INTRO 4.0

COMUNICAÇÃO EM REDE

EuroProfis

edit value
apoio à gestão

@nced
ASOCIACIÓN NACIONAL DE CENTROS DE e-LEARNING Y DISTANCIA

bit schulungscenter
member of bit group

Cofinanciado pelo Programa Erasmus+ da União Europeia

Parceiro associado:
udima
UNIVERSIDAD A DISTANCIA DE MADRID

INTRODUÇÃO À REVOLUÇÃO INDUSTRIAL 4.0

Estes materiais didáticos foram desenvolvidos no âmbito do projeto "Indústria 4.0 – INTRO 4.0" financiado pela Comissão Europeia e que tem como objetivo obter uma visão geral do que está a ser feito na indústria europeia em termos da Indústria 4.0.

O conteúdo destes materiais didáticos oferece informações relevantes e úteis relativamente à Indústria 4.0 que tem como grupos-alvo: adultos, professores (ensino profissional e ensino superior), formadores, *coaches*, empregadores, colaboradores, público-geral e fornecedores de soluções inovadoras.

A informação que consta neste relatório está relacionada com os relatórios "Estado atual da Indústria 4.0" e "Relatório síntese das entrevistas/questionários realizados junto de especialistas e investigação específica da indústria produtiva", ambos desenvolvimentos pelos parceiros do projeto.

ÍNDICE

ESTE CONTEÚDO PODE SER MAIS INTERESSANTE PARA AS EMPRESAS

ESTE CONTEÚDO PODE SER MAIS INTERESSANTE PARA O PÚBLICO GERAL

OBJETIVOS DE APRENDIZAGEM

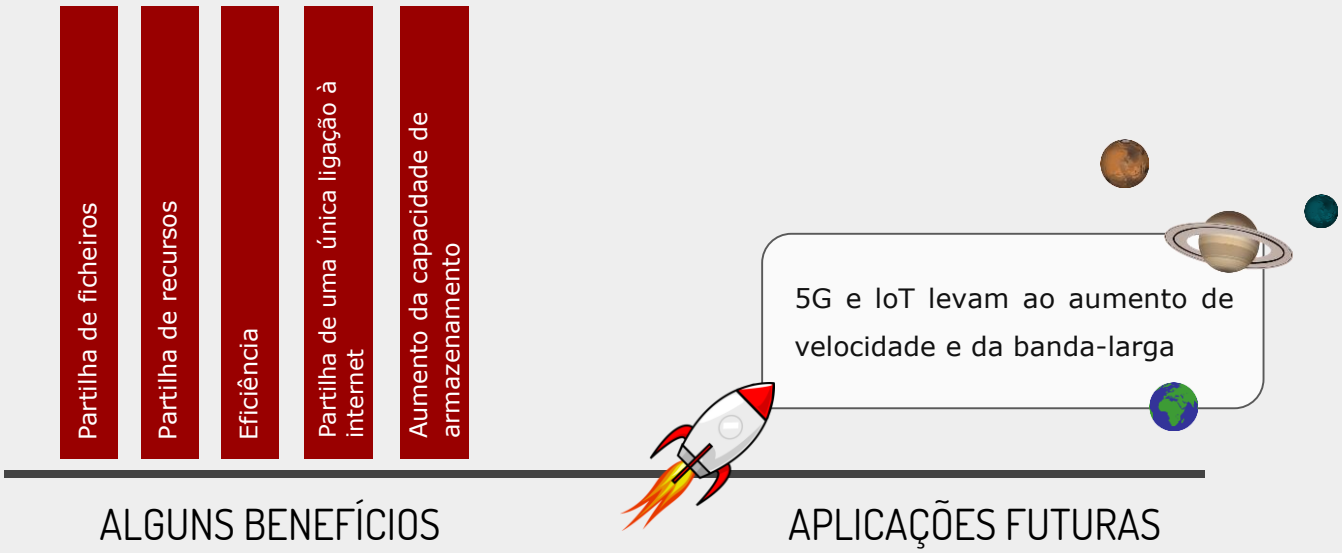
- Compreender os fundamentos da comunicação em rede
- Identificar os diferentes tipos de rede
- Conhecer a importância da internet das coisas
- Estimar os benefícios que a comunicação em rede pode ter para as empresas
- Reconhecer as aplicações futuras

INTRODUÇÃO

A **comunicação de rede** corresponde a um conjunto de dispositivos que inclui *hardware* e *software* que estão conectados entre si.

Objetivos de aprendizagem

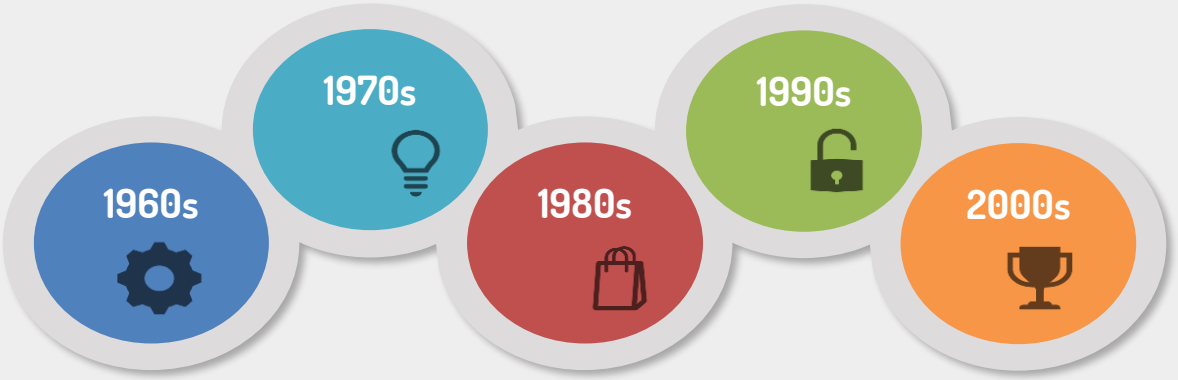
- Compreender os fundamentos da comunicação em rede
- Identificar os diferentes tipos de rede
- Conhecer a importância da internet das coisas (IoT)
- Estimar os benefícios que a comunicação em rede pode ter para empresas
- Reconhecer as aplicações futuras



