Erasmus Plus Programme – KA2 Strategic Partnerships for higher education

IO1: Industrial Cyber Security Training Course for Technicians in Industry 4.0

Portuguese Version

Project № 2018-1-ES01-KA203-050493

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 1

Sistemas Industriais - Componentes e Caracteristicas

1.1 Componentes de um Sistema de Controle Industrial

Description

Componentes de um Sistema de Controle Industrial

Table of contents

1. Definição de um Sistema de Controlo Industrial

2. Estrutura

2.1. Nível de campo (nível 0)

2.2. Controle Direto (nível 1)

2.3. Supervisão das instalações (nível 2)

2.4. Controle de Produção (nível 3)

2.5. Programação de Produção (nível 4)

1. Definição de um Sistema de Controlo Industrial

Sistema de Controle Industrial (**ICS**) é um termo geral que abrange vários tipos de sistemas de controle, redes e instrumentação associada utilizada para controle de processos industriais. Como se apresenta na Figura 1.1, o controle de processo é implementado usando loops nos quais o valor de uma variável de processo medida (PV) é automaticamente ajustado para igualar o valor de um ponto de ajuste desejado (SP). Inclui o sensor do processo, a função do controlador, e o elemento de controle final (FCE) que são exigidos para o controle automático.

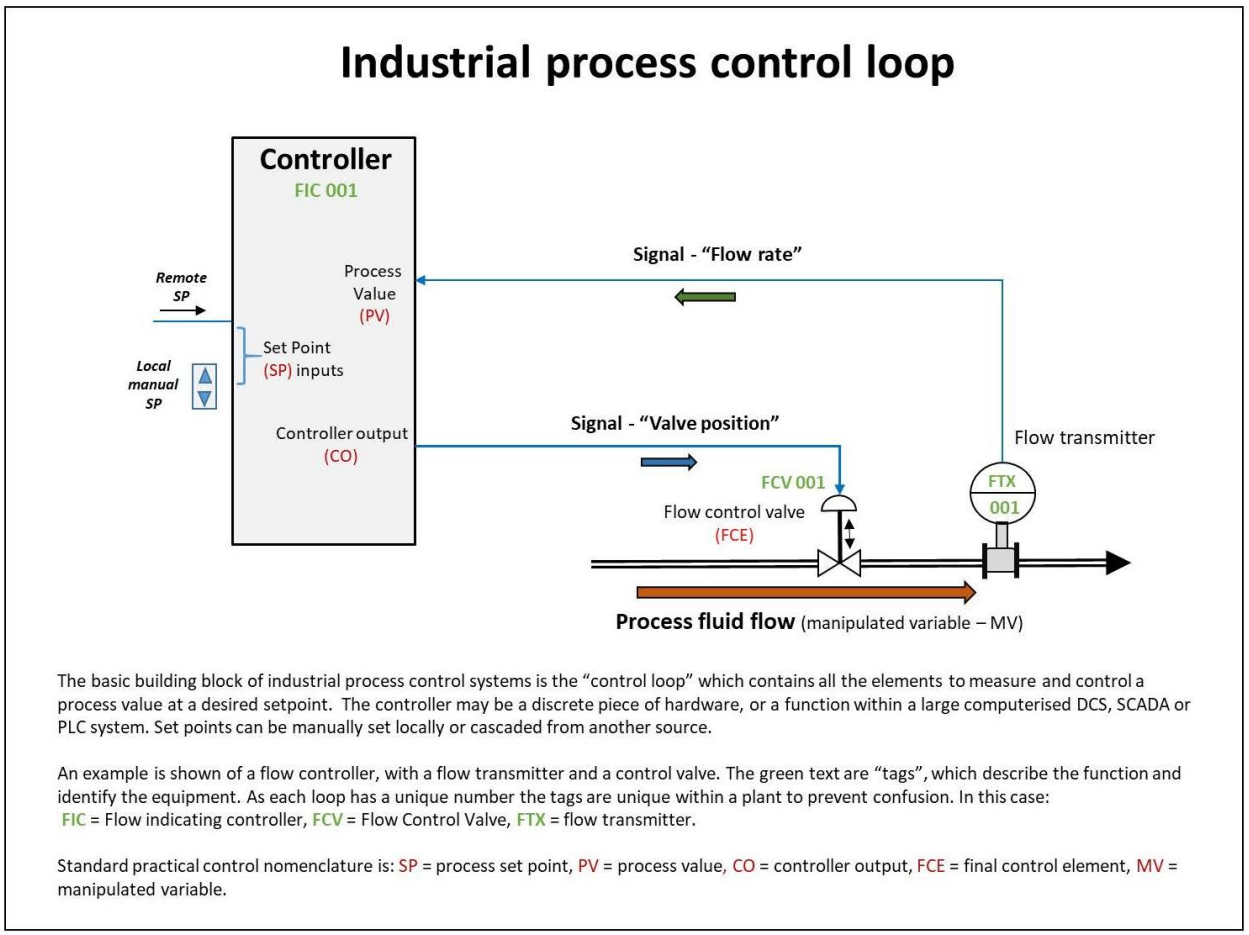


Figura 1.1- Ciclo de controle de processo industrial (fonte: Wikipedia)

Esses sistemas podem variar desde alguns controladores modulares montados em painéis a grandes sistemas de controle interligados, distribuídos e interativos com muitos milhares de ligações de campo. Todos os sistemas recebem dados de sensores remotos medindo variáveis de processo, comparam-nas com os pontos definidos desejados e derivam funções de comando que são utilizadas para controlar um processo através dos elementos de controle finais, como válvulas de controle.

Existem vários tipos de ICSs, os mais comuns são **Sistemas de Controle de Supervisão e Aquisição de Dados (SCADA)** e **Sistemas de Controle Distribuído (DCS)**. Na prática, grandes sistemas SCADA têm evoluído para se tornarem muito semelhantes aos sistemas de controle distribuídos em função, mas usando vários meios de interação com a fábrica.

Como se apresenta na Figura 1.2, os ICS estão integrados nas empresas industriais como mostra o próximo diagrama. A equipa de gestão utiliza dados da fábrica e toma decisões com base nesses ICSs, resultando em planos que são transferidos para o nível de produção e devem ser realizados utilizando recursos controlados pelo ICS.

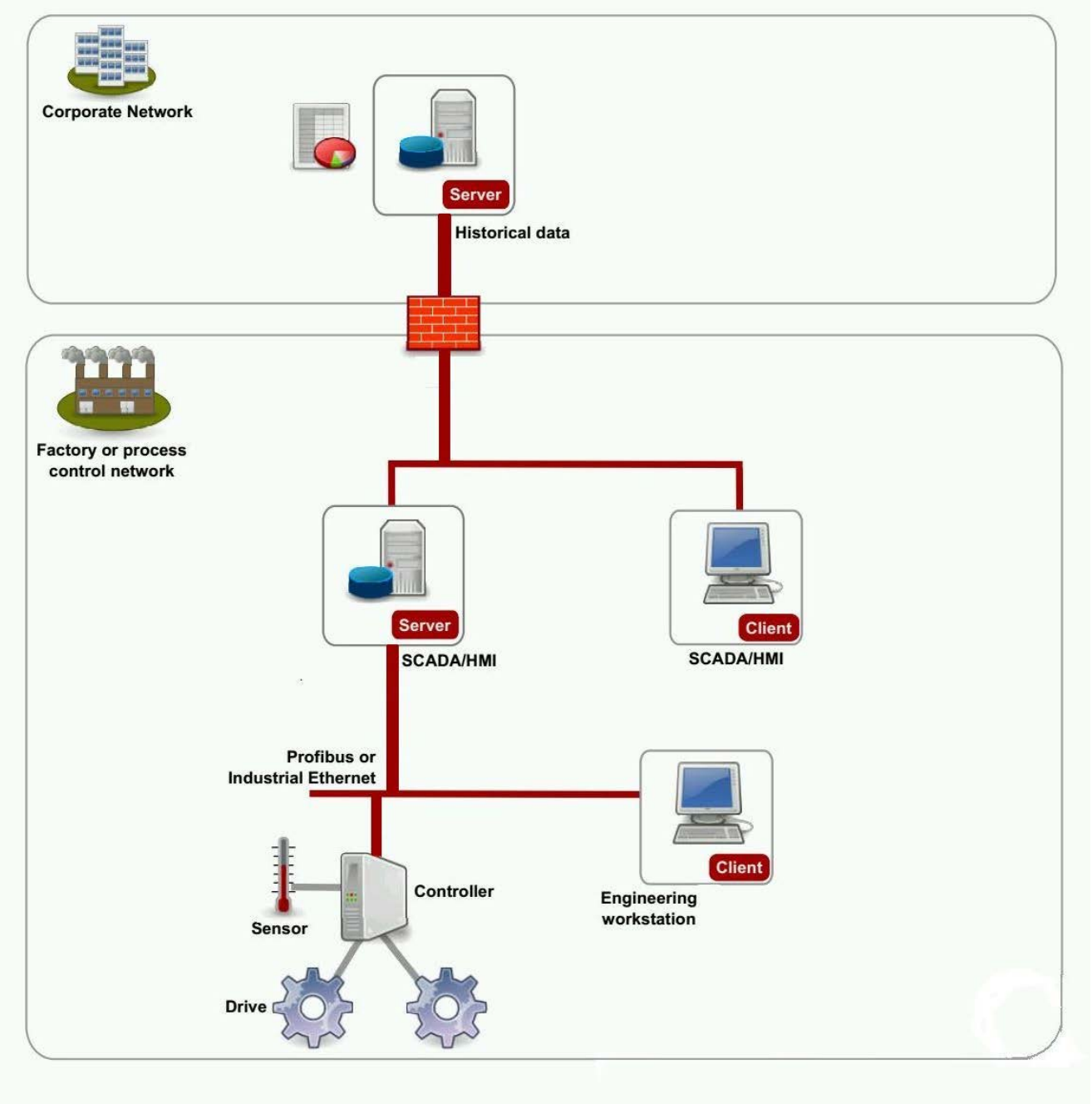


Figura 1.2 - Integração do ICS numa empresa (fonte: Open Security Archive)

Um caso específico de ICS é o Sistema de Instrumentos de Segurança (**SIS**), que consiste num conjunto de controlos de hardware e software projetados especialmente para sistemas de processo críticos , como os usados em **refinarias, instalações químicas e nucleares**, para fornecer proteção, como abrir/fechar uma válvula em estado crítico, a fim de reduzir a sobrepressão de gases perigosos ou a alta temperatura de líquidos.

O sistema de instrumentos de segurança é composto pelos mesmos tipos de elementos de controlo (incluindo sensores, solucionadores lógicos, atuadores e outros equipamentos de controlo) de um Sistema Básico de Controlo de Processo (BPCS).

No entanto, todos os elementos de controlo num SIS são dedicados exclusivamente ao bom funcionamento do SIS. Os sistemas de **suporte**, como a energia, o ar do instrumento e as comunicações, são geralmente necessários para a operação do SIS. Os sistemas de suporte devem ser projetados para fornecer a **integridade e a confiança necessárias**.

2. Estrutura

Os ICSs são tipicamente divididos em **5 níveis**, mostrados na Figura 1.3. Cada nível tem a sua própria funcionalidade e deve comunicar com os outros níveis para executar as ações planeadas.

A aquisição de dados começa no nível 1 **RTU** ou **PLC** e inclui leituras de instrumentação e de relatórios de estado do equipamento que são comunicados ao SCADA nível 2, conforme necessário. Os dados são então compilados e formatados de forma a que um operador da sala de controlo, usando a interface **HMI** (Interface Homem Máquina), possa tomar decisões de supervisão para ajustar ou substituir os controlos normais de RTU ou PLC. Os dados também podem ser fornecidos a um histórico, geralmente construído num sistema de gestão de base de dados de mercadorias, para permitir auditorias de tendências e outras auditorias de análise.

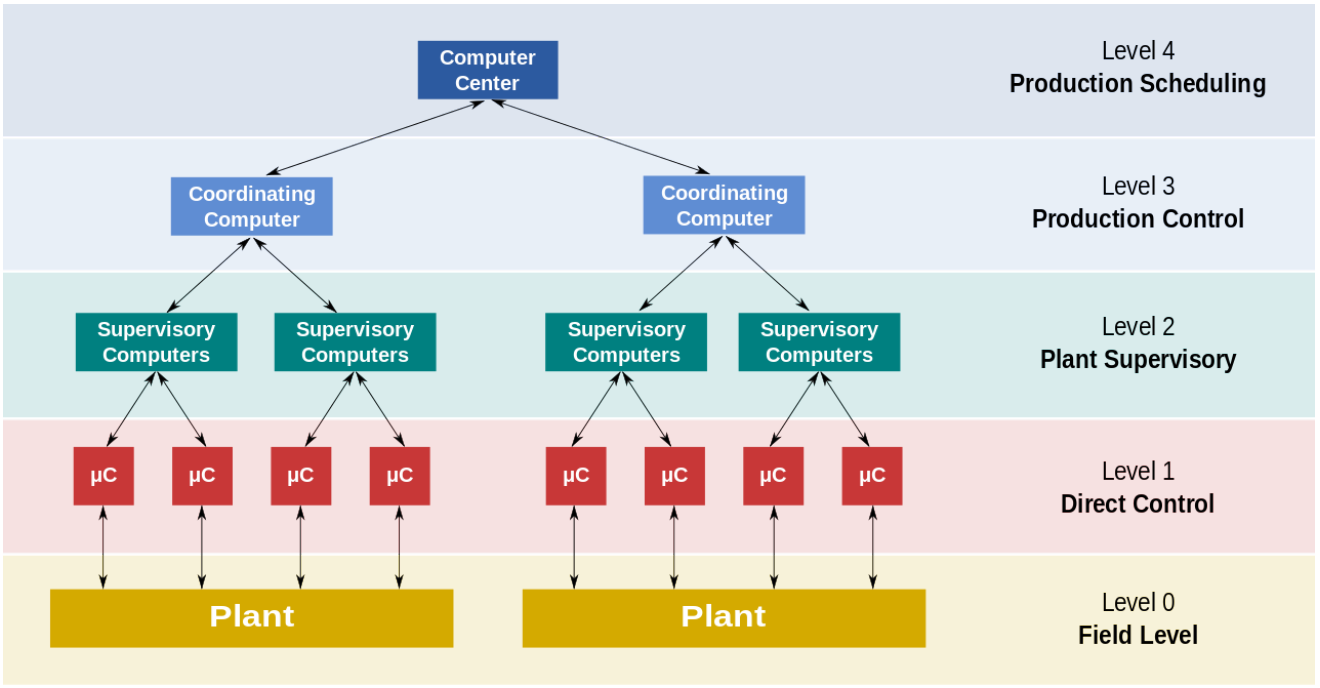


Figura 1.3 - Níveis de ICS (fonte: Wikipedia)

2.1. Nível de campo (nível 0)

Este nível contem os dispositivos do campo tais como **sensores** e elementos de controlo final, ou **atuadores**.

De uma forma geral, um sensor é um dispositivo, módulo ou subsistema cujo objetivo é detectar eventos ou mudanças no seu ambiente e enviar essa informação para outros componentes eletrónicos, frequentemente um processador de computador. Um sensor é sempre usado com outros elementos eletrónicos.

Os sensores (a Figura 1.4 apresenta um sensor de infravermelhos) são utilizados em objetos do quotidiano, como botões sensíveis ao toque (sensor tátil) e em processos industriais para medir magnitudes diferentes (pressão, posição, temperatura ...).

