguidas pela totalidade de profissionais envolvidos com as atividades da empresa, o que inclui funcionários, fornecedores, sócios e acionistas.

A PSI é essencial, uma vez que abrange os procedimentos que os profissionais precisam adotar no cotidiano da empresa. Ela contempla as tecnologias que devem ser utilizadas, os processos a serem conduzidos, as sanções aplicadas a quem desobedecer às diretrizes, assim como quais dados são sigilosos e devem ser mantidos sob total segurança.



A política funciona como uma esfera reguladora da manipulação dos dados empresariais. Dessa maneira, algumas ações são necessárias. Identifique as melhores práticas a serem tomadas em cada setor, quem são as pessoas responsáveis e os níveis de acesso de cada usuário de sistemas dentro da empresa. Também atente a outras informações que julgue necessárias para orientar o seu time a agir corretamente no tratamento das informações, para dar a elas a proteção adequada.

A elaboração de uma PSI, com o seu devido cumprimento, funciona como um pré-requisito para que ocorra a proteção dos dados de uma empresa. Isso porque de nada adianta a implementação de ferramentas tecnológicas, como as que mostraremos a seguir, se não houver o cultivo cotidiano de uma cultura empresarial em prol da segurança da informação.

Uma PSI, na qual estejam estabelecidas as diretrizes de proteção de dados, em conjunto ao uso de instrumentos tecnológicos adequados, ajuda a garantir a efetivação de práticas eficientes de segurança da informação. Levando em conta a importância da conjugação desses dois elementos, na seção seguinte, indicaremos algumas tecnologias cuja implementação é fundamental para cuidar dos segredos informacionais de uma empresa.

9.3.2. Implemente as tecnologias necessárias

Com o atual desenvolvimento tecnológico, não existe empresa que trabalhe 100% manual na hora de manipular dados. Tanto aquelas que foram criadas recentemente quanto as mais conservadoras utilizam algum tipo de tecnologia para coletar, armazenar, processar e analisar informações.

Para manter o sigilo desses dados, você precisa de tecnologias auxiliares que promovam a cibersegurança. Existem diversos recursos tecnológicos que atuam, em conjunto ou de modo isolado, na proteção dos dados de uma empresa:

- Conexões seguras;
- Criptografia de dados;
- Assinatura eletrônica;
- Armazenamento em nuvem;
- Antivírus;
- Antispywares.

Cada empresa deve analisar o nível de segurança necessário e aplicar as tecnologias mais adequadas ao seu perfil e condições. Estas que listamos acima são bastante acessíveis e conferem uma excelente proteção aos dados do seu negócio.

9.3.3. Proteja suas redes de Wi-Fi

Quando falamos em conexão, é bom lembrar que operar com uma rede sem fio de internet é muito importante para o ganho de eficiência nos mais diversos tipos de atividades desenvolvidas no interior de uma empresa. E não poderia ser diferente. Isso ocorre em razão da facilidade, rapidez e comodidade de acesso, navegação e troca de informação próprios dos dispositivos de conexão Wi-Fi.

No entanto, se não for manipulada de modo adequado, uma rede sem fios pode trazer riscos para a segurança dos negócios. Sem a devida proteção, usuários não autorizados facilmente obtêm acesso à rede Wi-Fi, podendo invadir o banco de dados da

empresa, roubar as informações e até mesmo praticar ações que danificam, destroem ou copiem periodicamente as informações registradas.

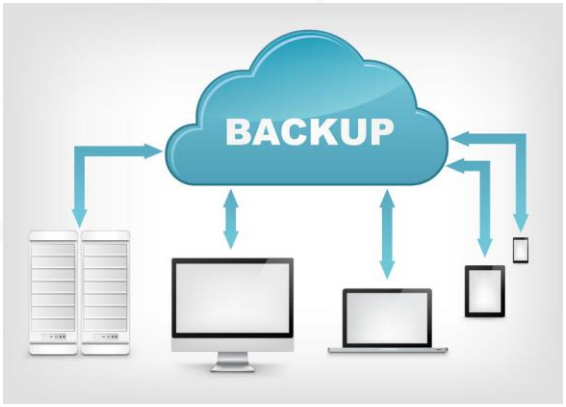
Por isso, é fundamental que sejam implementados mecanismos que protejam a rede sem fio de um negócio. Uma solução viável, tendo em vista a sua simplicidade e agilidade, é a criação de senha de acesso, a qual deve ser forte, isto é, ser composta por letras, números e caracteres especiais, que, em conjunto, dificultam a descoberta da chave por usuários indesejados.

Outra ação eficiente é efetuar o cadastro dos equipamentos autorizados a acessarem a rede Wi-Fi da corporação, o que bloqueia o acesso de pessoas não autorizadas. Essa medida é ainda vantajosa porque ajuda a ter um maior controle no que se refere a quem exatamente acessa o banco de dados da empresa ou mesmo faz alguma alteração nele.

Ambas as alternativas permitem a navegação de usuários temporários, como colaboradores eventuais, clientes e fornecedores. Isso pode ser feito por meio da criação de logins para visitantes e do registro de equipamentos por tempo determinado, com a predeterminação do período de acesso do dispositivo.