PARA QUE SERVE?

A rede de comunicações está na base da nossa sociedade. Uma rede de comunicações é um conjunto de dispositivos que compreende *hardware* e *software* conectados entre si seja, ou não, na mesma localização geográfica, para facilitar a comunicação e a partilha de informações. Temos então: máquinas de ultrassom, telefones móveis, comunicações via internet, transações bancárias, aprendizagem *online*, controlo de fronteiras, redes de transporte, imagens de satélite,… e a lista continua e tudo isto é possível através de redes de comunicação. Na sociedade atual não é possível prescindir delas.

A rede de comunicação moderna baseia-se em servidores, clientes, meios de transmissão, dados, sistemas operativos, *switches*, rotadores, cabos, impressoras e vários dispositivos periféricos que estendem a comunicação entre dispositivos da rede local para redes cobertas globalmente.



Em 1962, o cientista da computação do MIT J.C.R. Licklider surge com a ideia de uma rede global de computadores

Em 1973, Robert Kahn e Vinton Cerf colaboraram para desenvolver um protocolo para interligar várias redes. Mais tarde este protocolo torna-se o protocolo de controlo de tansmissão/ protocolo de internet (TCP/IP)

Em 1981, a empresa 3Com da Metcalfe anuncia produtos Ethernet para estações de trabalho de computadores e computadores pessoais e isto permite o estabelecimento de redes locais (LANs)

O CERN desenvolve o *hypertext markup language* (HTML) e o *uniform resource locator* (URL) dando origem à primeira encarnação da world wide web

A ascensão e a proliferação da Wi-Fi bem como de dispositivos móveis como *smartphones*. Em 2005, surge o primeiro vídeo com gatos na Internet

PARA QUE SERVE?

TIPOS E ESTRUTURAS DE REDE

As redes podem ter ou não fios sendo que a maioria das redes é uma mistura de ambas.

Rede com vs sem fios

As primeiras redes (anteriores a 2008) eram predominantemente com fios. Contudo, atualmente a maioria das redes utiliza uma mistura de rede com e sem fios.

As redes com fios usam a Ethernet como protocolo de *link* de dados. Contudo, é improvável que isto mude com a IoT pois os dispositivos de IoT serão predominantemente sem fios.

As redes com fios possuem as seguintes vantagens/desvantagens:

Vantagens

- As portas Ethernet são encontradas em quase todos os portáteis, computadores e *netbooks* mesmo naqueles com 8 anos de idade
- São mais rápidas que redes *wireless* (sem fios). As taxas de dados aumentaram periodicamente dos 10 megabits por segundo para 1 gigabyte por segundo e a maioria das redes domésticas usa 10-100mbps
- Mais seguras que o *wireless* (sem fios)

Ethernet é uma família de tecnologias de rede de computador frequentemente usada em LANs, redes de áreas metropolitana (MAN) e redes de longa distância (WAN)

PARA QUE SERVE?

Desvantagens

- Precisa de usar o cabo que podem ser inestésticos, difíceis de instalar e caros
- Não podem ser usadas facilmente entre edifícios (devido a questões relacionadas com planeamento, etc.)
- Uma nova tecnologia que usa cabos de redes superam muitas destas desvantagens. A *Powerline networking* é comum em casas e pequenos escritórios
- Não são suportadas por telemóveis e *tablets*

Rede sem fios - vantagens e desvantagens

As redes sem fios usam o protocolo de *link* de dados por Wi-fi embora existam outras opções sem fios que estão a ser desenvolvidas na IoT. Consulte a informação disponível em: tecnologias de rede sem fios para a IoT.

As redes sem fios (*wireless*) têm as seguintes vantagens/desvantagens:

Vantagens

- Geralmente são mais fáceis de configurar
- Podem ser usadas em redes domésticas e públicas
- Não necessitam de cabos
- Podem ser usadas em telemóveis e *tablets*

Desvantagens

- Geralmente são mais lentas do que as redes com fio
- Limitada
- Aberta a "escutas"
- Noção é tão segura, depende da configuração

PARA QUE SERVE?

Topologia de redes e *design*

Existem várias formas de conectar os pontos de acesso de rede entre si. Este aspeto, normalmente, não é considerado em redes pequenas mas, à medida que as redes se vão tornando maiores, este aspeto ganha maior relevância.

As tecnologias de conexão mais comuns como o Wi-Fi ou o Bluetooth estão desenhadas para funcionar usando uma topologia de rede específica. Neste sentido, quando se projetam redes e se escolhem protocolos de ligação é importante compreender quais são estas topologias.