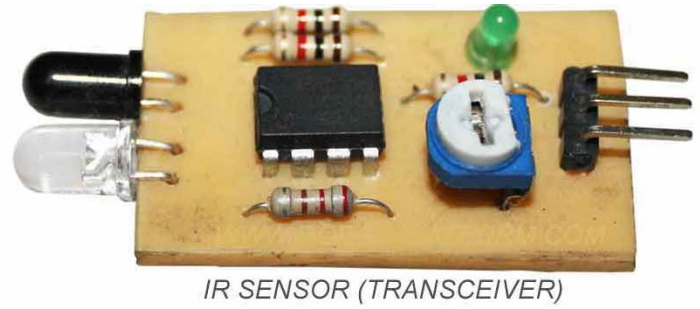


Figura 1.4- sensor IR (fonte: Wikipedia)

Um atuador (a Figura 1.5 mostra uma válvula hidráulica) é um componente de uma máquina responsável por mover e controlar um mecanismo ou sistema, por exemplo, abrindo uma válvula. Em termos simples, é um "motor".
Um atuador requer um sinal de controlo e uma fonte de energia. O sinal de controlo é de energia relativamente baixa e pode ser constituído por tensão ou corrente elétrica, pressão pneumática ou hidráulica, ou até energia humana. Quando recebe um sinal de controlo, um atuador responde convertendo a energia do sinal em movimento mecânico.

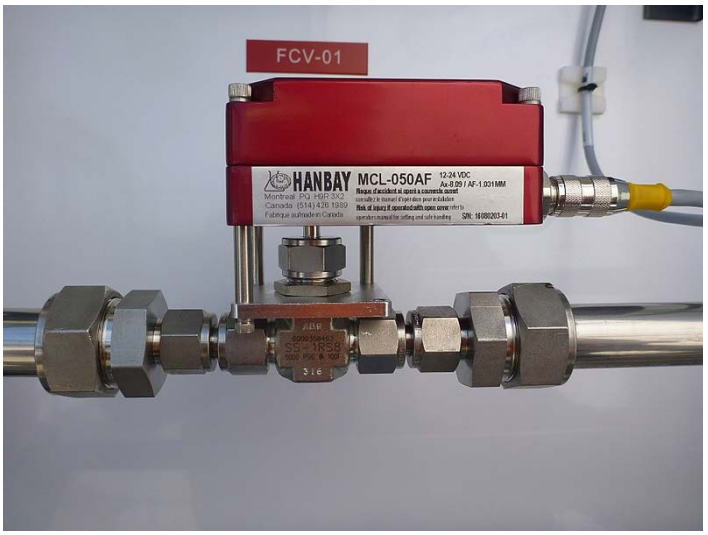


Figura 1.5 - Válvula Hidraulica (fonte: Wikipedia)

2.2. Controle Direto (nível 1)

Esse nível contém os módulos de entrada/saída industrializados (I/O) e os seus processadores eletrónicos distribuídos associados. Contém os controladores lógicos programáveis (PLCs) ou as unidades terminais remotas (RTUs).

Um **controlador lógico programável** (**PLC**) é um computador digital industrial que foi reforçado e adaptado para o controlo de processos de fabrico, como linhas de montagem ou dispositivos robóticos, ou qualquer atividade que exija controlo de alta confiança e facilidade de programação e de diagnóstico de falhas no processo.

Um PLC (Figura 1.6) é um exemplo de um sistema de tempo real "rígido", pois os resultados de saída têm de ser produzidos em resposta às condições de entrada dentro de um período de tempo limitado, caso contrário, ocorrerá uma operação não intencional.

Figura 1.6- Controlador Lógico Programável (fonte: Wikipedia)

A Figura 1.7 mostra uma unidade terminal remota **(RTU)**, que consiste num dispositivo eletrónico controlado por microprocessadores que medeia a interação de objetos no mundo físico com um sistema de controle distribuído ou sistema SCADA (Controlo Supervisão e Aquisição de Dados), transmitindo dados de telemetria para um sistema principal e usando mensagens do sistema de supervisão principal para controlar objetos ligados. Outros termos que podem ser usados para a RTU são unidade remota de telemetria e unidade remota de telecontrolo.

Figura 1.7- Unidade terminal remota (fonte: Wikipedia)

2.3. Supervisão das instalações (nível 2)

Este nível contém os **computadores supervisores**, que recolhem informações dos nós do processador no sistema, e fornecem os ecrãs de controlo do operador.

O nível 2 contém o software **SCADA** e a plataforma de computação. O software SCADA existe apenas neste nível de supervisão, pois as ações de controlo são executadas automaticamente pelas RTUs ou PLCs de Nível 1. As funções de controlo do SCADA geralmente são restritas a intervenções básicas de substituição ou de supervisão. Por exemplo, um PLC pode controlar o fluxo de água de refrigeração através de parte de um processo industrial, até um ponto nível determinado, mas o software do sistema SCADA permitirá que os operadores alterem os pontos definidos para o fluxo.

O SCADA também permite que as condições do **alarme**, como perda de fluxo ou alta temperatura, sejam exibidas e registradas. Um **loop de controlo de feedback** é diretamente controlado pela RTU ou PLC, mas o software SCADA monitoriza o desempenho geral do loop.

A **interface homem-máquina (HMI)** (a Figura 1.8 mostra um painel tátil típico de uma HMI) é a janela do operador do sistema de supervisão. Apresenta graficamente informações da fábrica ao pessoal operacional, em diagramas que são uma representação esquemática da área controlada, e as páginas de registo de alarmes e entradas. A HMI está vinculada ao computador de supervisão SCADA para fornecer dados em tempo real qie permitam acionar os diagramas, os registos de alarme e os gráficos de tendências. Em muitas instalações, a HMI é a interface gráfica do utilizador do operador, recolhe todos os dados de dispositivos externos, cria relatórios, executa alarmes, envia notificações, etc..

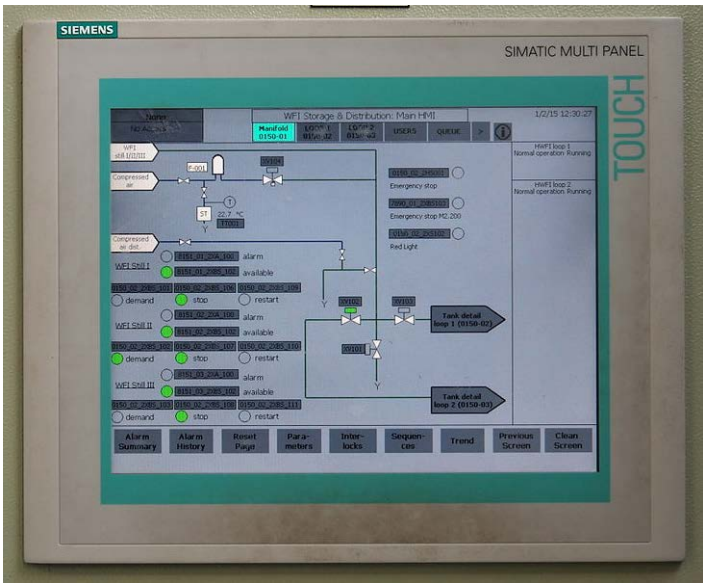


Figura 1.8- Painel Tátil HMI (fonte: Wikimedia)

O núcleo do sistema SCADA é a **Estações de Trabalho (workstation) de Supervisão**, que recolhe dados sobre o processo e envia comandos de controlo para os dispositivos ligados na área. Refere-se ao computador e software responsáveis pela comunicação com os controladores de ligação na área, os RTUs e PLCs, e inclui o software HMI em execução nas estações de trabalho do operador.

Em sistemas SCADA menores, o computador de supervisão pode ser composto por um único PC. Neste caso, a HMI faz parte deste computador. Em sistemas SCADA maiores, a estação principal pode incluir várias HMIs hospedadas em computadores clientes, vários servidores para aquisição de dados, aplicações de software distribuídas e áreas de recuperação de desastres. Para aumentar a integridade do sistema, os vários servidores são geralmente configurados numa formação com redundância dupla ou hot-standby, fornecendo controlo e monitorização contínuos, no caso de mau funcionamento ou falha do servidor.

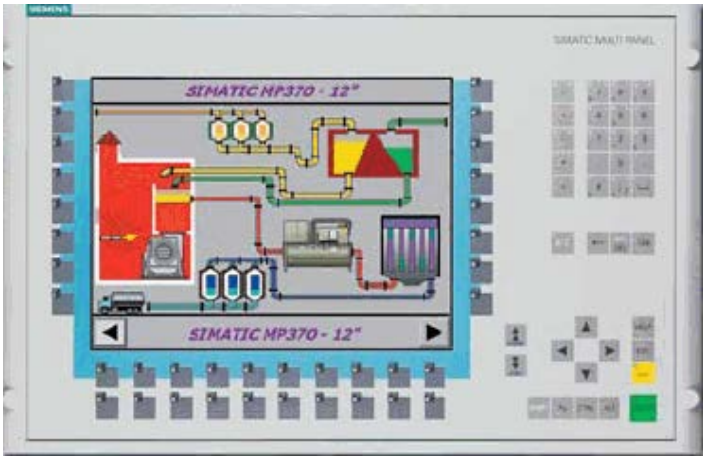


Figura 1.9 - Ecrã SCADA (fonte: Wikimedia)

2.4. Controle de Produção (nível 3)

Os níveis 3 e 4 não constituem estritamente controlo de processo no sentido tradicional, mas é onde o controlo e a programação da produção ocorrem.

Este nível não controla diretamente o processo, mas relaciona-se com **a monitorização da produção e dos objetivos**. Contém sistemas MES, CMMS e WMS

Sistemas de Execução de Fabrico (MES) são sistemas informatizados usados na produção para rastrear e documentar a transformação de matérias primas em produtos acabados. O MES fornece informações que ajudam os tomadores de decisão de produção a entender de que forma as condições atuais do chão da fábrica podem ser otimizadas para melhorar a produção. O MES trabalha em tempo real para permitir o controlo de vários elementos do processo de produção. A Figura 1.10 mostra as diferentes partes de um sistema MES.

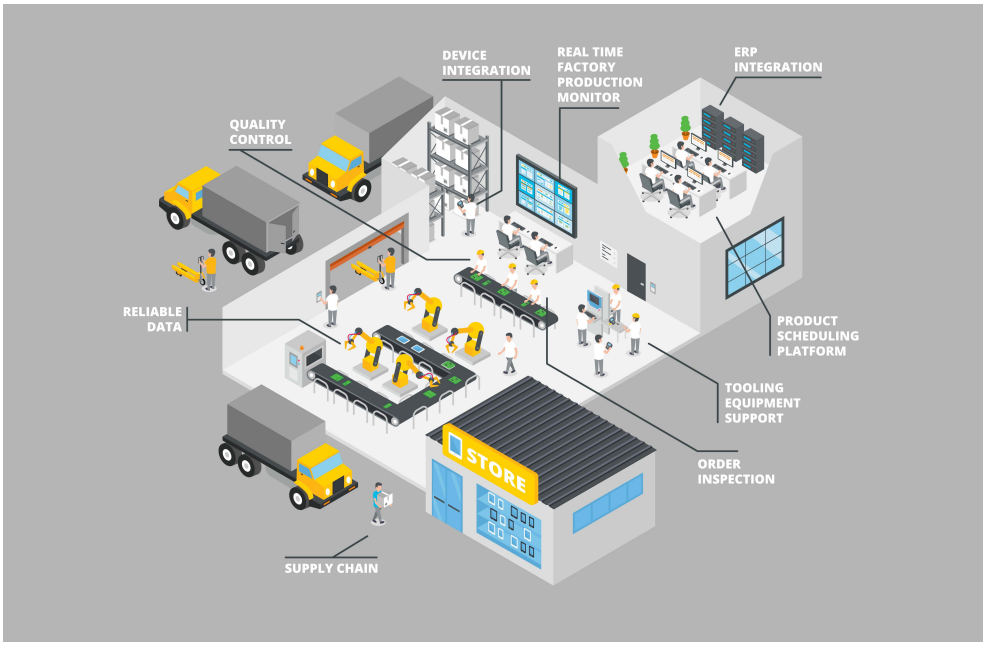


Figura 1.10- - Organização da empresa para gestão do MES (fonte: Wikimedia)

Sistema de Gestão de Armazém (WMS) é uma aplicação de software, concebida para suportar e otimizar a funcionalidade do armazém e a gestão do centro de distribuição. Estes sistemas facilitam a gestão no planeamento diário, na organização, na equipa, na direção e controlo da utilização dos recursos disponíveis, para movimentar e armazenar materiais, dentro e fora de um armazém, além de apoiar a equipa no desempenho desses movimentos.

O sistema informatizado de gestão de manutenção (CMMS), é um pacote de software que mantém uma base de dados informatizada sobre as operações de manutenção de uma organização. Estas informações destinam-se a ajudar os trabalhadores da manutenção a realizarem as suas tarefas com mais eficiência (por exemplo, determinar que máquinas requerem manutenção e quais os depósitos que contêm as peças de reposição necessárias) e para ajudar a Gestão a tomar decisões informadas (por exemplo, calcular o custo da reparação de avarias da máquina versus a manutenção preventiva de cada máquina, possivelmente permitindo assim uma melhor alocação de recursos).

2.5. Programação de Produção (nível 4)

Este nível contém sistemas de ERP e a sua principal função é fornecer informações e suporte a decisões para a equipa de gestão.

Planeamento de recursos empresariais (ERP) é geralmente referido como uma categoria de software de gestão de negócios - geralmente um conjunto de aplicações integradas - que uma organização pode utilizar para recolher, armazenar, gerir e interpretar dados, em tempo real, a partir dessas diversas atividades de negócio. Fornece uma visão integrada e continuamente atualizada dos principais processos de negócios, usando bases de dados comuns mantidas por um sistema de gestão de base de dados.

Os sistemas ERP rastreiam os recursos comerciais - dinheiro, matérias primas, capacidade de produção - e o estado dos compromissos comerciais: pedidos, ordens de compra e registo de pagamentos. As aplicações que compõem o sistema compartilham dados entre vários departamentos (manufatura, compra, venda, contabilidade, etc.) que fornecem os dados.