9.3.4. Faça backups

Bastante comum no universo tecnológico, backup é uma expressão em língua inglesa que significa cópia de segurança. Trata-se de um conjunto de procedimentos relativos a outra vertente crucial da segurança da informação: proteção contra a perda de dados, ação que é tão necessária quanto protegê-los do acesso feito por usuários não autorizados.



Com a realização de backups periódicos, a empresa garante que dispõe de todas as informações de que pode precisar, evitando as consequências trazidas por imprevistos. E isso é fundamental, uma vez que, embora os recursos tecnológicos sejam cada vez mais sofisticados e desenvolvidos, ainda é comum haver perdas de dados, por falha computacional ou erro humano.

Além disso, o backup, principalmente os que são feitos em nuvem, protege as informações de potenciais roubos aos equipamentos em que estão armazenadas. Como não podemos prever o futuro ou apenas contar com a sorte, essa é uma ação essencial para promover a segurança das informações empresariais.

9.3.5. Armazene seus documentos na nuvem

Como mostramos no tópico anterior, guardar adequadamente as informações relativas a um negócio é muito importante para o seu funcionamento. Por isso, o local de armazenamento desses dados deve ser o mais seguro possível, tanto no que se refere ao acesso de usuários quanto no que diz respeito ao backup feito para manter cópias extras das informações.

Nessa perspectiva, o armazenamento em nuvem figura como uma excelente solução. Isso porque, ao consistir em uma tecnologia que permite o armazenamento de dados de forma remota, por meio da internet e sem a necessidade de um local físico para a guarda dos arquivos, o sistema em nuvem confere, ao mesmo tempo, praticidade e segurança no processo de arquivamento e acesso informacional.

Esse tipo de serviço de armazenamento permite que a empresa proteja suas informações de modo a compartilhá-las somente com os usuários autorizados. Tal compartilhamento seguro é possível uma vez que uma nuvem privada, modelo comumente usado no mundo comercial, tem sua proteção feita por meio do firewall da empresa, o que confere maior controle dos dados.

9.3.6. . Firme um contrato de confidencialidade

Cada pessoa que se relaciona direta ou indiretamente com dados sigilosos deve assinar um documento destes comprometendo-se a manter a confidencialidade dos dados trocados com a sua organização.

Empresas de tecnologia já têm bastante familiaridade com contratos de confidencialidade, já que desenvolvem inovações que estão na dianteira do mercado. Já pensou se o protótipo do novo iPhone vaza e os concorrentes lançam produtos semelhantes antes da Apple? Seria um desastre comercial.

O contrato de confidencialidade não pode impedir que alguém roube as informações da sua empresa e transmita a terceiros, no entanto, é a garantia de que você poderá ser indenizado por isso. Portanto, trata-se de um documento com validade jurídica, que deve ser assinado e guardado com todo o rigor.

9.3.7. Gerencie os riscos

A perda de dados sigilosos pode se dar de muitas maneiras: um vírus que rouba a informação de um computador, um hacker que invade o sistema da empresa, uma inundação que coloca a perder seu servidor e um pendrive perdido. Estes são só alguns exemplos de situações que podem ocorrer.

Antes que elas aconteçam, o ideal é que você mapeie todos esses riscos, por mais absurdos que possam ser, e crie um plano de ação para reduzir ao máximo as possibilidades de que eles venham a se tornar realidade. Por exemplo: em vez de manter seus funcionários levando informações sigilosas em pendrives, opte pelo armazenamento na nuvem. Essa solução traz mobilidade sem afetar a segurança da informação.

Evite também enviar contratos impressos para assinatura, o que abre brechas para fraudes e vazamento de informações. Prefira a assinatura eletrônica e tramite seus documentos completamente pela via digital. Quanto menos pessoas tiverem contato com os dados da empresa, menor a chance de ver seu segredo comercial divulgado por aí.

9.3.8. Treine sua equipe

Quando as políticas de segurança da informação são impostas pela diretoria sem a devida explicação, a reação natural das pessoas é rechaçar as orientações. Isso porque elas não sabem quais motivos levaram à implementação de tais práticas. O que você deve

fazer é conscientizar seu time, seus fornecedores, diretores e demais parceiros de negócios a respeito da importância de se manter esses dados sob proteção.

Já pensou se o protótipo do carro de corrida da McLaren cai em mãos erradas? É todo um investimento que se perde, uma tecnologia empregada que passa a ser de domínio público e que prejudica a performance da empresa por um longo tempo. Além de reforçar a comunicação, certifique-se de que todos sabem operar os sistemas que a empresa utiliza com a aplicação de login e senha de acesso.

9.3.9. Tenha um plano de contingência

O plano de contingência é executado quando a companhia sofre com desastres e precisa prosseguir com as atividades operacionais da melhor forma possível. Logo, essa estratégia preventiva precisa considerar um conjunto de situações possíveis e quais as principais reações para assegurar a disponibilidade do sistema e dos dados, a fim de garantir a continuidade do negócio.

É necessário que todos os setores tenham prévio sobre como precisam agir caso uma ocorrência desagradável (invasão, vazamento etc.) surja de forma repentina — para

evitar que nenhuma das informações críticas se percam e a companhia fique inativa por muito tempo.