As topologias mais comuns são: Bus, Ring, Mesh, Star, Hybrid.

As antigas redes *Ethernet* usam uma estrutura *bus* enquanto as redes de *Ethernet* modernas e as redes Wi-Fi usam a estrutura *star bus (*híbridas*)*.

Topologias de rede – física vs lógica

O modo como os pontos de acesso de uma rede comunicam entre si pode ser muito diferente consoante o modo como estes pontos de acesso estão fisicamente interligados.
A maioria das redes domésticas e das pequenas empresas usa uma topologia de *bus* física. As topologias lógicas comuns são *peer to peer* e *client server*. A *web* (www) é uma rede de servidores cliente ao nível lógico. Numa rede *peer to peer,* todos os pontos de acesso de uma rede são iguais e qualquer ponto de rede pode comunicar com outro e, além disso, nenhum ponto de rede tem uma função especial. Este foi o modelo original de rede do *Windows* (*Windows* para grupos de trabalho).

PARA QUE SERVE?

Modelo de rede *peer to peer*

Vantagens

- Fácil de configurar
- Não depende de um único ponto de rede
- Mais resiliente
- Melhor distribuição do tráfego de rede
- Não exige uma gestão central
- Requere *hardware* menos dispendioso

Desvantagens

- Menos segura e mais difícil de proteger
- Mais difícil de gerir
- Mais difícil para realizar cópias de seguranças
- Mais difícil de localizar informações

Este foi o modelo originalmente usado para as antigas redes Windows (*Windows* para grupos de trabalho).

Um exemplo moderno de rede *peer to peer* é a BitTorrent.

Embora esse modelo de rede não seja muito popular devido à IoT este modelo de rede poderá tornar-se mais popular.

PARA QUE SERVE?

Client server

Numa rede *client server* o servidor tem uma função especial por exemplo, funcionar como servidor de arquivo, controlador de domínio, servidor de internet etc. Numa rede *client server* um cliente conecta-se a um servidor para usar os serviços apropriados. Este é o modelo de rede usado na *web* e na Internet e em grandes redes *windows*.

Vantagens

- Fácil de encontrar recursos pois estão disponíveis no servidor
- Fácil de proteger
- Fácil de gerir
- Fácil de realizar cópias de segurança

Desvantagens

- Os servidores são o único ponto de falha
- Necessidade de *hardware* dispendioso
- Concentra o tráfego de rede

Um exemplo moderno de rede *client server* é a internet. O facebook, o twitter, a pesquisa no Google e outros serviços de internet utilizam este modelo de rede.

PARA QUE SERVE?

Tamanho da rede

O tamanho das redes varia consideravelmente e, frequentemente, são usadas as seguintes terminologias:

- ***Personal Area Network* (PAN):** conecta dispositivos locais como, por exemplo, um computador e uma impressora
- **LAN:** conecta dispositivos num ou vários escritórios
- ***Metropolitan Area Network* (MAN):** conecta dispositivos entre vários edifícios (como por exemplo um *campus*)
- ***Wide Area Network* (WAN):** conecta dispositivos num ou em vários países

Níveis, camadas e protocolos de rede

Um protocolo define um conjunto de regras que determinam como os computadores interagem entre si.

Ethernet e Wi-Fi são protocolos de ligação que são responsáveis pelo enquadramento dos dados nos media (com ou sem fios).

Ethernet e Wi-Fi usam um endereço físico conhecido como endereço MAC de 48 bits.

Os endereços EUI 64 são endereços MAC com 64 bits que substituirão endereços MAC em IPV6, 6LoWPAN, ZigBeeand e outros novos protocolos de rede.

É possível dividir a rede em níveis ou camadas distintas sendo que cada nível ou camada é responsável por uma função em particular.

O Open Systems Interconnection (OSI) usa um modelo de 7 camadas e as redes TCP/IP usam um modelo de 4 camadas.

PARA QUE SERVE?

Uma vez que as redes TCP/IP (TPC: *Transmission Control Protocol* e IP: *Internet Protocol*) são as mais comuns o modelo TCP/IP é o mais importante para compreender. Os níveis são os seguintes:

- Nível de conexão de dados por exemplo, Ethernet, Wi-Fi
- Rede por exemplo, IPv4 Address aulas e sub-redes e IPv6 explicado para principiantes.
- Nível de transporte por exemplo, TCP, UDP: ver TCP vs UDP
- Nível de aplicação por exemplo, HTTP: ver HTTP para principiantes

Endereço de rede *sing*

O que é um endereço de IP?

Todos os dispositivos conectado a uma rede e à Internet possuem um endereço IP.

> Um endereço de protocolo da internet (endereço IP) é um rótulo numérico atribuído a cada dispositivo (por exemplo, a um computador e/ou impressora) que participa numa rede de computadores que usa o protocolo de internet para comunicar.

Existem duas versões de endereços de IP: o IPv4 e o IPv6, respetivamente.

O IPv4 é usado desde o início da internet e é implementado na internet e em redes domésticas e empresariais.

O IPv4 utiliza 32 bits para o endereço de IP muito embora, devido ao rápido crescimento da internet, todos os endereços IPv4 tenham sido alocados a partir de 2013.

PARA QUE SERVE?

Técnicas como a *Network Address Translation* (NAT) aumentaram a vida útil do IPv4, permitindo assim o uso de endereços IP privados dentro das redes.