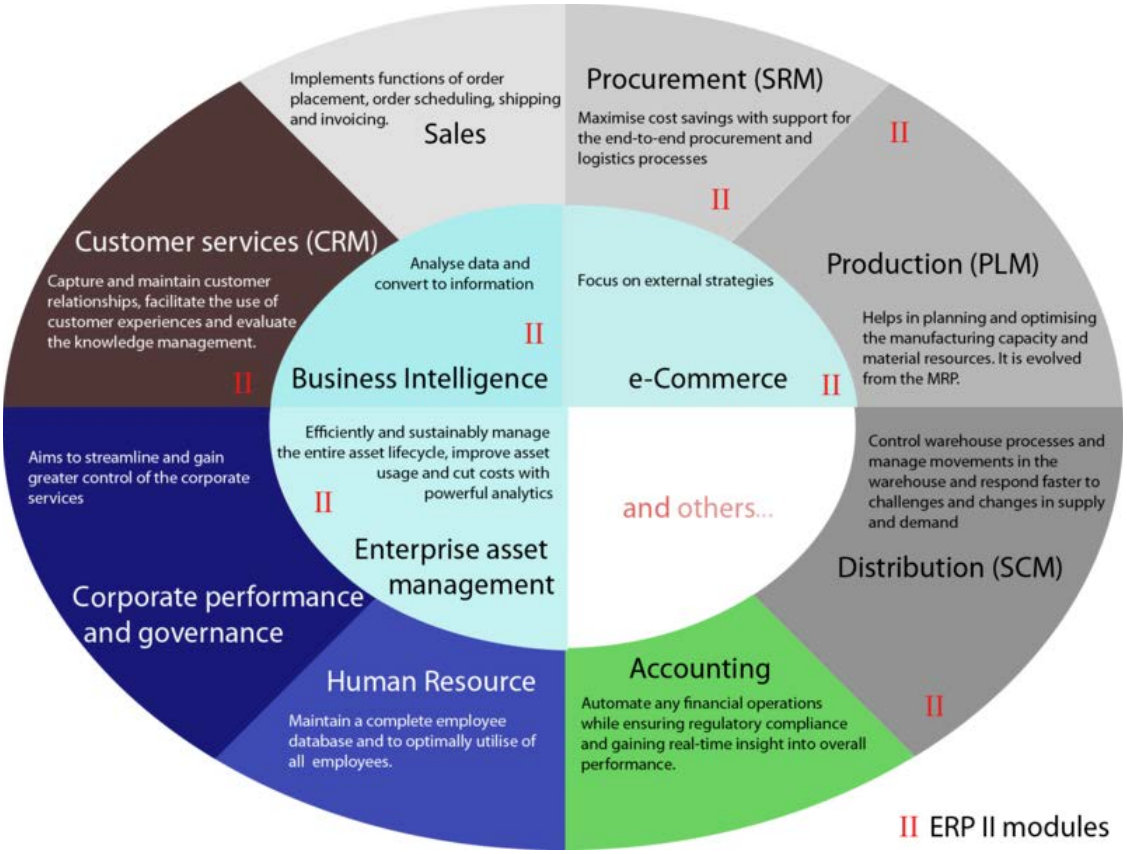


Figura 1.11- Módulos ERP de acordo com a estrutura da empresa (fonte: Wikipedia)

1.2 Design e arquitetura de redes

Description

Design e arquitetura de redes

Table of contents

1. Níveis OSI

2. Encapsulamento de dados

3. Topologias físicas
3.1. Topologia BUS
3.2. Topologia em estrela
3.3. Topologia em anel
3.4. Topologia celular

4. Desempenho da rede

5. Redes de computadores

6. Protocolos de rede
6.1. Padrões de série: RS232, RS485
6.2. Ethernet
6.3. TCP / IP

7. Segmentação de rede
7.1. Switches e VLANs
7.2. Routers e sub-redes
7.3. Firewalls

8. Acesso remoto
8.1. Telnet e SSH
8.2. Área de trabalho remota
8.3. VPN

1. Níveis OSI

No capítulo anterior, afirmou-se que os Sistemas de Controle Industrial (Figura 1.12) são compostos por dispositivos interligados que compartilham e transferem informações entre eles. Neste capítulo, estudaremos quais são as estruturas de rede mais comuns e quais as suas características.

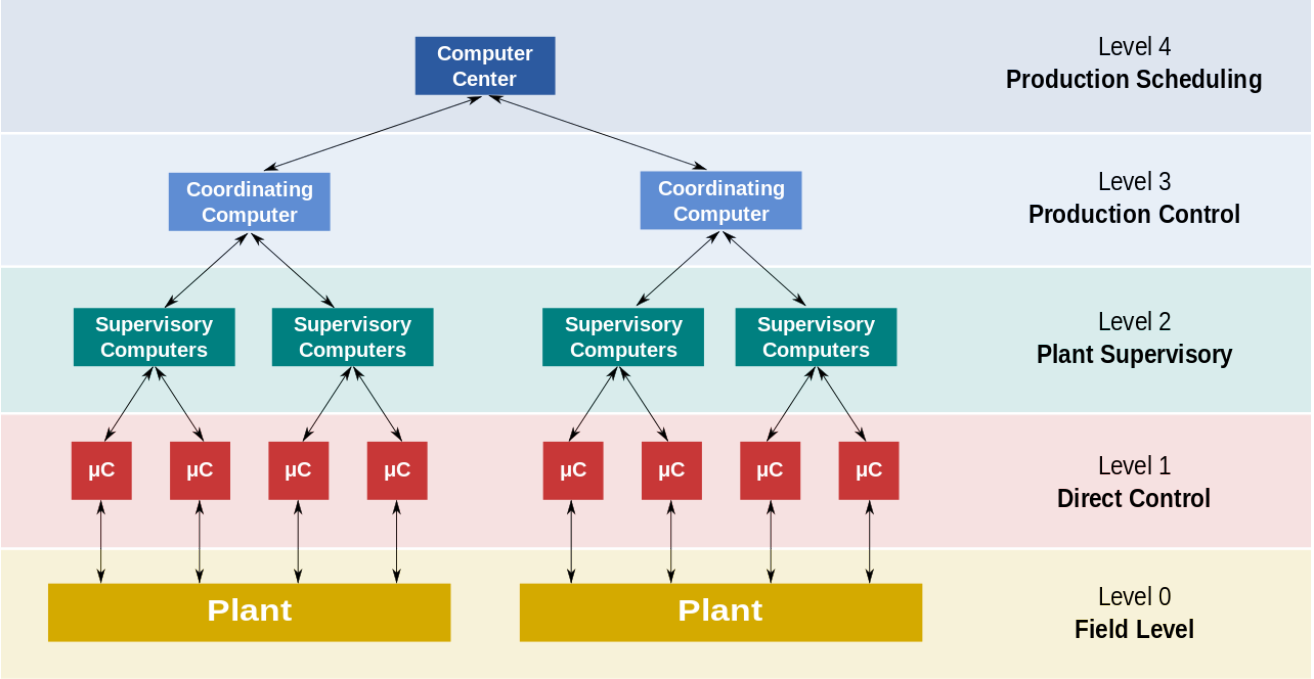


Figura 1.12- Níveis ICS (fonte: Wikipedia)

Nesse sentido, começaremos a estudar o **Modelo de Interligação de Sistemas Abertos** (**modelo OSI**), que é um modelo concetual que caracteriza e padroniza as funções de comunicação de um sistema de telecomunicações ou de computação independentemente da estrutura e tecnologia internas subjacentes. O seu objetivo é a interoperabilidade de diversos sistemas de comunicação com protocolos padrão. O modelo divide um sistema de comunicação em camadas de abstração. A versão original do modelo definiu sete camadas.

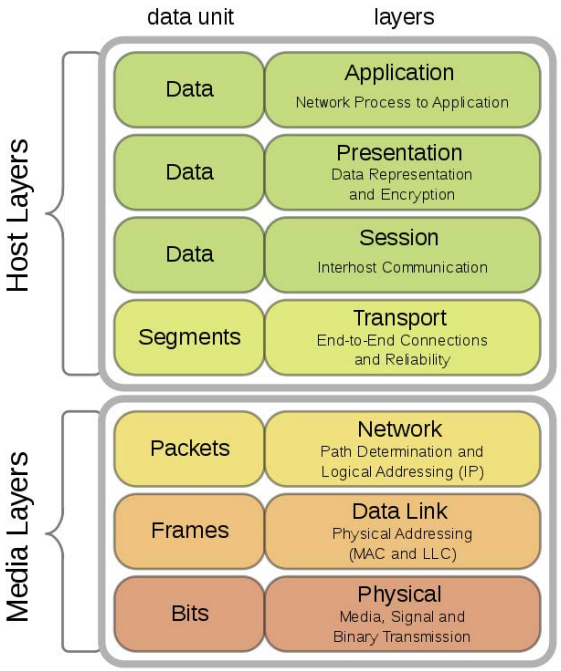


Figura 1.13- Níveis OSI (fonte: Wikipedia)

A **camada física** é responsável pela transmissão e recepção de dados em bruto, não estruturados, entre um dispositivo e um meio de transmissão físico.

Converte os bits digitais em sinais elétricos, de rádio ou ópticos. As especificações da camada definem características como níveis de tensão, tempo de mudanças de tensão, taxas de dados físicos, distâncias máximas de transmissão, esquema de modulação, método de acesso ao canal e conectores físicos.

A **camada de vínculo de dados** fornece a transferência de dados de nó a nó. Divide-se em duas subcamadas:

Camada de controle de acesso médio (**MAC**) - responsável por controlar como os dispositivos numa rede obtêm acesso a um meio e à permissão para transmitir dados.

Camada de controle de link lógico (**LLC**) - responsável por identificar e encapsular protocolos da camada de rede e controla a verificação de erros e a sincronização de quadros.

Os protocolos **802.3 Ethernet** e **802.11 Wi-Fi**, operam na camada de relação de dados.

A **camada de rede** é responsável por **transferir** sequências de dados (**pacotes**) de um nó para outro ligados em "**redes diferentes**". Estes nós são identificados por um endereço de camada 3, tipicamente **endereço IP**.

Os **routers** são responsáveis por transferir os pacotes para os nós de destino, encontrando o seu percurso nas diferentes redes.

A **camada de transporte** é responsável por **transferir** sequências de dados (chamadas **segmentos**) de uma origem para um host de destino, mantendo a **qualidade de serviço**. Protocolos como o **TCP** e o **UDP** funcionam nesse nível. **As portas** definidas neste nível são os pontos de entrada para os serviços públicos do servidor.

A **camada de sessão** controla os **diálogos** (também conhecidos como ligações ou sessões) entre computadores (entre aplicações locais e remotas).

A **camada de apresentação** permite a comunicação entre sistemas com **sintaxe** e semântica diferente (por exemplo, códigos **ASCII** e EBCDIC, compressão de vídeo **MPEG** ou estrutura de dados XML).

A **camada de aplicações** interage com as **aplicações de software** que implementam um componente de comunicação. Tais aplicações (por exemplo, servidor/clientes **FTP** , navegadores de internet...) estão fora do âmbito do modelo OSI.

Os protocolos conhecidos da Camada 7 são **HTTP**, **Modbus.**

2. Encapsulamento de dados

Em redes de computadores, o **encapsulamento** é um método de projetar protocolos de comunicação modulares, onde cada camada cria uma unidade de dados de protocolo (PDU) ao adicionar-se um cabeçalho (e algumas vezes trailer) contendo informações de controlo à PDU da camada acima.

A camada física é responsável pela transmissão física de dados, o encapsulamento de ligações permite a rede local, o Internet Protocol (IP) fornece a direção global de computadores individuais e o Protocolo de Controle de Transmissão (TCP) seleciona o processo ou aplicação, ou seja, a porta que especifica o serviço como um servidor Web ou TFTP.

Por exemplo, no conjunto de protocolos da Internet, o conteúdo de uma página Web é encapsulado com um cabeçalho HTTP, depois por um cabeçalho TCP, um cabeçalho IP e, finalmente, por um cabeçalho e trailer de enquadramento. O enquadramento é encaminhado para o nó de destino como um fluxo de bits, onde é desencapsulado nas respectivas PDUs e interpretado em cada camada pelo nó recetor.

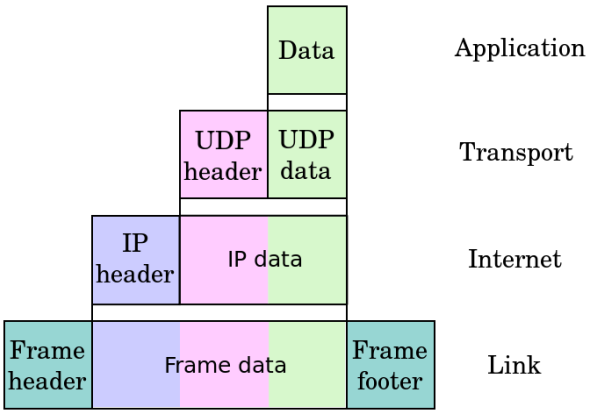


Figura 1.14- Encapsulamento de dados (fonte: Wikipedia)

3. Topologias físicas

Topologia de rede é a organização dos elementos (links, nós, etc.) de uma rede de comunicação.

Topologia física é o posicionamento dos vários componentes de uma rede (por exemplo, localização do dispositivo e instalação de cabos), enquanto a topologia lógica ilustra como os dados fluem dentro de uma rede. As distâncias entre nós, interligações físicas, taxas de transmissão ou tipos de sinal podem diferir entre duas redes diferentes, mas as suas topologias podem ser idênticas.

A topologia física de uma rede é uma especificidade da camada física do modelo OSI.

3.1. Topologia BUS

Na topologia bus, as estações de trabalho são conectadas diretamente a uma ligação half-duplex linear comum, com algum meio, como um par trançado ou um cabo coaxial, e recebem todo o tráfego gerado por cada estação. No término da linha, precisam de um resistor de fim que elimine os saltos do sinal.

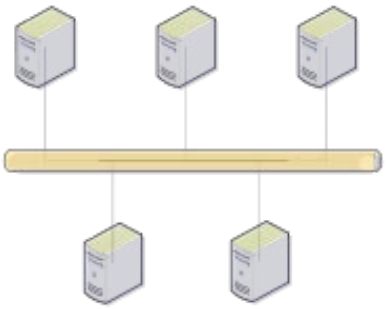


Figura 1.15- Topologia Bus (fonte: Wikipedia)

3.2. Topologia em estrela

Numa rede em estrela, cada host é ligado a um hub central (geralmente um switch), que retransmite as mensagens das estações de envio para as recetoras. Esta é uma das topologias de rede de computadores mais comuns.

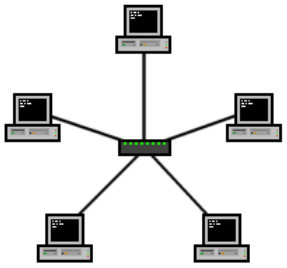


Figura 1.16- Topologia em Estrela (fonte: Wikipedia)

3.3. Topologia em anel

Uma rede em anel é uma topologia de rede na qual cada nó se liga exatamente a outros dois nós, formando um único caminho contínuo para sinais, através de cada nó. Os dados passam de um nó para outro, e cada nó lida com cada pacote de dados ao longo do percurso.

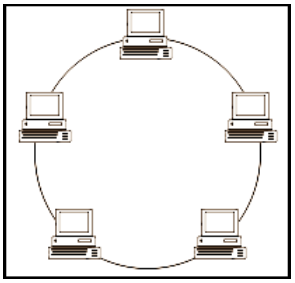


Figura 1.17- Topologia em Anel (fonte: Wikimedia)

3.4. Topologia celular

Uma rede celular é uma rede de comunicação em que o último link é sem fio. A rede é distribuída por áreas chamadas células, cada uma servida por pelo menos um ponto de acesso. Estes nós fornecem à célula a cobertura de rede que pode ser usada para transmissão de voz, dados e outros tipos de conteúdo.

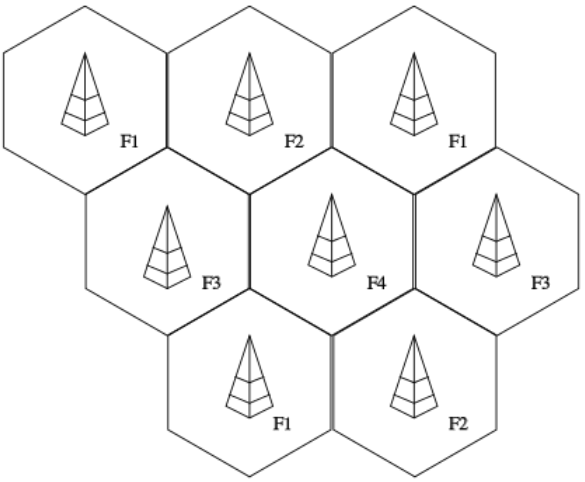


Figure 1.18- Topologia Celular (fonte: Wikipedia)

4. Desempenho da rede

Largura de banda e **Latência** (Figura 1.19) são duas das características mais relevantes numa rede digital.

A latência é expressa numa unidade de tempo, geralmente milissegundos (ms). Latência consiste na quantidade de tempo que os dados levam para passarem de um ponto para outro. A latência depende da distância física que os dados têm de percorrer pelos cabos, redes e similares para chegarem ao seu destino.

A largura de banda (bandwidth) é expressa em bits por segundo (bps). Refere-se à quantidade de dados que podem ser transferidos durante um segundo. Obviamente, quanto mais largo for o tubo, mais bits podem ser transferidos por segundo. E se sua largura de banda estiver congestionada, a sua latência (atraso) aumentará.

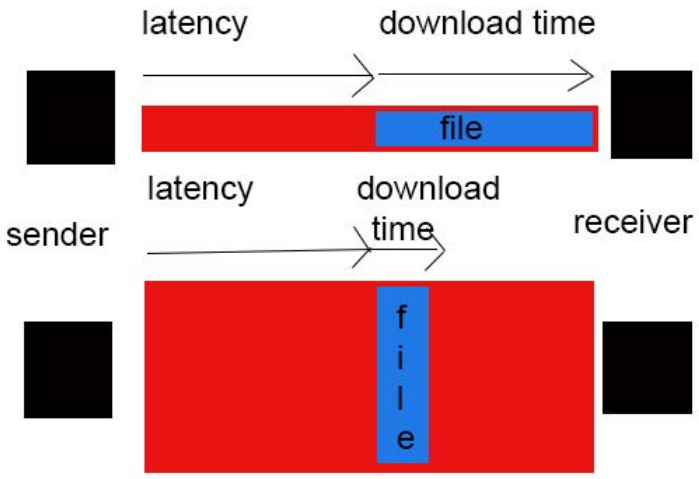


Figura 1.19 - Latência de transmissão e largura de banda (fonte: Wikipedia)

Na transmissão digital, a **taxa de erro de bits** (**BER**) corresponde ao número de erros de bits por unidade de tempo. A taxa de erro de **bits** (também **BER**) é o número de erros de bits dividido pelo número total de bits transferidos durante um intervalo de tempo estudado. A taxa de erro de bit é uma medida de desempenho sem unidade, geralmente expressa como uma percentagem.

Os bits recebidos de um fluxo de dados sobre um canal de comunicação podem ser alterados devido a ruído, interferência, distorção ou erro de sincronização de bits. O parâmetro Relação Sinal-Ruído (SNR) indica a proporção do sinal não desejado relacionado com o sinal de transmissão de informações. Como mostra a Figura 1.20, quanto mais elevado for o SNR (melhor sinal), menor o BER (menos erros durante a transmissão).

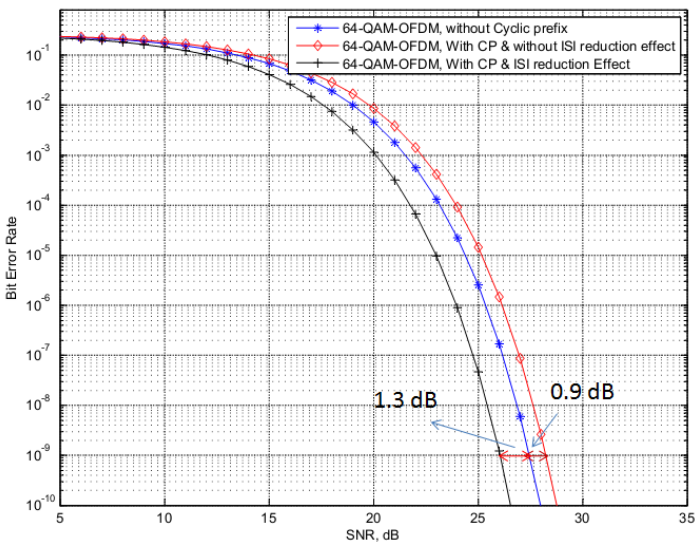


Figura 1.20- SNR vs BER (fonte: Wikipedia)

5. Redes de computadores

Uma **rede local** (**LAN**) é uma rede de computadores que liga computadores numa área limitada, como uma residência, escola, laboratório, campus universitário ou edifício de escritórios.

Ethernet e Wi-Fi são as duas tecnologias mais comuns usadas em redes locais.

1000BASE-T e **cabeamento estruturado** são a base da maioria das LANs comerciais atualmente. Embora o cabo de fibra ótica seja comum para ligações entre comutadores de rede, o uso de fibra em computadores de secretária é raro.

Numa **LAN sem fios**, os utilizadores têm movimento ilimitado dentro da área coberta. As redes sem fio tornaram-se populares em residências particulares e em pequenas empresas, devido à sua facilidade de instalação. A maioria das LANs sem fio utiliza Wi-Fi, pois é incorporada em smartphones, tablets e laptops. Os convidados têm normalmente acesso à Internet por meio de um serviço de hotspot.

As LANs simples consistem, normalmente, em cablamento e um ou mais comutadores. Um switch pode ser ligado a um router, a um modem por cabo, ou a um modem ADSL para acesso à Internet.

Uma LAN pode incluir uma grande variedade de outros dispositivos de rede, como **firewalls**, balanceadores de carga e sistemas de deteção de intrusão na rede. As LANs avançadas são caracterizadas pela utilização de links redundantes com switches, usando o protocolo spanning tree para evitar loops, a capacidade de gerir diferentes tipos de tráfego através da qualidade de serviço (QoS) e a capacidade de segregar tráfego com **VLANs**.

Nas camadas mais altas da rede, os protocolos como NetBEUI, IPX/SPX, AppleTalk e outros já foram comuns, mas o Internet Protocol Suite (**TCP/IP**) tem prevalecido como padrão de escolha atual.

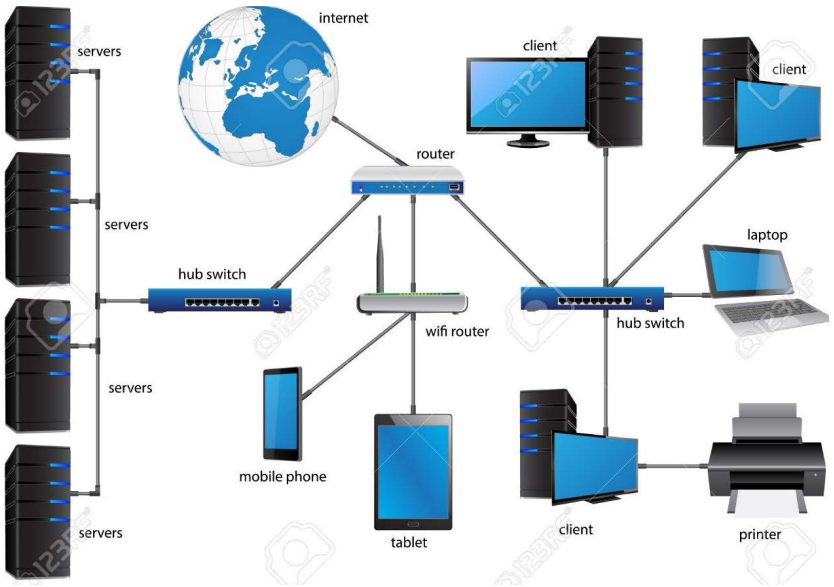


Figura 1.21- Estrutura da rede LAN (fonte: Wikimedia)

As redes LAN podem manter ligações com outras redes LAN por meio de linhas alugadas, serviços alugados ou pela Internet, usando as tecnologias de **rede virtual privada** (VPN). Dependendo de como as conexões são estabelecidas e protegidas, e da distância envolvida, essas redes LAN também podem ser classificadas como uma rede de área metropolitana (MAN) ou uma rede de área alargada (WAN).

Uma **rede de área ampla** (**WAN**) é uma rede de telecomunicações que se estende por uma grande distância geográfica para cumprir o principal

objetivo das redes de computadores. As redes de área ampla são frequentemente estabelecidas com circuitos de telecomunicações alugados.

Entidades comerciais, educacionais e governamentais usam redes de área ampla para retransmitir dados para funcionários, estudantes, clientes, compradores e fornecedores de vários locais do mundo. Em geral, este modo de telecomunicações permite que uma empresa efetivamente realize e cumpras as suas funções diárias, independentemente da localização. A Internet pode ser considerada uma WAN.

Muitas WANs são construídas para uma organização específica e são privadas, por exemplo, uma rede que ligue os diferentes escritórios de uma empresa à sua sede. Outras, criadas por fornecedores de serviços da Internet, fornecem ligações da LAN de uma organização para a Internet.

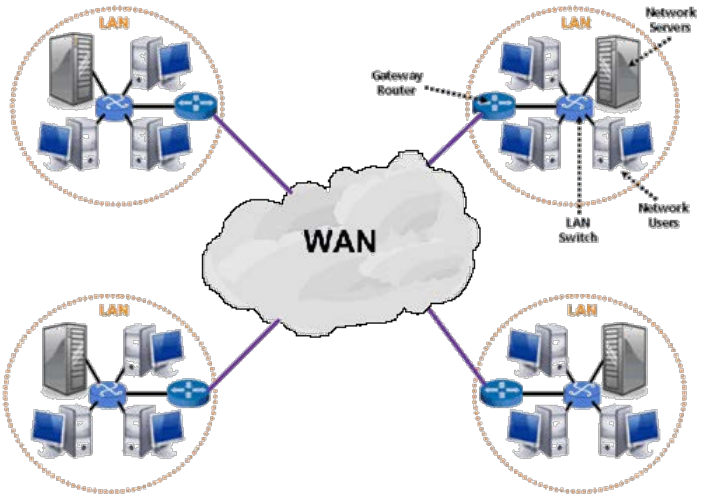


Figura 1.22- Rede WAN (fonte: Wikimedia)

Muitas tecnologias estão disponíveis para ligações WAN, como linhas telefónicas comutadas por circuito, transmissão de ondas de rádio e fibra óptica.

6. Protocolos de rede

O método padronizado pelo qual os nós têm permissão para transmitir informações ao bus ou à rede é denominado de **protocolo**. O protocolo define as regras, sintaxe, semântica e sincronização da comunicação e possíveis métodos de recuperação de erros. Os protocolos podem ser implementados por hardware, software ou por uma combinação de ambos.

Múltiplos protocolos geralmente descrevem diferentes aspectos de uma única comunicação. Um grupo de protocolos projetados para trabalhar juntos são conhecidos como um conjunto de protocolos.

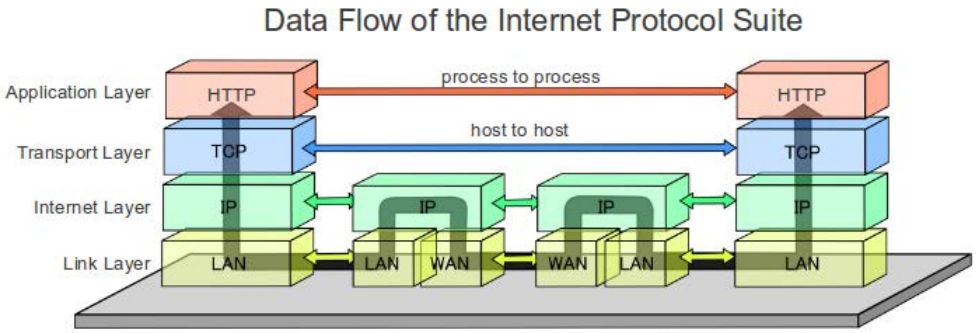


Figura 1.23- - Conjunto de protocolos TCP/IP (fonte: Wikimedia)

6.1. Padrões de série: RS232, RS485

Na transmissão de dados, a **comunicação em série**é o processo de envio de dados um bit de cada vez, sequencialmente, através de um canal de comunicação ou bus de computador. São muito comuns nas redes industriais devido à sua simplicidade, e o RS-232 e o RS-485 são alguns dos protocolos de comunicação em série mais difundidos. Estes protocolos correspondem à camada física do modelo OSI.

RS-232 refere-se a um padrão para transmissão de dados de comunicação em série. Define formalmente os sinais que se conectam entre um **DTE** (equipamento de terminal de dados), como um terminal de computador, e um **DCE**

(equipamento de terminação de circuito de dados ou equipamento de comunicação de dados), como um modem. Portanto, não pode ser considerado um protocolo de rede, mas um protocolo de comunicação ponto a ponto.

A norma define as características elétricas e o tempo dos sinais, o significado dos sinais e o tamanho físico e os pins de saída dos conectores. O padrão RS-232 tinha sido comumente usado nas **portas de série do computador**.

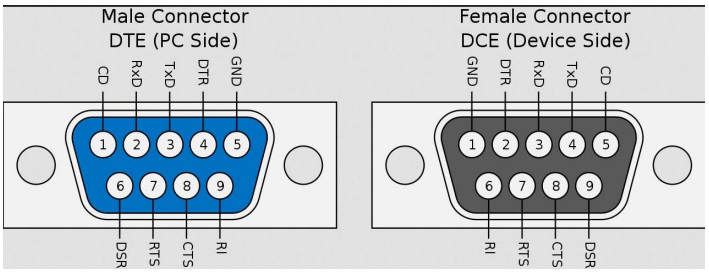


Figura 1.24- Layout dos pins de ligação RS-232 (fonte: Wikimedia)

O RS-232, quando comparado a interfaces posteriores, como o RS-485 e Ethernet, possui recursos mais baixos. Nos computadores pessoais modernos, o USB substituiu o RS-232 na maioria das suas funções de interface periférica. Mas, devido à sua simplicidade, as interfaces RS-232 ainda são utilizadas - principalmente em máquinas industriais, onde uma ligação de dados com fio de curto alcance, ponto a ponto e baixa velocidade é totalmente adequada.

RS-485 é um padrão que define as características elétricas de drivers e receptores para uso em sistemas de comunicação de série.

As redes de comunicações digitais que implementam o padrão podem ser usadas efetivamente em longas distâncias e em ambientes eletricamente ruidosos.

Vários receptores podem ser conectados a essa rede num bus linear multiponto. Essas características tornam o RS-485 útil em sistemas de controle industrial e aplicações similares.

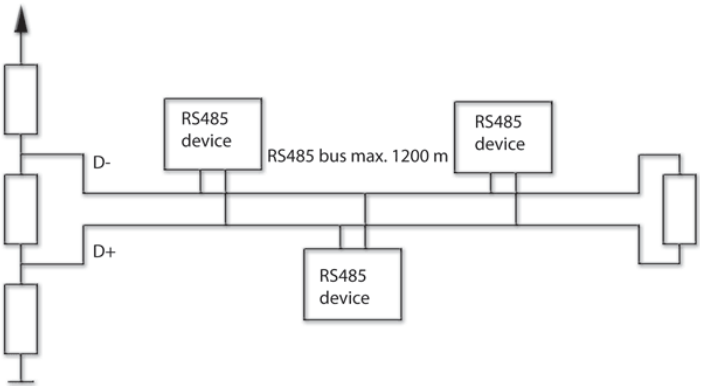


Figura 1.25- - Estrutura da rede RS-485 (fonte: Wikimedia)

Os computadores pessoais podem precisar de conversores de rede (geralmente RS232 para RS485 ou USB para RS485) para se ligarem a uma rede RS485.

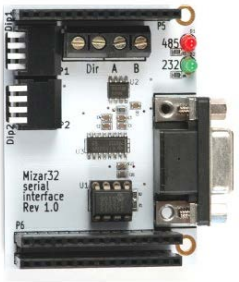


Figura 1.26- Conversor RS-485 / RS-232 (fonte: Wikimedia)

6.2. Ethernet

Ethernet é uma família de tecnologias de rede de computadores comumente usadas em redes de área local (LAN). As variantes Ethernet mais recentes usam par trançado (cabos UTP **e conectores RJ45**) e links de cabos de fibra óptica ou par trançado em conjunto com os comutadores (**switches**). Os padrões Ethernet compreendem várias variantes de fiação e sinalização da **camada física** OSI.

Figura 1.28- Cabo Ethernet (UTP+RJ45) (fonte: Wikimedia)

A topologia física mais comum para redes Ethernet é a topologia **estrela** baseada em comutadores.