Todavia, o IPv4 será eventualmente substituído pelo IPv6, que utiliza 128 bits para o endereço e, consequentemente, pode alojar muitos mais *hosts* (computadores/dispositivos).

A implantação do IPv6 na internet está a acontecer lentamente e, por esse motivo, o endereço de IP IPv4 permanecerá ativo por muitos anos, especialmente nas redes domésticas e em pequenos escritórios.

À medida que o IPv6 avançar, tornar-se-á necessário operar com dois endereços até que a migração seja concluída e o IPv4 seja descontinuado.

Os endereços IP são endereços lógicos e são atribuídos por um administrador de rede ou podem ser atribuídos automaticamente usando um Dynamic Host Configuration Protocol (DHCP).

O importante é observar que o endereço IP de um dispositivo não é fixo.

Endereços de IP privados e públicos

Tanto o IPv4 como o IPv6 possuem gamas de endereços públicos e privados.

Os endereços privados são usados em redes domésticas/comerciais e não podem ser rastreados a partir da internet.

Para o endereço de IP IP4, os endereços privados começam com 10.x.x.x ou 192.168.x.x ou 172.16.x.x.

Por sua vez, os endereços de IP públicos podem ser acedidos na internet a partir de qualquer lugar e podem ser rastreados.

PARA QUE SERVE?

Atribuição de endereços de IP

A maioria das redes modernas utiliza a atribuição automática de endereços de IP através de um DHCP, sendo que a atribuição manual de endereços de IP é feita apenas em casos especiais.

No caso de redes domésticas, o *router* ou *hub* da internet fornece, regra geral, serviços DHCP para a rede e, no caso de redes maiores, é normalmente usado um servidor DHCP.

A maioria das máquinas *Windows* irá atribuir automaticamente o seu próprio endereço de IP caso não encontre um servidor DHCP. Esta situação pode causar alguns problemas. Para consultar os tipos de problemas que podem ser encontrados consulte a informação: resolução de problemas em ligações pela internet.

Endereços de IP e nome dos domínios

Os computadores utilizam números (neste caso endereços de IP) mas as pessoas usam nomes pois são muito mais fáceis de lembrar.

Quando se digita um nome de um domínio num navegador de internet esse nome é traduzido num endereço IP por um servidor DNS que, regra geral, está localizado na internet.

PARA QUE SERVE?

TOP 5 DAS COMPETÊNCIAS DE COMUNICAÇÃO EM REDE PARA COLABORADORES

Figura 1. Top 5 das competências de comunicação em rede mais importantes para trabalhadores. Fonte: Elaboração própria

Os profissionais de redes de computadores gerem o funcionamento diário de redes de computadores. A exigência de trabalhadores qualificados nas áreas das TIC deve crescer à medida que as empresas investem em tecnologia recente e rápida.

Adicionalmente, um profissional de rede de computadores bem-sucedido deverá possuir várias competências de forma a dar suporte aos sistemas de computadores de uma organização, incluindo:

PARA QUE SERVE?

Competências analíticas

Aprender a avaliar o desempenho da rede e do sistema e detectar e monitorizar as alterações nos sistemas de computadores.

Competências informáticas

Trabalhar com uma variedade de tecnologias, incluindo redes de área local, redes de longa distância, segmentos de rede, intranets, *hardware* e *software*. Os administradores qualificados em computação na nuvem e em tecnologia móvel são bastante procurados.

Competências de comunicação

Fornecer suporte de TI e comunicar problemas e soluções a administradores e colaboradores com menos experiência em tecnologia.

Competências de resolução de problemas

Aprender a resolver rapidamente os problemas que surgem em redes de computadores.

Competências de *multi-tasking*

Capacidade de gerir vários problemas e projetos ao mesmo tempo numa organização.

PARA QUE SERVE?

Os investigadores estimam que dentro dos próximos dois anos existam 20,4 bilhões de dispositivos da IoT conectados sendo que este aumento no número de dispositivos de IoT também se traduzirá num aumento significativo do número de profissionais ligados à IoT. Desta forma, podemos afirmar que uma profissão ligada à IoT poderá ser bem remunerada dada a sua crescente exigência. Porém, os candidatos precisarão de possuir um conjunto de competências específicas para garantir uma carreira promissora nesta área.

Competências para uma carreira em IoT

1. *Business intelligence*
2. *Segurança dos dados*
3. *Design* de aplicações
4. Aplicações móveis
5. *Hardware* da IoT
6. Redes
7. Sensores
8. *Embedded chips*
9. Computação na nuvem
10. Solução de problemas na IoT

BOAS PRÁTICAS

Tecnologia para vestir

Magoo project

O Magoo é um dispositivo especificamente desenhado para deficientes visuais que é acessível, fácil de usar e elegante. Este dispositivo fornece duas funções básicas: deteção de obstáculos e assistência à navegação que funciona através de *feedback* tátil.

Na deteção de obstáculos, o utilizador utiliza um colar que contém um sensor ultrassónico que vibra (através de *feedback* tátil) no pescoço se o utilizador estiver a 2 metros de distância de uma barreira que se encontre à sua frente.

A segunda peça é uma luva de braço que apresenta uma componente Wi-Fi, um *design* bonito e uma componente tátil na sua parte superior. O utilizador insere o seu destino através de um comando de voz e o circuito integrado na luva viaja com o GPS para encontrar a rota ideal para chegar ao destino final (a cada 0,1 milhas) encontrando um vetor de direção.