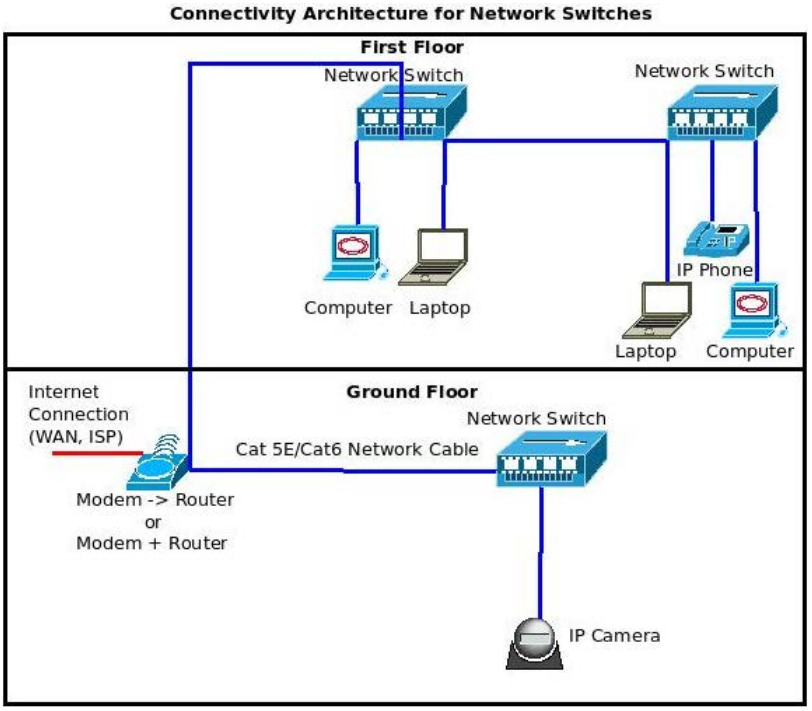


Figura 1.29- Rede Ethernet em topologia estrela (fonter: Wikipedia)

Os ICSs na indústria baseiam-se geralmente no protocolo Ethernet que facilita a partilha de informações entre dispositivos OT e estações de trabalho de IT. Switches industriais são usados para ligar equipamentos de OT, como PLCs, HMI e monitores (Figura 1.30).

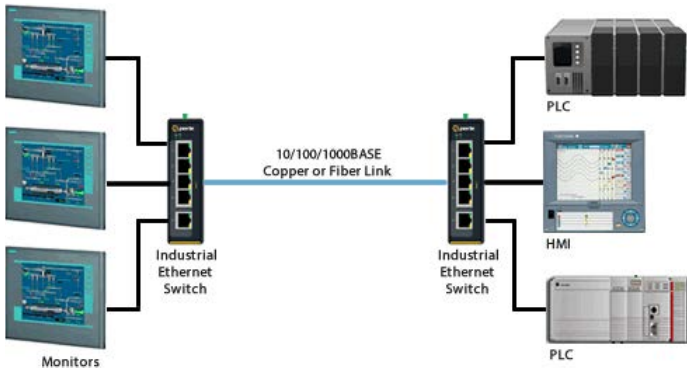


Figura 1.30 - - Estrutura de rede Ethernet industrial

Cada um dos nós (computadores, PLCs...) ligado a uma rede Ethernet precisa de uma placa especial (**Network Interface Controller**, NIC - Controlador de Interface de Rede) que fornece a interface física e o procedimento lógico (**CSMA/CD**) necessários para aceder e trocar informações através dessa rede.

Figura 1.31- Ethernet NIC (fonte: Wikipedia)

Os sistemas que se comunicam pela Ethernet dividem um fluxo de dados em partes mais curtas denominadas **enquadramento**. Cada enquadramento contém endereços de origem e de destino (**endereço MAC** de 48 bits) e dados de verificação de erros para que os enquadramentos danificados possam ser detectados e eliminados. De acordo com o modelo OSI, a Ethernet fornece serviços incluídos na camada de **dados de ligação**.

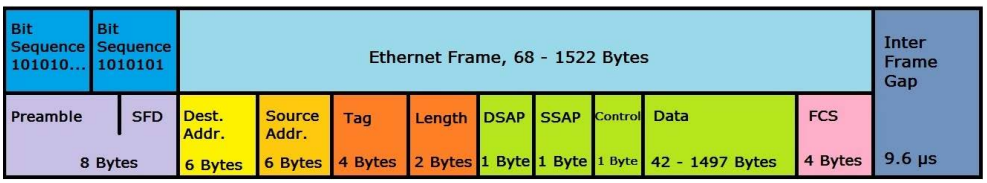


Figura 1.31- Frame Ethernet (fonte: Wikipedia)

O Protocolo da Internet (IP) é habitualmente transportado pela Ethernet e, portanto, é considerado uma das principais tecnologias que compõem a Internet.

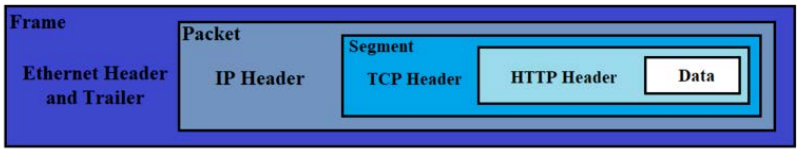


Figura 1.32- Pacote IP encapsulado no quadro Ethernet (fonte: Wikimedia)

6.3. TCP / IP

O **conjunto de protocolos da Internet** é o modelo concetual e o conjunto de protocolos de comunicação usados na Internet e em redes de computadores similares. É conhecido como **TCP/IP** porque os protocolos fundamentais no conjunto são o Protocolo de Controlo de Transmissão (TCP - Transmission Control Protocol) e o protocolo da Internet (IP). A Figura 1.33 compara o modelo OSI com a implementação do TCP/IP, na qual os protocolos da camada de aplicação (FTP...) utilizam os serviços de transporte fornecidos pelos protocolos TCP/IP.

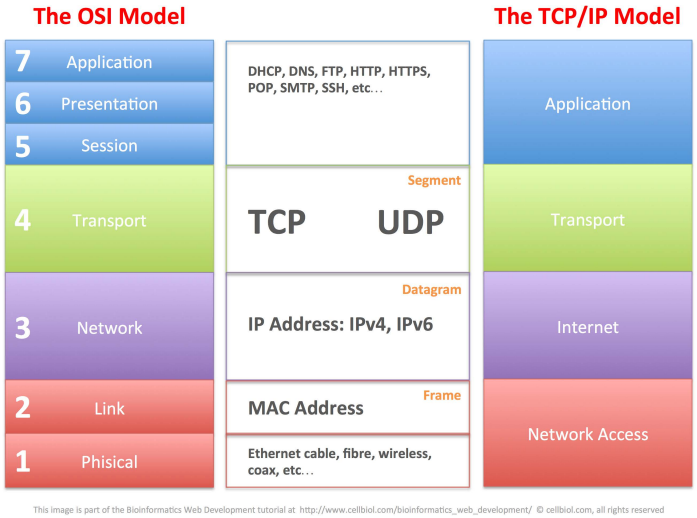


Figura 1.33- Pilha do protocolo de comunicação (fonte: blog.pythian.com)

O TCP/IP fornece comunicação de dados **de ponta a ponta**, especificando como os dados devem ser empacotados, endereçados, transmitidos, roteados e recebidos. Essa funcionalidade está organizada em **quatro camadas de abstração**. Do menor para o maior, as camadas são **a camada de ligação** (geralmente baseada em Ethernet), contendo métodos de comunicação para dados que permanecem num único segmento de rede (link); **a camada de internet** (baseada no protocolo IP), fornecendo internetworking entre redes independentes; **a camada de transporte** (com base no protocolo TCP), manipulando a comunicação host-a-host; e **a camada de aplicação** (protocolos como HTTP e FTP são definidos nessa camada), fornecendo troca de dados para aplicações processo-a-processo.

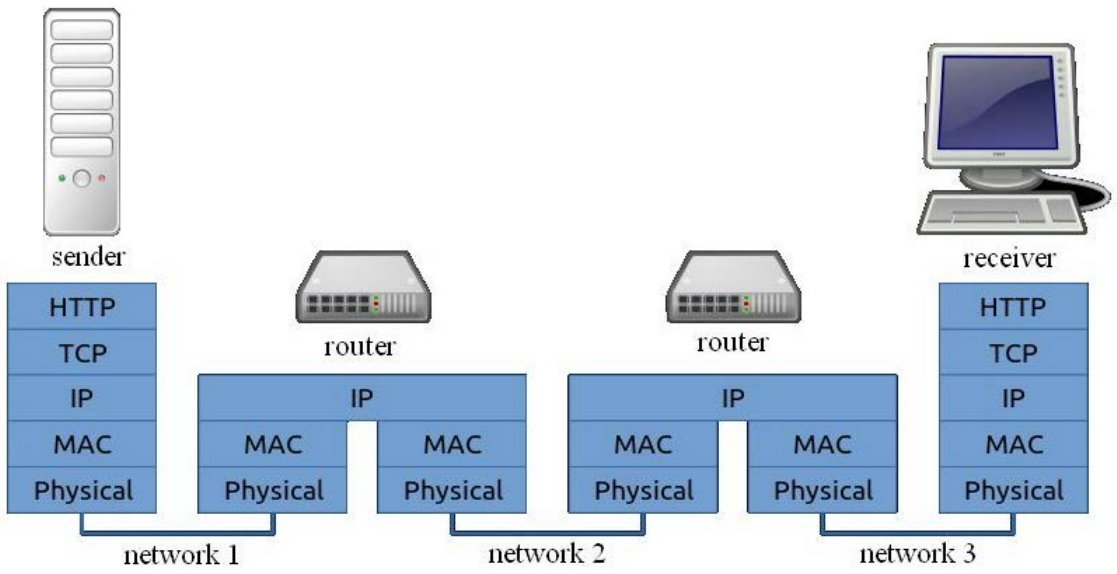


Figura 1.34- Estrutura de conexão TCP/IP (fonte: Wikimedia)

Um **router** é um dispositivo de rede que encaminha pacotes de dados entre redes de computadores. Os dados enviados pela Internet, como uma página da Web ou e-mail, encontram-se na forma de pacotes de dados. Um pacote de dados é normalmente encaminhado de um router para outro através das redes que constituem uma internetwork até atingirem o nó de destino.

Figura 1.35- Routing de pacotes IP (fonte: http://routinglab.blogspot.com)

O routing baseia-se em **endereços IP atribuídos aos nós**. Os endereços IP (v4) podem ser representados em qualquer notação que expresse um valor inteiro de 32 bits. São frequentemente escritos na notação decimal com pontos, que consiste em quatro octetos do endereço expressos individualmente em números decimais e separados por pontos.

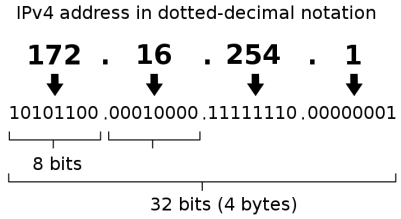


Figura 1.36- Estrutura de endereço IP (fonte: Wikimedia)

As informações são enviadas de um nó de transmissão para um receptor em forma de pacotes IP, incluindo os endereços IP de origem e destino.

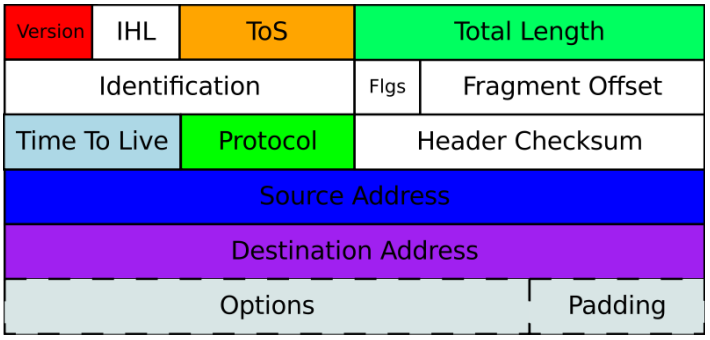


Figura 1.37- Estrutura de endereço IP (fonte: Wikimedia)

7. Segmentação de rede

Segmentação de rede em redes de computadores consiste no ato ou prática de dividir uma rede de computadores em sub-redes, como se representa na Figura 1.38, cada um constituindo um segmento de rede. As vantagens dessa divisão são principalmente aumentar o desempenho e melhorar a segurança.

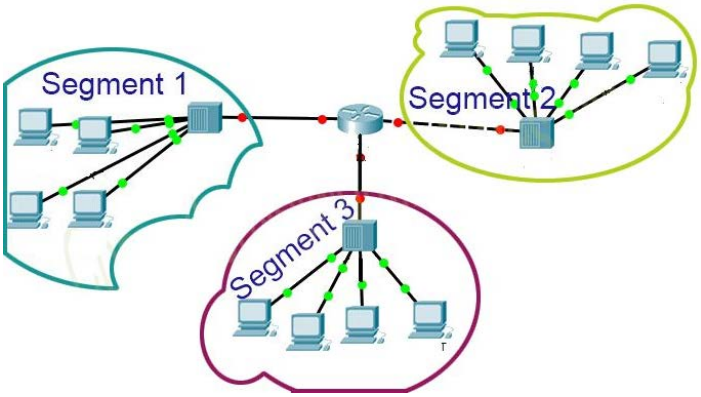


Figura 1.38- Segmentação de rede

Alcança-se **o desempenho melhorado**, porque numa rede segmentada há menos hosts por sub-rede, minimizando o tráfego local e reduzindo o congestionamento.

Segurança aprimorada é alcançada devido aos aspetos seguintes:

As transmissões são contidas na rede local. A estrutura de rede interna é visível do exterior.

Há uma superfície de ataque reduzida disponível. Os vetores de ataque comuns podem ser parcialmente aliviados pela segmentação de rede adequada, pois funcionam apenas na rede local. Ao criar segmentos de rede que contêm apenas os recursos específicos para os utilizadores a quem autoriza o acesso, está a criar um ambiente de menor privilégio.

O controlo de acesso de visitante alcança-se implementando VLANs para segregar a rede.

7.1. Switches e VLANs

Uma LAN virtual (**VLAN**) é qualquer domínio de broadcast particionado e isolado numa rede de computadores na camada de ligação de dados (camada OSI 2).

Para subdividir uma rede em VLANs, o equipamento de rede (normalmente switchers) deve ser configurado pelo software, atribuindo um grupo de portas a cada VLAN.

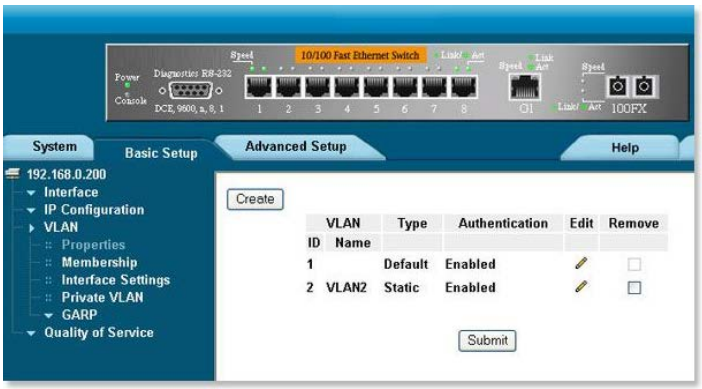


Figura 1.39- Ecrã de configuração da VLAN

Uma vez que as portas são atribuídas a cada VLAN, os dados não podem ser trocados entre nós (computadores, PLC...) ligados a diferentes portas VLAN.

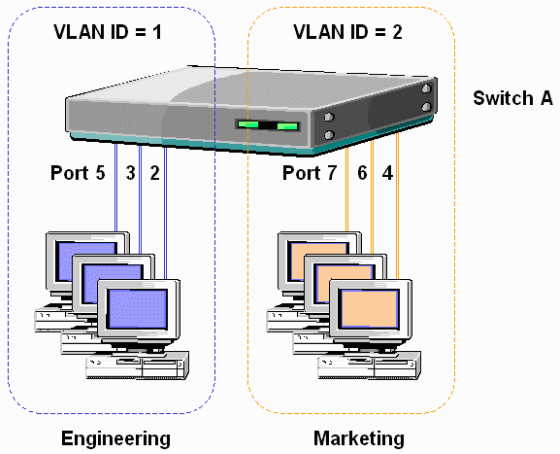


Figura 1.40- Segmentação de VLAN em umnum switch (fonte: http://photos1.blogger.com/blogger/6124/4181/320/vlan-fig1.png)

As VLANs funcionam aplicando as **tags**(esse método é desenvolvido sob o padrão 802.1Q) ao enquadramento da camada 2, criando a aparência e a funcionalidade do tráfego de rede que está fisicamente numa única rede, mas atua como se estivesse dividido entre redes separadas.

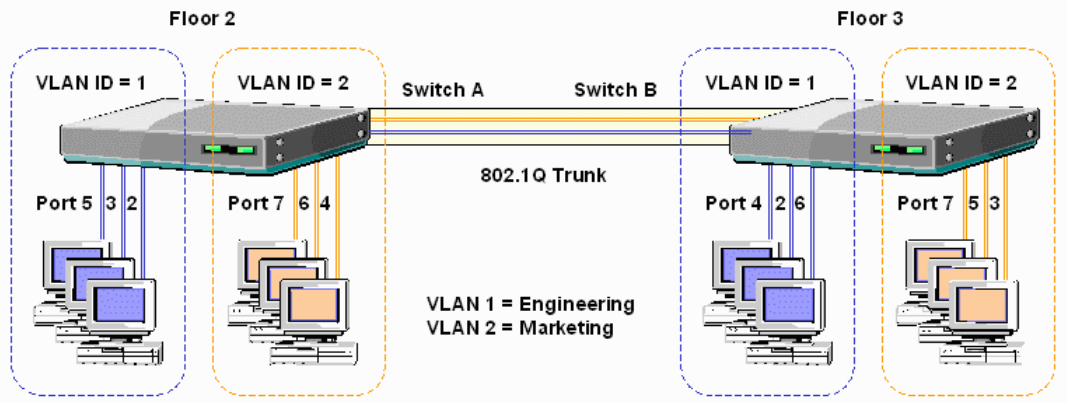


Figura 1.41- VLAN tagging (fonte: Wikimedia)

As VLANs permitem que os administradores de rede agrupem hosts, mesmo que os hosts não estejam diretamente ligados ao mesmo comutador de rede.

7.2. Routers e sub-redes

Em termos técnicos, um **router**é um dispositivo de gateway de rede da Camada 3, o que significa que entra em contacto com duas ou mais redes e que o router opera na camada de rede do modelo OSI. A Figura 1.42 mostra como três routers interconectam redes LAN diferentes (identificam-se pelos endereços de rede 150.10.0.0, 160.10.0.0 e 170.10.0.0).

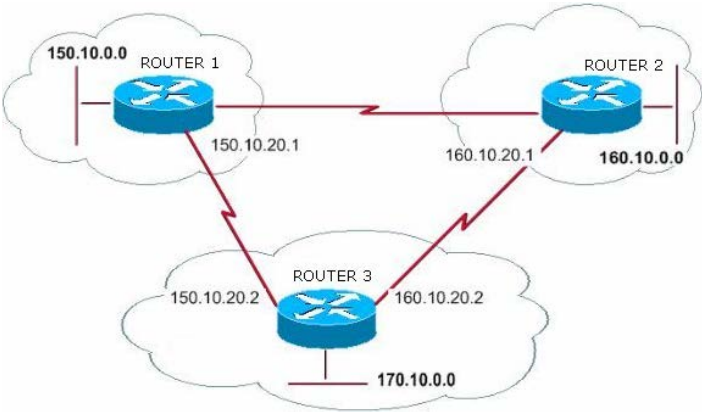


Figura 1.42- Router interligando diferentes redes LAN.

Para orientar as informações de uma origem para um nó de destino, é necessário um sistema de endereçamento, que geralmente está baseado nos endereços IPv4.

Um endereço IP é dividido em dois campos, **o identificador de rede** (usado pelos routers para encontrar a rede de destino na Internet) e **o identificador de host** (um identificador para um host específico) (Figura 1.43).

O número de bits dedicados a cada campo é definido pela **máscara** aplicada a um endereço IP, usando bits lógicos "1" para a parte da rede do endereço e "0" para a parte do host. O número de bits alocados à parte da rede é usado para a identificação do endereço IP da rede correspondente (por exemplo, no endereço de host 192.168.1.110/**24** , os primeiros 24 bits são alocados para o endereçamento de rede, portanto 192.168.1.0**/ 24** é o endereço IP da rede à qual o host pertence).

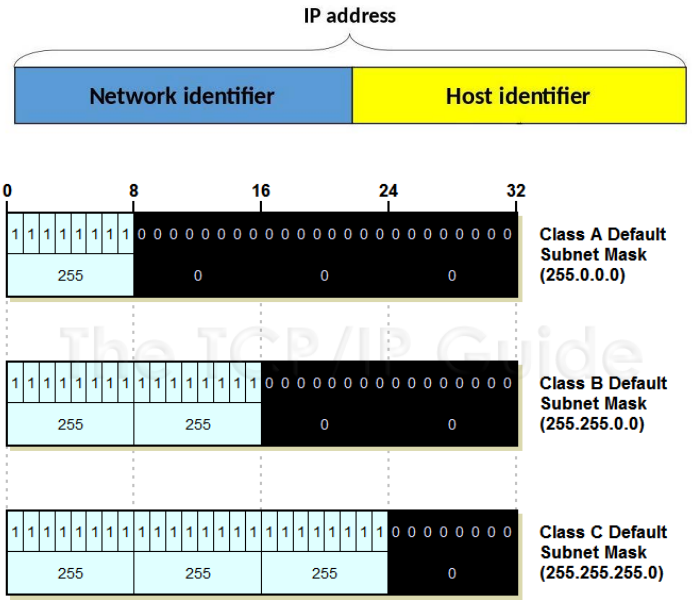


Figura 1.43- Classe de endereço IP vs máscara IP

Uma sub-rede é uma subdivisão lógica (Figura 1.44) de uma rede IP. A prática de dividir uma rede em duas ou mais redes denomina-se **sub-rede**.

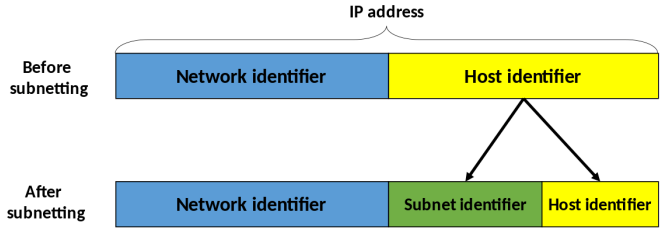


Figura 1.44- Identificador de sub-rede (fonte: Wikipedia)

Alguns bits do campo identificador do host são alocados (modificando a máscara de rede IP para adicionar mais bits "1" alocados ao campo de sub-rede) para criar um **identificador de sub-rede**. Os computadores que pertencem à mesma sub-rede são endereçados com um identificador de sub-rede idêntico em seus endereços IP.

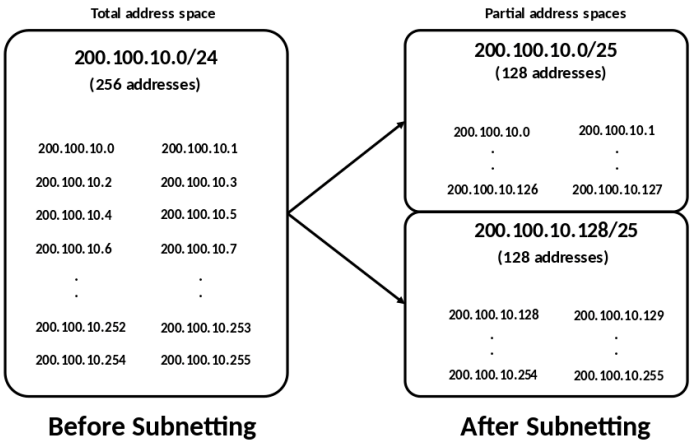


Figura 1.45- Segmentação de sub-redes IP (fonte: Wikimedia)

Os computadores localizados em sub-redes IP diferentes precisam de um router comunicar entre si; portanto, a sub-rede é um método válido para segmentar uma rede em partes isoladas.

7.3. Firewalls

Uma **firewall** é um sistema de segurança de rede que monitoriza e controla o tráfego de entrada e saída da rede com base em regras de segurança predeterminadas. Uma firewall normalmente estabelece uma barreira entre uma rede interna confiável e uma rede externa não confiável, como a Internet.

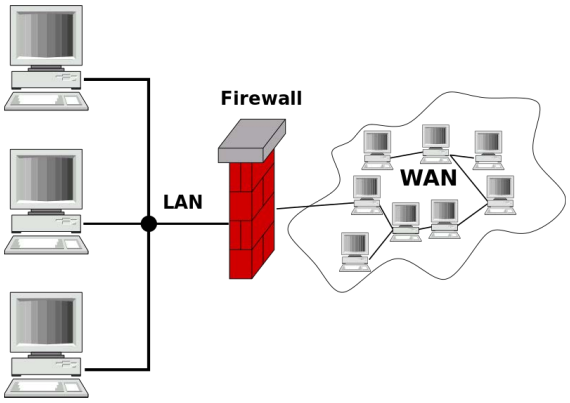


Figura 1.46- Proteção baseada em firewall (fonte: Wikipedia)

A firewall filtra pacotes transferidos entre computadores. Quando um pacote não corresponde às **regras de filtragem**, a firewall rejeita o pacote, caso contrário, pode passar. Os pacotes podem ser filtrados por endereços de rede de origem e destino, número de protocolo, fonte e porta de destino.

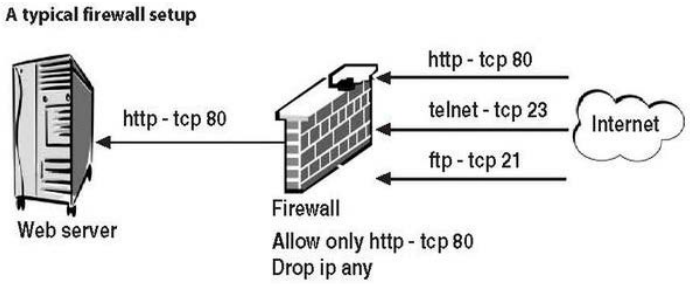


Figura 1.47- Regras de filtragem da firewall (fonte: Wikimedia)

DMZ ou **zona desmilitarizada** é uma sub-rede que contém os serviços externos de uma organização face a uma rede maior, como a Internet. O objetivo de uma DMZ é adicionar uma camada de segurança à LAN da organização: um nó de rede externo pode aceder apenas ao que está exposto na DMZ, enquanto o restante da rede da organização está com firewall.

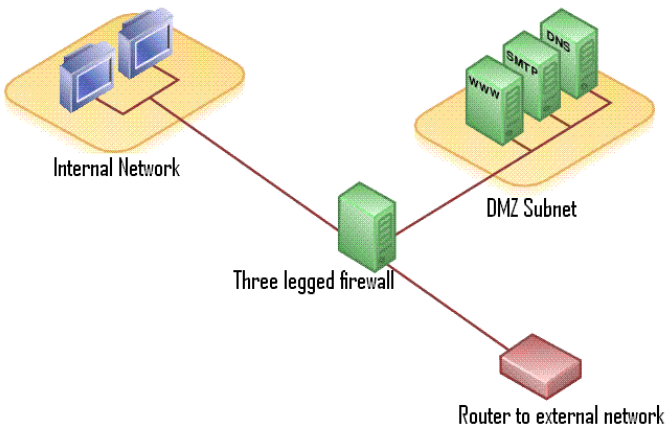


Figura 1.48- Firewall baseada em DMZ (fonte: Wikimedia)

8. Acesso remoto

Um **serviço de acesso remoto** (**RAS**) é qualquer combinação de hardware e software que permite uma ligação entre um cliente e um computador host, conhecido como servidor de acesso remoto.

Muitos fabricantes de help desk utilizam este serviço para **solucionar questões técnicas dos problemas dos seus clientes**. Existem várias aplicações de **desktop remotos** profissionais, de terceiros, de código aberto e de acesso livre.

8.1. Telnet e SSH

Telnet e SSH (Secure Shell) são dois protocolos de rede usados na ligação a **servidores remotos** para facilitar qualquer tipo de comunicação. Permitem que os administradores de rede acedam e façam a gestão remota de um dispositivo que trabalha com um emulador de terminal .

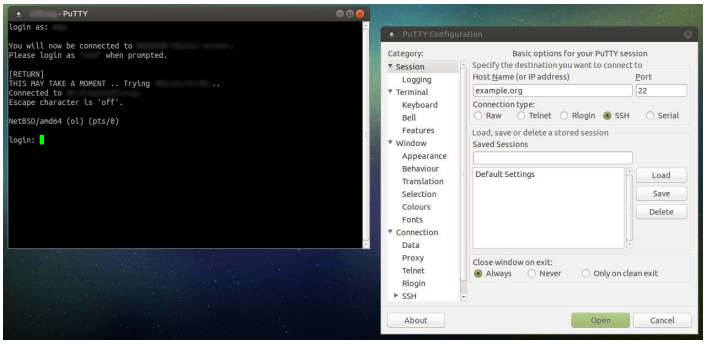


Figura 1.50- Terminal Remoto

A principal diferença entre o Telnet e o SSH consiste no facto de o SSH fornecer mecanismos de segurança (criptografa dados trocados usando a chave pública **criptografia**) que protegem os utilizadores que estabelecem uma ligação segura entre dois hosts remotos pela Internet, enquanto o Telnet não possui medidas de segurança, uma vez que os dados utilizador/senha são descodificados.

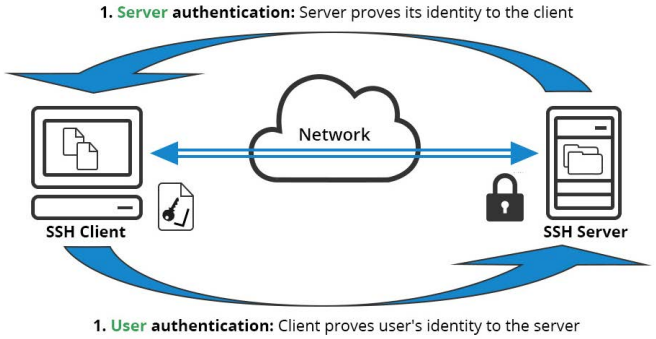


Figura 1.51- Ligação codificada baseada em SSH

8.2. Área de trabalho remota

Ambiente de trabalho remoto refere-se a um software que permite que o ambiente de área de trabalho de um computador pessoal seja executado remotamente num sistema enquanto é exibido num dispositivo cliente separado. A tomada remota de um ambiente de trabalho é uma forma de administração remota.

Figura 1.52- Remote desktop (fonte: http://www.itarian.com)

Remote Desktop Protocol (**RDP**) é um protocolo multi-canal desenvolvido pela Microsoft que permite que um utilizador se ligue a outro computador através de uma interface gráfica por meio de uma ligação de rede. O utilizador emprega o software cliente RDP (incluído em muitos sistemas operativos) para esse fim, enquanto o outro computador tem de executar o software do servidor RDP (incluído apenas no sistema operativo do Windows).