Ao utilizar esta luva o utilizador ao mexer o braço consegue rastrear a direção correta do seu destino. Quando o braço do utilizador se alinha com o "vetor de direção correta" (de acordo com as indicações do GPS), o utilizador recebe um *feedback* tátil e isto ajuda a pessoa invisual a chegar ao seu destino final sem que se perca durante o seu caminho.

BOAS PRÁTICAS

Boas práticas da Universidade de Mary Washington (Google Glass Explorer)

A Universidade de Mary Washington fazia parte do programa Google Glass Explorer e este programa está agora a caminhar para a sua próxima fase de desenvolvimento.
O Google Glass Explorer é uma tecnologia portátil semelhante a um *smartphone.* Este dispositivo encaixa-se numa estrutura de vidro ocular e possui uma câmara montada na cabeça e uma tela colocada no olho direito. Para comunicar com este mini portátil é possível usar o comando de voz ou o toque e, similarmente a um *smartphone*, é possível fazer o *download* de aplicações que oferecem novas funcionalidades ao dispositivo.

O Google Glass Explorer num ambiente educacional:

Estudantes:
O Google Glass Explorer permite aos estudantes o registo de interações, processos, *role play*, a realização de atividades para falar em público, trabalhar em grupo, criar estratégias de resolução de problemas, tutoriais e trabalhos de campo, movimentos da cabeça e do corpo na prática desportiva, tomar notas e realizar pesquisas simples no Google.
Com a realidade aumentada através de QR Codes é possível visualizar conteúdos (vídeos, texto, imagens) e realizar traduções em tempo real. Este programa está acessível para pessoas com deficiências visuais, auditivas e físicas.

BOAS PRÁTICAS

Professores:

O Google Glass Explorer permite aos professores documentar em tempo real a aprendizagem do aluno durante palestras, demonstrações, atividades de experiências práticas e trabalhos de campo. Além disso, o Google Glass Explorer permite gravar aulas na perspetiva do professor e combinar as mesmas com a perspetiva do aluno para uma reflexão. Adicionalmente, é possível realizar tutoriais para ajudar a esclarecer perceções erradas ou a responder a perguntas colocadas por alunos; tomar notas; receber as perguntas dos alunos durante as palestras; procurar alunos; ver anotações dos diapositivos durante a apresentação; utilizar a tecnologia durante avaliações internas; conectar-se através de *hangouts* do Google; criar vídeos de conteúdo; exibir informações ao aluno para adaptar as aulas às suas necessidades; exibir vários tipos de informações; e, enviar e receber mensagens.

Usos gerais:

Criar guias para a realização de vídeos (na primeira pessoa e em tempo real); criar documentários para melhorar o *storytelling*; capturar a vida quotidiana; conectar-se com outras pessoas através de *hangouts* do Google; transferir conteúdo do Glass para o Google+ do computador facilitando o acesso; realizar pesquisas personalizadas; projetar e criar aplicações; e, criar legendas ocultas.

A Internet das Coisas

Universidade de Wisconsin–Madison

No laboratório de IoT desta universidade, os investigadores, em colaboração com trabalhadores na área industrial, estão a desenvolver vários dispositivos, como um centro de mensagens digitais em casa, uma pulseira de monitorização do estado de saúde ou dispositivos conectados a bicicletas para alertar sobre a aproximação entre veículos. Nesta universidade, os estudantes com grandes ideias podem juntar-se ao projeto e aprimorar a tecnologia e a sua habilidade para negócios.

BOAS PRÁTICAS

IoT Lab

O IoT Lab é uma plataforma de investigação que explora o potencial do *crowdsourcing* e da IoT em estudos multidisciplinares permitindo mais interações com os utilizadores finais. Esta plataforma coloca as pessoas no centro do processo de investigação e inovação e dá-lhes o poder de mudar o mundo e a forma como o entendemos.

IoT na educação médica

Este artigo descreve a plataforma de Aprendizagem *IoTFlip* ou *IoT Flipped* que usa os dispositivos da IoT, os dados da IoT e o *Case Based Learning* para criar uma plataforma baseada em aprendizagem invertida relacionada com a educação médica.

Algumas das principais empresas:

XILINX®

Google

INGENU simply genius

ARM

CISCO

IBM

BOSCH

R-Style Lab

BENEFÍCIOS PARA EMPRESAS

Configurar uma rede de computadores é uma maneira rápida e confiável de partilhar informações e recursos dentro de uma empresa de forma a aproveitar ao máximo os sistemas e equipamentos de Tecnologias de Informação (TI) disponíveis.

Os principais benefícios das redes são:

Partilha de ficheiros
Pode partilhar dados entre diferentes utilizadores ou aceder aos dados de forma remota se os mantiver noutros dispositivos conectados à rede.

Partilha de recursos
O uso de dispositivos periféricos conectados à rede como impressoras, *scanners* e fotocopiadoras, a partilha de *software* entre vários utilizadores e economizar dinheiro.

Partilha uma única conexão à internet
É económico e pode proteger os sistemas se a rede for segura.

Aumentar a capacidade de armazenamento
É possível aceder a arquivos e multimédia, como imagens e músicas, que estão armazenados remotamente noutras máquinas ou dispositivos de armazenamento ligados à rede.