Atualmente, a Microsoft refere-se ao seu software cliente oficial RDP como Ligação Remota de Ambiente de Trabalho, anteriormente conhecida como "Cliente de Serviços de Terminal".

O RDP não atualizado é atualmente um dos principais pontos de entrada de **ransomware**. É muito importante manter o Windows atualizado para evitar este tipo de ataques. Existem algumas opções para o proteger. Siga a ligação para obter mais informações

O Virtual Network Computing (**VNC**) é um sistema de partilha de área de trabalho gráfica de código aberto que utiliza o protocolo RFB (Remote Frame Buffer) para controlar remotamente outro computador. Transmite através de uma rede as ações do teclado e do rato de um computador para outro, retransmitindo as atualizações do ecrã na outra direção.

Podem ligar-se a um servidor VNC multiplos clientes em simultâneo. As utilizações habituais desta tecnologia incluem o suporte técnico remoto e o acesso a arquivos ou documentos guardados no computador do trabalho a partir de um computador doméstico ou vice-versa.

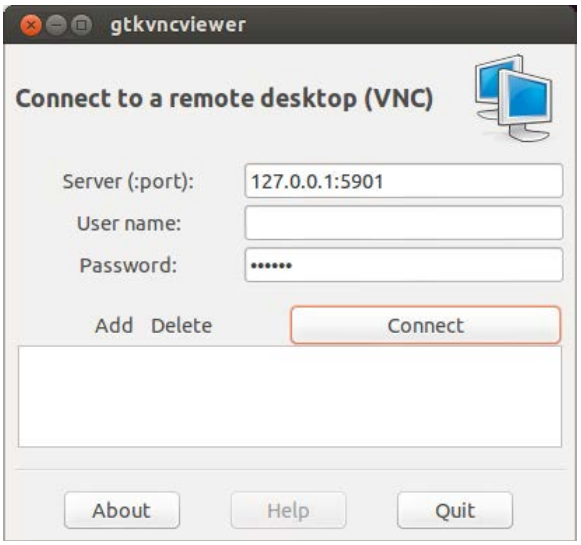


Figura 1.53- Login Remote desktop login (fonte: flickr VNC)

O TeamViewer é um software proprietário para controlo remoto, partilha de área de trabalho, reuniões online, conferências na web e transferência de ficheiros entre computadores. Uma vez instalado num computador, permite ligações remotas aos utilizadores com permissão.

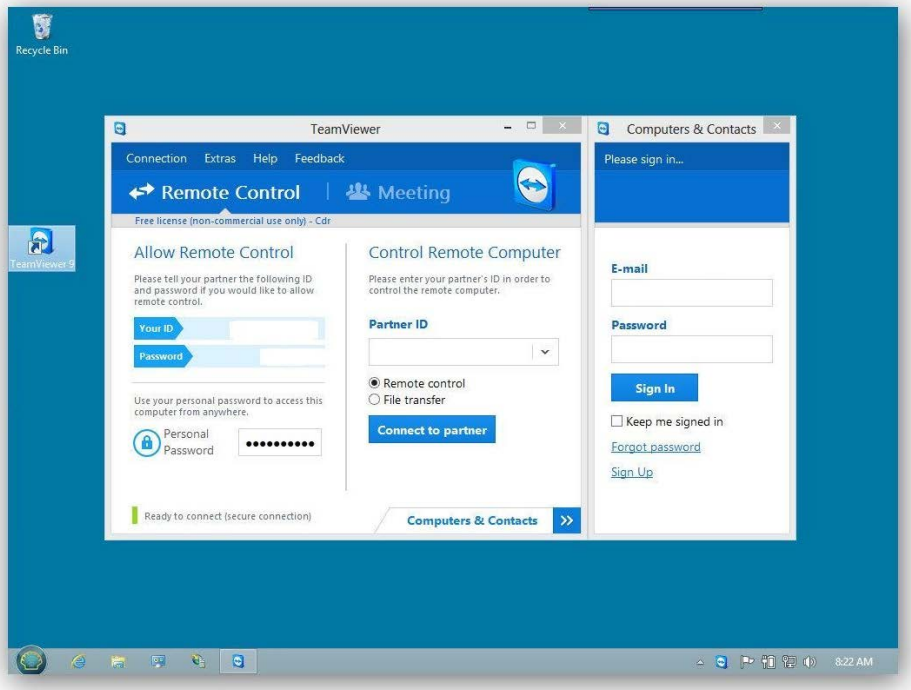


Figura 1.54- Configuração da ligação remota do Teamviewer

8.3. VPN

Uma **rede virtual privada** (**VPN**) estende uma rede privada através de uma rede pública e permite que os utilizadores enviem e recebam dados através de redes públicas ou partilhadas como se os seus dispositivos estivessem diretamente ligadas à rede privada.

Para garantir a segurança, a ligação de rede privada estabelece-se usando um protocolo codificado em camadas de **tunelamento** e os utilizadores da VPN usam métodos de autenticação, incluindo senhas ou certificados.

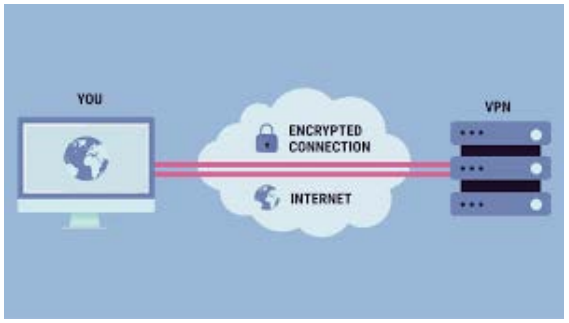


Figura 1.55- Conexão VPN (fonte: http://hardzone.es)

1.3 Protocolos de Redes Industriais

Description

Protocolos de Redes Industriais

Table of contents

1. Protolocos Fieldbus
1.1. ModBus
1.2. ProfiBus
1.3. Ethernet Industrial

2. Protocolo OPC

1. Protolocos Fieldbus

Fieldbus é o nome de uma família de protocolos de redes de computadores industriais utilizados para controlo distribuído em tempo real.

Num sistema de controlo industrial existe, geralmente, uma interface homem-máquina (HMI) no topo da hierarquia, vinculada a uma camada intermediária de controladores lógicos programáveis (PLC) por meio de um sistema de comunicações não críticas em termos de tempo (por exemplo, Ethernet). Na parte inferior do sistema de controlo está o fieldbus que liga os PLCs (Camada 1) aos componentes que realmente fazem o trabalho (Camada 0), como sensores, atuadores, motores elétricos, luzes da consola, interruptores, válvulas e contatores

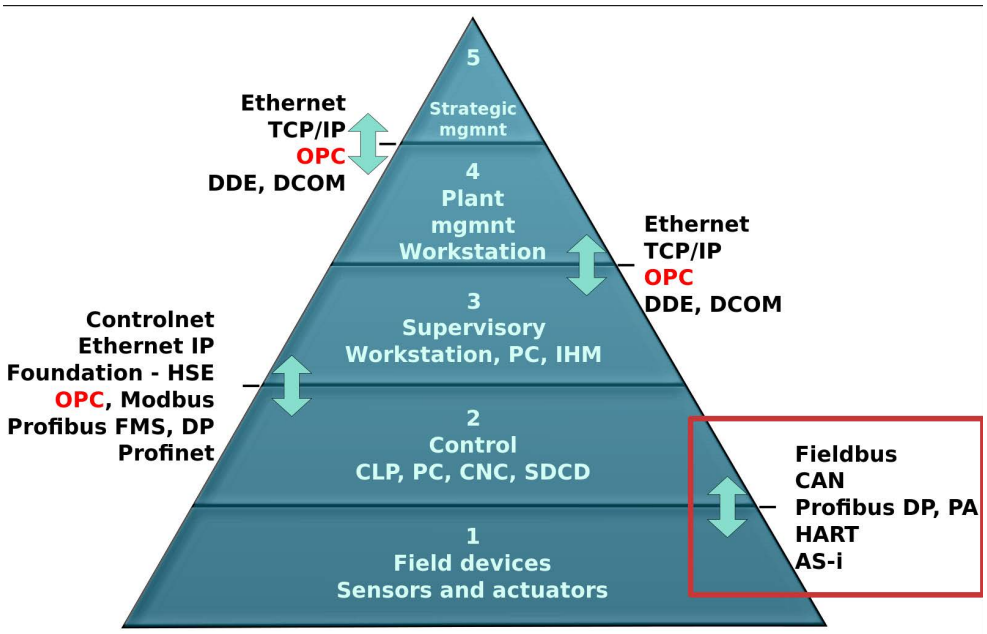


Figura 1.56- Esquema de nível de fieldbus (fonte: Wikimedia)

O Fieldbus é um sistema de rede industrial para controlo distribuído **em tempo real** , equivalente às ligações atuais do tipo LAN, que requerem apenas um ponto de comunicação no nível do controlador e permitem a ligação de vários dispositivos ao mesmo tempo.

1.1. ModBus

O Modbus é um protocolo de comunicação de série (geralmente implementado em RS-232 ou RS-485) utilizado para comunicar PLCs. Tornou-se um protocolo de comunicação padrão e agora é um meio comum de ligação de dispositivos eletrónicos industriais pelos aspetos que seguem:

publicado abertamente e isento de taxas,

move bits ou palavras em bruto sem impor muitas restrições aos fornecedores.

O Modbus é frequentemente utilizado para ligar um computador de supervisão (**mestre**) a uma RTU remota (**servo**) nos sistemas SCADA. Define-se como um protocolo mestre/servo (Figura 1.57), o que significa que um dispositivo que opera como mestre pesquisará um ou mais dispositivos que operam como servos. Isto significa que um dispositivo "servo" não pode oferecer informações voluntariamente; tem de esperar para ser solicitado. O mestre gravará dados nos registros de um dispositivo servo e lerá os dados dos registos de um dispositivo escravo.

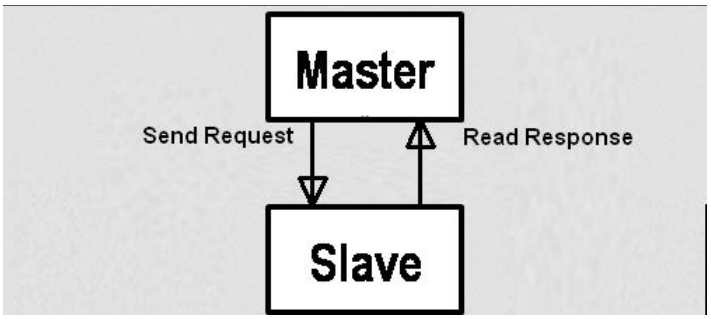


Figura 1.57- Processo de comunicação do Mestre/Escravo

Cada troca de dados consiste numa solicitação do mestre, seguida de uma resposta do servo. Como se mostra na Figura 1.58, cada pacote de dados, seja de solicitação ou de resposta, começa com o endereço do dispositivo ou endereço servo, seguido do código da função, seguido dos parâmetros que definem o que está a ser solicitado ou fornecido. Os formatos exatos da solicitação e resposta estão documentados em detalhe na especificação do protocolo Modbus.

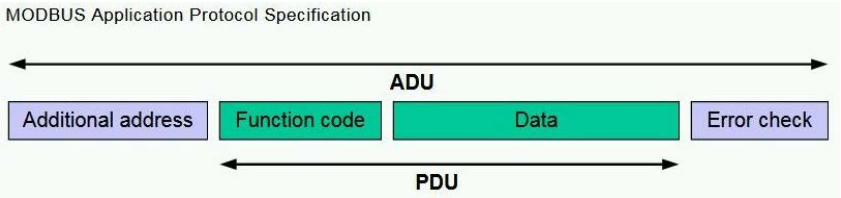


Figura 1.58- Estrutura do pacote de dados Modbus (fonte: Modbus Organization)

Como mostra a Figura 1.59, o protocolo **Modbus TCP** encapsula pacotes de dados de solicitação e de resposta Modbus RTU num pacote TCP transmitido através de redes Ethernet padrão. O endereço de maior importância aqui é o endereço IP. A porta padrão para o Modbus TCP é 502, mas o número da porta pode ser reatribuído.

A soma de verificação e o diagnóstico de erros são tratados pela Ethernet no caso do Modbus TCP.

A versão TCP do Modbus segue o modelo de referência de rede OSI. O Modbus TCP define as camadas de apresentação e de aplicação no modelo OSI.

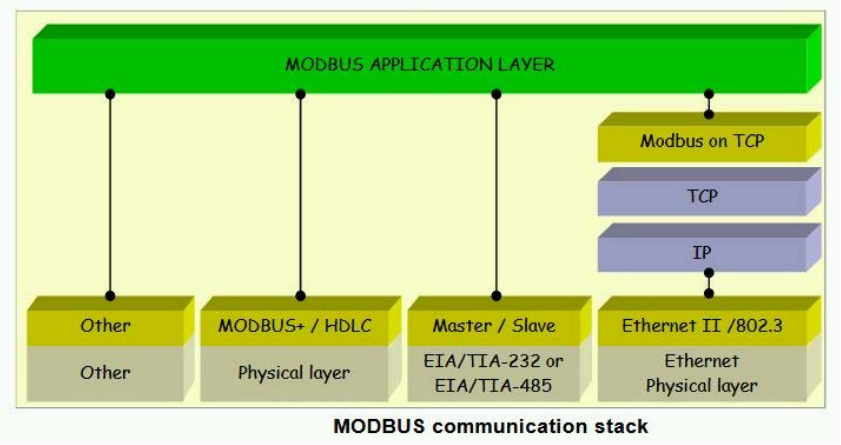


Figura 1.59- Pilha de protocolos Modbus (fonte: Modbus Organization)

O Modbus TCP é executado na Ethernet (ligação de dados e camada física) e o Modbus RTU é um protocolo de nível em série (camada física). Para comunicar ambas as redes, é necessário um **gateway** (Figura 1.60) para converter um protocolo no outro, adicionando ou removendo um cabeçalho de 6 bytes que permita o encaminhamento no Modbus TCP.

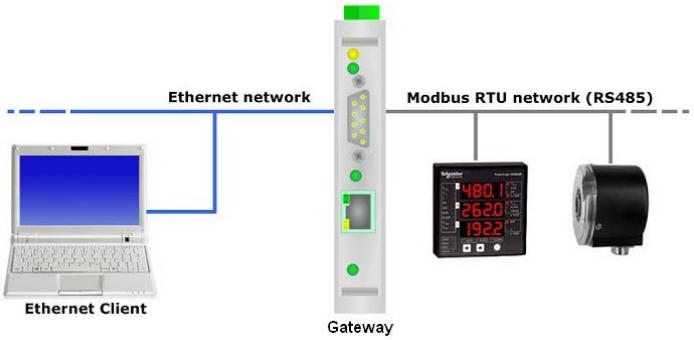


Figura 1.60- Gateway de comunicação TCP-RTU

O Modbus TCP é o protocolo comum que liga as restantes opções do Modbus através de gateways.

1.2. ProfiBus

Profibus (Process Field Bus) é um padrão para comunicação de fieldbus em tecnologia de automação. Não deve ser confundido com o padrão Profinet para Ethernet industrial.

Existem duas variações do Profibus em uso atualmente (Figura 1.62); o mais utilizado é o Profibus DP:

- **PROFIBUS DP** (Periféricos Descentralizados) é utilizado para comandar sensores e atuadores através de um controlador centralizado num sistema de produção automatizado.