Os computadores em rede também podem ajudar a melhorar a comunicação, de tal modo que:

- Funcionários, fornecedores e clientes possam partilhar informações e estabelecer contacto mais facilmente

- A empresa pode tornar-se mais eficiente - por exemplo, o acesso em rede a uma base de dados pode evitar que os mesmos dados sejam digitados várias vezes, o que poupa tempo e evita erros

- A equipa pode consultar informação e fornecer um serviço melhor, em função da informação a que acede e pode partilhar com o cliente

BENEFÍCIOS PARA EMPRESAS

Benefícios de custos das redes de computadores

Armazenar a informação numa base de dados centralizada pode ajudar a reduzir custos e a aumentar a eficiência. Por exemplo:

A equipa pode lidar com mais clientes em menos tempo, pois tem acesso partilhado às bases de dados de clientes e de produtos

Pode reduzir custos através da partilha de periféricos e de acesso à internet

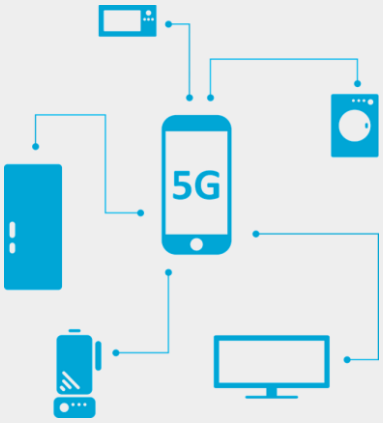
Pode centralizar a administração da rede, o que significa que necessitará de menos suporte por parte das equipas de TI

É possível reduzir erros e melhorar a consistência fazendo com que toda a equipa trabalhe a partir de uma única fonte de informação. Desta forma, podem disponibilizar-se versões padrão de manuais e diretórios e fazer cópias de segurança dos dados de forma periódica, garantindo-se, assim, uma maior consistência.

APLICAÇÕES FUTURAS

Proteger as redes de comunicação de amanhã

O 5G e outras tecnologias da próxima geração estão a colocar em alerta os gestores de segurança e de TI. Desta forma, é importante conhecer que é necessário para proteger estes novos serviços.



A TI global está a mudar muito rapidamente com tecnologias como o 5G e a loT levando ao aumento de velocidade da banda-larga e também aumentando a complexidade da conectividade. Com estas mudanças contínuas e as migrações para a próxima geração de redes de telecomunicações, os fornecedores de serviços de comunicação vêm-se obrigados a lidar não apenas com a nova tecnologia mas também com os requisitos de segurança que a acompanham.

Na linha de frente, para enfrentar estes desafios, estão os gestores de segurança, empresas e fornecedores de TI que se encarregam de supervisionar a implementação e a manutenção de novas redes e os problemas de segurança associados.

Mesmo que a tecnologia 5G possa ainda parecer uma realidade distante está na hora de os gestores de TI e de segurança aprenderem sobre estas questões e se prepararem para o que está para vir.

APLICAÇÕES FUTURAS

Partilha da responsabilidade de segurança

À medida que o ecossistema de TI global passa por uma rápida evolução, será fundamental que os departamentos de TI possuem bastantes conhecimentos da nova arquitetura de rede, da implementação de sistemas de segurança e, em última instância, de quem será responsável pelo quê. Uma vez que a tecnologia 5G e, por extensão, os seus serviços e tecnologias - como loT, IPv6 e *machine-to-machine* (M2M) se tornem o padrão no cenário de comunicações, os operadores, gestores de segurança e de TI precisarão de enfrentar e superar um conjunto de desafios de segurança que serão os mais complexos de sempre.

Alguns dos desafios específicos incluem:

Falta de pessoal qualificado e experiente para lidar com questões de segurança

Falta de orçamento para dar formação a funcionários e implementar soluções de segurança

Existência de demasiados problemas e os aspetos ligados à segurança acabam por ser desvalorizados

Falta de visibilidade no ambiente da rede geral

Uma vez que os departamentos de TI das empresas de telecomunicações precisarão de superar estes problemas enquanto estiverem a adaptar uma rede para o 5G e, eventualmente, operar uma rede exclusiva 5G, estes necessitarão do apoio de um parceiro confiável que entenda de camadas de rede, da camada do cliente e da camada de segurança. Esta ajuda deve abranger experiência comprovada em vários tipos de dados, como dados de clientes, dados de transações e dados de rede, para garantir que as informações confidenciais sejam partilhadas e protegidas de uma série de ameaças. A existência de fortes competências em arquitetura de segurança podem ser o pilar da segurança efetiva através de técnicas como a segmentação.

APLICAÇÕES FUTURAS

Proteger as redes 5G torna-se ainda mais complexo quando o *network slicing* (ou seja, a capacidade de criar múltiplas mini-redes simultâneas que operam com diferentes requisitos de serviço e segurança) entram em ação. Esta capacidade de invocar rapidamente uma instância 5G durante um período e local específico tornará os aspetos ligados à segurança uma prioridade ainda maior sendo que esta situação é um desafio para os gestores de TI e de segurança que ficarão encarregues de proteger esses dados.

Os seus clientes recorrerão a estes gestores caso exista algum tipo de problema e esta situação exigirá portanto sólidos conhecimentos e proatividade relativamente às questões de segurança. Por estes motivos, a maioria das operadoras não conseguirá "sobreviver" sozinha e ter sucesso quando for necessário superar as barreiras de segurança do 5G e outras mudanças relacionadas com redes de comunicação.

Desta forma, as operadores necessitarão de trabalhar com parceiros confiáveis que tenham experiência e histórico suficiente para garantir a integridade dos dados, a privacidade do cliente e a conformidade com qualquer ordem. Essa abordagem pode incluir:

01 Arquitetura de segurança sólida, incluindo segmentação de rede e um conjunto completo de ferramentas de segurança interoperáveis

02 Mecanismos de auditoria e garantia para fornecer aos clientes a melhor infraestrutura de segurança possível para produtos, soluções e serviços

03 Forte foco na segurança e na privacidade de dados pessoais, incluindo a identificação e proteção de informações confidenciais

04 Suporte para protocolos e sistemas de segurança estabelecidos

05 Uma organização de segurança dedicada para suportar diagnósticos e monitorizar continuamente a rede e os dados dos operadores

APLICAÇÕES FUTURAS

Implementar um plano de segurança mais eficiente

As operadoras de comunicação precisam de garantir que o subscritor e outros dados/informação estão seguros dentro dos limites da sua rede bem como nas situações em que os dados/informação atravessam nuvens públicas ou privadas. Ao implementar um plano de segurança, os operadores de comunicação podem proteger dados confidenciais, bem como proteger o *software* e os serviços de armazenamento e processamento dos dados e adequá-los às suas necessidades.

Esta estratégia incorporará os princípios do modelo de responsabilidade partilhada descrito acima e facilitaria o alinhamento das estruturas e padrões de segurança do setor tendo com o objetivo de proporcionar elevados níveis de segurança junto dos seus clientes.

Esta abordagem estratégica inclui o fornecimento de serviços e soluções seguros, projetados para garantir a confidencialidade, integridade e disponibilidade dos próprios dados e dos sistemas dos clientes contra ameaças provenientes de ataques cibernéticos, *hackers* e outras formas de invasão.

A segurança nunca deve ser alvo de uma reflexão tardia, pelo que a associação a um parceiro que leve a segurança a sério e que forneça uma solução forte aos seus clientes é fundamental para quem avança para o mundo do 5G.

CONTEÚDO AVANÇADO

Eficiência de transmissão (comunicações e rede de dados)

Um objetivo de uma rede de comunicação de dados envolve mover o maior volume possível de dados/informação precisa através de uma rede. Quanto maior o volume, maior a eficiência da rede e menor o seu custo associado. A eficiência da rede é afetada pelas características dos circuitos, como taxas de erro e velocidade máxima de transmissão, assim como pela velocidade do equipamento de transmissão e receção, a metodologia de deteção e controlo de erros e o protocolo usado pela camada de ligação de dados.

Cada protocolo que discutimos utiliza alguns bits ou bytes para delinear o início e o fim de cada mensagem e para controlar erros. Estes bits e bytes são necessários para que a transmissão ocorra, embora não façam parte da mensagem, não adicionam valor ao utilizador mas contam com o número total de bits que podem ser transmitidos.

Cada protocolo de comunicação possui bits de informação e bits de sobrecarga. Enquanto que os bits de informação são usados para transmitir o significado do utilizador os bits de sobrecarga são usados para verificação de erros e marcação do início e fim de caracteres e pacotes. Um bit de paridade usado para a verificação de erros é um bit de sobrecarga porque não é usado para enviar os dados do utilizador. Se não fosse importante detetar erros, o bit de verificação de erro de sobrecarga poderia ser omitido e os utilizadores continuariam a entender a mensagem.

CONTEÚDO AVANÇADO

A eficiência de transmissão é definida como o número total de bits de informação (isto é, bits na mensagem enviada pelo utilizador) dividido pelo total de bits na transmissão (ou seja, bits de informação mais bits de sobrecarga).
Vejamos um exemplo sobre como calcular a eficiência de transmissão de uma transmissão assíncrona. Suponha que estamos a usar o ASCII de 7 bits e temos 1 bit para paridade, mais 1 bit inicial e 1 bit final ou seja, existem 7 bits de informação em cada letra mas o total de bits por letra é 10 (7 + 3). Neste caso, a eficiência do sistema de transmissão assíncrona é de 7 bits de informação divididos por 10 bits totais, ou seja, a eficiência do sistema de transmissão é de 70%.

Por outras palavras, com a transmissão assíncrona, apenas 70% da taxa de dados está disponível para o utilizador uma vez que 30% é usado pelo protocolo de transmissão. Se tivermos um circuito de comunicação usando um *modem dial-up* que recebe 56 Kbps, o utilizador terá uma taxa de dados efetiva (ou *throughput*) de 39,2 Kbps algo que é muito ineficiente.

Podemos melhorar a eficiência de um sistema de transmissão assíncrona se reduzirmos o número de bits de sobrecarga em cada mensagem ou se aumentarmos o número de bits de informação. Por exemplo, se removermos os bits de paragem da transmissão assíncrona, a eficiência aumentará para 7/9 ou 77,8%. O *throughput* de um *modem dial-up* a 56 Kbps aumentaria para os 43,6 Kbps o que, não sendo ótimo é um pouco melhor.

CONTEÚDO AVANÇADO

A mesma fórmula básica pode ser usada para calcular a eficiência da transmissão síncrona. Por exemplo, suponha que estamos a usar o Software Development Life Cycle (SDLC). O número de bits de informação é calculado determinando quantos caracteres de informação estão na mensagem. Se a parte da mensagem do *frame* conter 100 caracteres de informação e se estivermos a usar um código de 8 bits, então existem 100x8=800 bits de informação.
O número total de bits são os 800 bits de informação mais os bits de sobrecarga que são inseridos para controlo de erros. A figura 4.9 mostra que o SDLC tem um marcador de início (8 bits); um endereço (8 bits); um campo de controlo (8 bits); e, uma sequência de verificação de *frames* (suponha que estamos a usar um CRC-32 com 32 bits) e um marcador final (8 bits). Isto dá um total de 64 bits de sobrecarga logo, a eficiência da transmissão é de 800/(800+64)=92,6%. Se o circuito fornecer uma taxa de dados de 56 Kbps, a taxa de dados efetiva disponível para o utilizador será de aproximadamente 51,9 Kbps.

Este exemplo mostra que as redes síncronas são geralmente mais eficientes do que as redes assíncronas e que alguns protocolos são mais eficientes do que outros. Além disso, quanto mais longa for a mensagem (1.000 carateres em vez de 100) mais eficiente será o protocolo. Por exemplo, suponha que a mensagem no exemplo do SDLC tem 1.000 bytes. A eficiência seria de 99,2% ou 8.000/(8000+64) fornecendo uma taxa de dados efetiva de cerca de 55,6 Kbps.

Regra geral quanto maior o campo de mensagem mais eficiente é o protocolo. Então, porque razão é que não se tem pacotes de 10.000 bytes ou mesmo 100.000 bytes para aumentar a eficiência? A resposta a esta pergunta está relacionada com o facto de que sempre que um *frame* com erros é recebido todos os *frames* tem de ser retransmitidos. Assim, se um arquivo inteiro for enviado como um pacote grande (por exemplo de 100K) e um bit for recebido com algum erro, todos os 100.000 bytes deverão ser enviados novamente. Ora, esta situação é claramente um desperdício de capacidade. Para além disso, a probabilidade de um *frame* conter um erro aumenta com o tamanho do *frame*, ou seja, os *frames* maiores são mais propensos a conter erros do que os *frames* mais pequenos devido à lei da probabilidade.

CONTEÚDO AVANÇADO

Assim, ao projetar um protocolo, existe um *trade-off* entre *frames* grandes e pequenos. Os *frames* pequenos são menos eficientes mas também são menos propensos a conter erros e tem um custo inferior, em termos de capacidade do circuito, caso seja preciso retransmitir caso haja um erro.

A taxa de transferência corresponde ao número total de bits de informação recebidos por segundo depois de ser considerada a sobrecarga de bits e a necessidade de retransmitir frames que contenham erros. De forma geral, os *frames* pequenos fornecem uma melhor taxa de transferência para circuitos com mais erros enquanto que os *frames* maiores fornecem uma melhor taxa de transferência em redes menos propensas a erros. Felizmente, na maioria das redes reais, a curva mostrada na figura 4.12 é muito plana na parte superior, o que significa que existe uma variedade de tamanhos de *frames* que fornecem um desempenho quase perfeito. Os tamanhos dos *frames* variam muito entre redes mas o tamanho ideal tende a situar-se entre os 2.000 e os 10.000 bytes.

O que é a IoT?

https://www.youtube.com/watch?v=LlhmzVL5bm8

Kit de ferramentas IoT

http://iotservicekit.com/

http://tilestoolkit.io/

EDUCAÇÃO

Checklist de segurança na IoT:

https://www.enisa.europa.eu/news/enisa-news/your-must-have-iot-security-checklist-enisas-online-tool-for-iot-and-smart-infrastructures-security

MOOCS:

- ❑ Introdução à Rede Informática - Standford University
- ❑ Fundamentos de Comunicação em Rede - Coursera
- ❑ Tecnologias Emergentes em Disposíveis Inteligentes e Móveis - Coursera

MANUAIS EXTERNAS PARA MAIS INFORMAÇÃO:

- ❑ Networking Fundamentals - Cisco
- ❑ Network-based communication for Industrie 4.0 - Plattform Industrie 4.0
- ❑ Computer networking fundamentals - Study
- ❑ Communication Networks - Samson

BIBLIOGRAFIA

- *Importance of Communication Networks*. Disponível em: https://study.com/academy/lesson/importance-of-communication-networks.html.
- *Networking Fundamentals*. (2006). Disponível em: https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf.
- *Benefits of computer networks.* Disponível em: https://www.nibusinessinfo.co.uk/content/benefits-computer-networks.
- Cope, S. (2018). *Basic Networking Concepts-Beginners Guide*. Disponível em: http://www.steves-internet-guide.com/networking/.
- *Top 5 Computer Networking Skills You Need to Learn Today* [Updated 2019]. (2019). Disponível em: https://potomac.edu/the-top-5-skills-needed-to-become-a-computer-network-professional/.
- *Top 10 skills you need for a high-paying IoT career.* (2018). Disponível em: http://techgenix.com/iot-career-skills/.

AUTOAVALIAÇÃO

- ★ Após a leitura deste texto tenho uma ideia clara do que é a comunicação em rede?
- ★ Que competências devo melhorar no meu trabalho?

- ★ Conheço os benefícios que a comunicação em rede pode trazer à minha empresa?
- ★ Como posso detetar necessidades de formação da minha equipa?

O apoio da Comissão Europeia à produção desta publicação não constitui a aprovação do seu conteúdo, o qual reflete apenas as visões dos autores, sendo que a Comissão Europeia não pode ser responsabilizada por qualquer uso que possa ser feito da informação nela contida.