- **O PROFIBUS PA** (Automação de Processos) é usado para monitorizar equipamentos de medição em aplicações de automação de processos. Esta variante foi projetada para uso em áreas de explosão/risco (Zona Ex0 e 1). A camada física está em conformidade com a IEC 61158-2 que permite que a energia seja fornecida pelo bus aos instrumentos de campo, limitando os fluxos de corrente para que não sejam criadas condições explosivas, mesmo que ocorra uma anomalia.

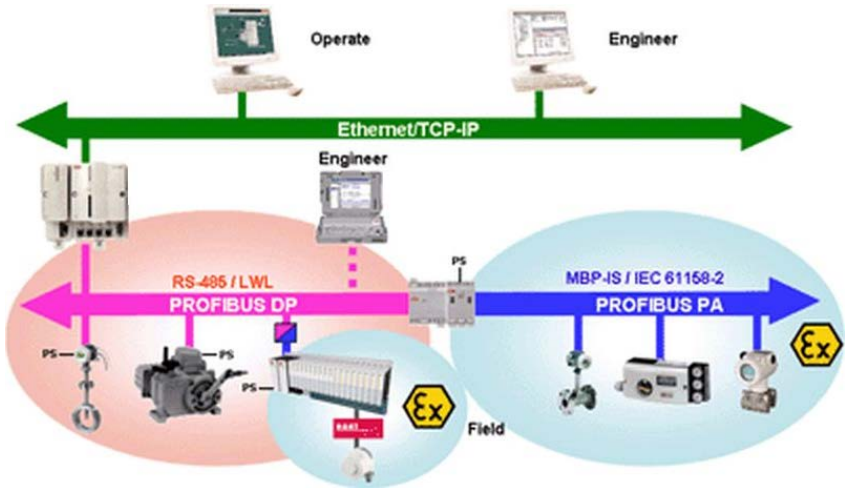


Figura 1.62- Profibus DP/PA

O Profibus é desenvolvido nas Camadas OSI 1,2 e 7 (Figura 1.63):

	OSI-Layer	PROFIBUS		
7	Application	DPV0	DPV1	DPV2
6	Presentation	--		
5	Session			
4	Transport			
3	Network			
2	Data Link	FDL		
1	Physical	EIA-485	Optical	MBP

Figura 1.63- Comparação dos níveis do modelo OSI-Profibus

Camada 1:

São especificados três métodos diferentes para a camada de transmissão de bits:

- Com transmissão elétrica conforme EIA-485. Podem ser usadas taxas de bits de 9,6 kbit/s a 12 Mbit/s. O comprimento do cabo entre dois repetidores é limitado de 100 a 1200 m, dependendo da taxa de bits utilizada. Este método de transmissão é usado principalmente com o PROFIBUS DP.

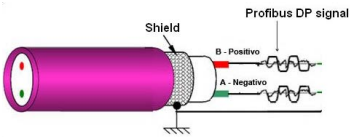


Figura 1.64- Cabo Profibus RS-485

- Na transmissão ótica via fibra ótica, são usadas topologias em estrela, bus e anel. A distância entre os repetidores pode ser de até 15 km. São necessários conversores de fibra ótica RS485 (Figura 1.65).

Figura 1.65- Conversor Optic fiber-RS485

- Com a tecnologia de transmissão MBP (Manchester Bus Powered), a alimentação de dados e de field é alimentada pelo mesmo cabo. Esta tecnologia é usada no Profibus PA.

Nas redes Profibus são geralmente utilizados conectores do tipo Sub-D de 9 pins.

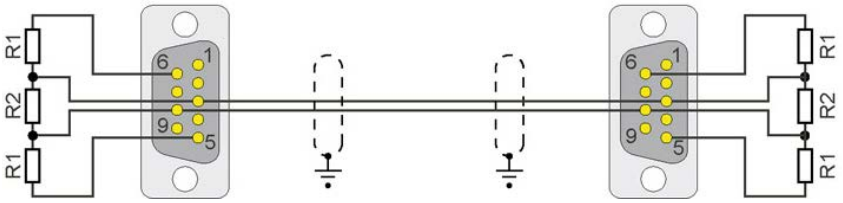


Figura 1.67- Conetor Profibus RS485 9 pin tipo D (source: Wikimedia)

Camada 2:

A camada de link de dados denomina-se **FDL** (Ligação de Dados do Fieldbus) e funciona com um método de acesso híbrido que combina a passagem de token com um método mestre-servo. Numa rede PROFIBUS DP, os controladores ou sistemas de controle de processo são os mestres e os sensores e atuadores são os **servos**. (Figura 1.68)

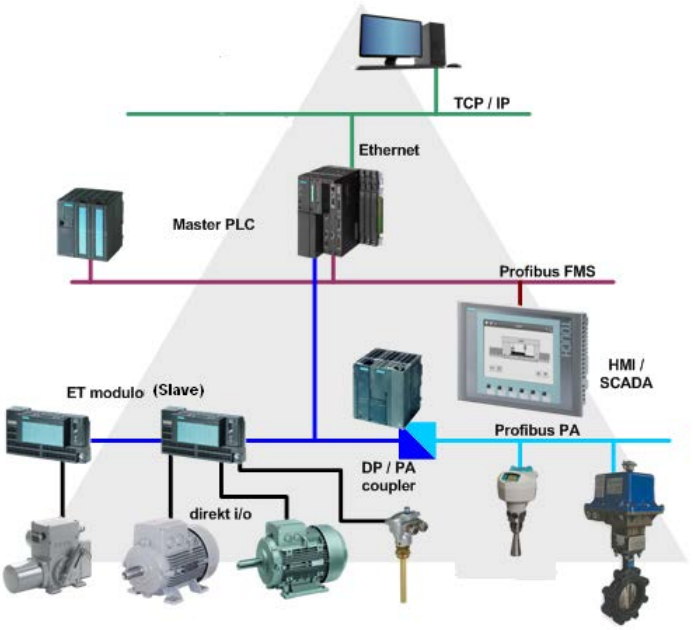


Figura 1.68- Arquitectura master-slave Profibus (source: Wikimedia)

O Profibus pode ser ligado a outras redes de barramento de campo usando o gateway necessário (Figura 1.69).

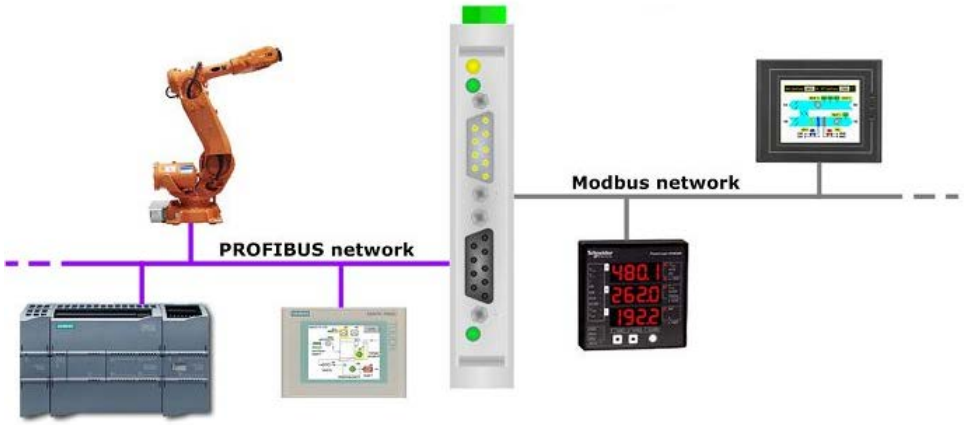


Figura 1.69- Interligação Profibus e Modbus via gateway

1.3. Ethernet Industrial

Ethernet Industrial utiliza os padrões desenvolvidos para Ethernet e implementa-os na produção de comunicações em rede (Figura 1.70). Modificando a camada de ligação de dados (Controle de acesso ao média), a Ethernet Industrial fornece **determinação** e o controlo em **tempo real** (baixa latência), que não é essencial para o trabalho em tecnologia da informação, mas é necessário em Tecnologia Operacional (automação industrial).

Além disso, tem de fornecer **interoperabilidade** de níveis mais altos do modelo OSI e **segurança** contra invasões externas à fábrica assim como contra utilizações não autorizadas dentro da fábrica.

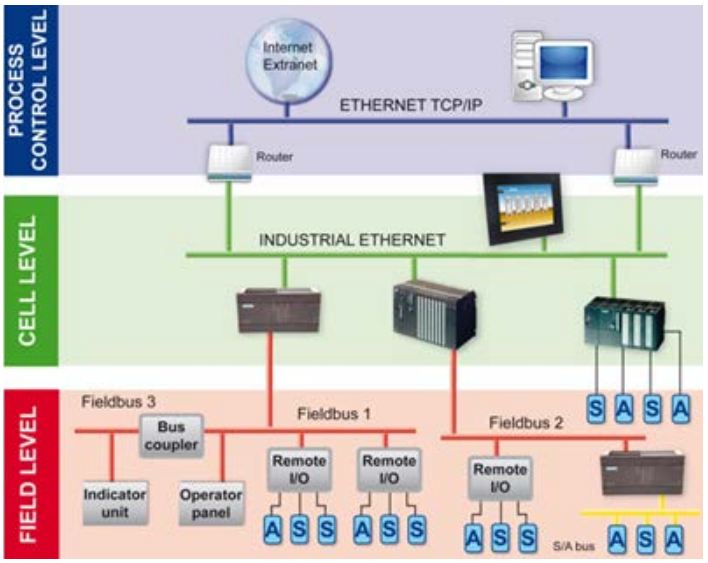


Figura 1.70 IArquitetura de rede Ethernet Industrial (fonte: Industrial Ethernet Book)

Os equipamentos Ethernet industriais foram projetados para **ambientes hostis** e precisam de recursos especiais, como conectores reforçados e interruptores de temperatura estendidos, necessários num ambiente industrial. Os componentes utilizados nas áreas de processamento da fábrica devem ser projetados para trabalhar com temperaturas extremas, com humidade e vibração que excedam as médias dos equipamentos de IT.

O uso de Ethernet de fibra ótica (portas **SFP**) reduz os problemas de ruído e fornece isolamento elétrico

Figura 1.71- Switch Ethernet industrial (fonte: Wikipedia)

Profinet consiste no padrão Ethernet Industrial aberto da Associação Internacional Profibus, sendo um dos padrões de comunicação utilizados com mais frequência em redes de automação.

O Profinet permite compatibilidade com as comunicações Ethernet (mais típicas dos ambientes de IT), mas deve considerar-se a diferença de velocidade que uma comunicação Ethernet possui numa rede corporativa em relação ao desempenho em tempo real exigido por uma rede industrial.

O uso do Profinet pode aportar as seguintes vantagens: Melhora a escalabilidade em infraestruturas.

Facilita o acesso a dispositivos de campo de outras redes.

Permite a execução de tarefas de manutenção de qualquer lugar através de ligações seguras (VPN) para manutenção remota.

O protocolo PROFINET consiste basicamente em três dispositivos (Figura 1.72).

Controlador IO: Mestre, onde o programa de controlo é executado

Aparelho IO: Dispositivo de campo remoto que mantém comunicação com um controlador

Supervisor IO: dispositivo gráfico programável no qual a análise de rede é feita.

Não existe nenhum tipo de hierarquia entre estes dispositivos, o que significa que cada IO tem a mesma importância numa rede PROFINET.

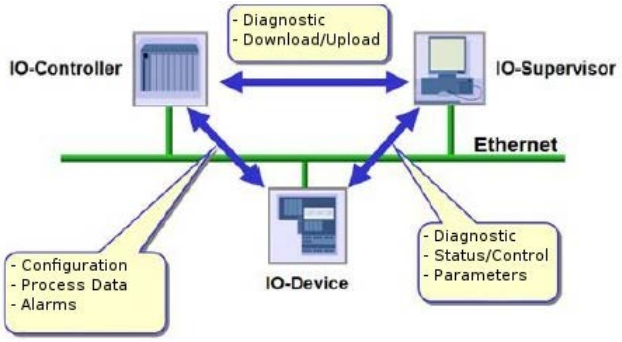


Figura 1.72- Tipos de dispositivos Profinet (fonte: www.semanticscholar.org)

O Profinet incorpora diferentes perfis através de uma interpretação específica dos dados transmitidos para cada caso, modificando o nível OSI 7 (aplicação). Existem 3 versões Profinet:

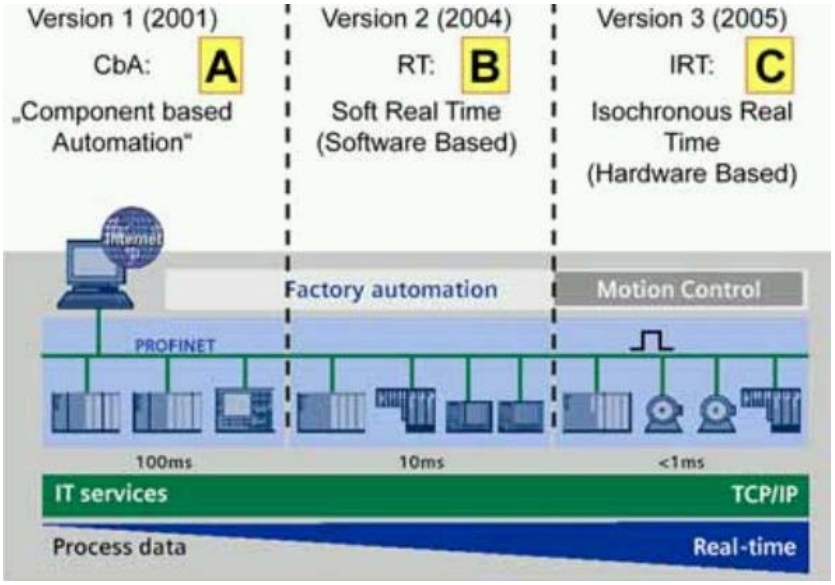


Figura 1.73- Perfis Profinet (fonte: www.semanticscholar.org)

- Versão 1 (Classe A): **Automação Baseada em Componentes (CBA)**

O seu tempo de ciclo típico é de 100ms e é utilizado para parametrização, não para comunicação de dados de processamento. Já não é suportado pelo Profibus.

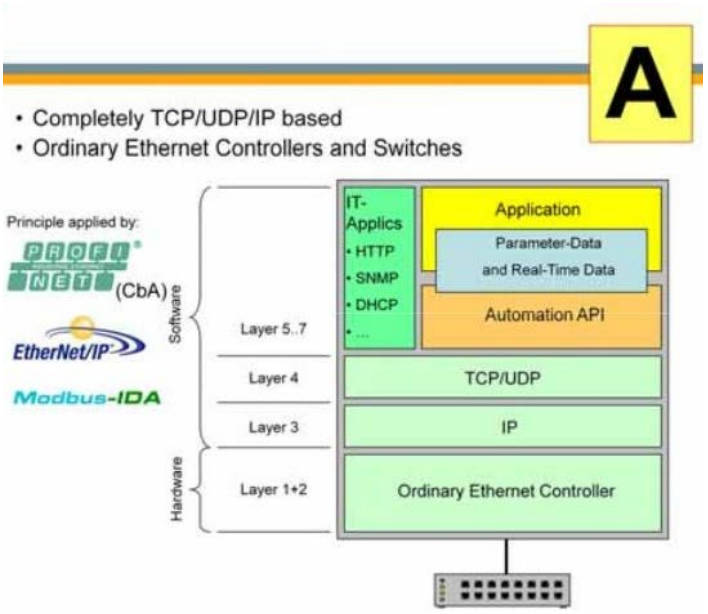


Figura 1.74- Arquitetura Profinet CBA (fonte: www.ethercat.org)

- Versão 2 (Classe B): **Tempo Real (RT)**

O seu tempo de ciclo típico é de 10ms, semelhante ao Profibus, e é utilizado para comunicação de dados de processamento.

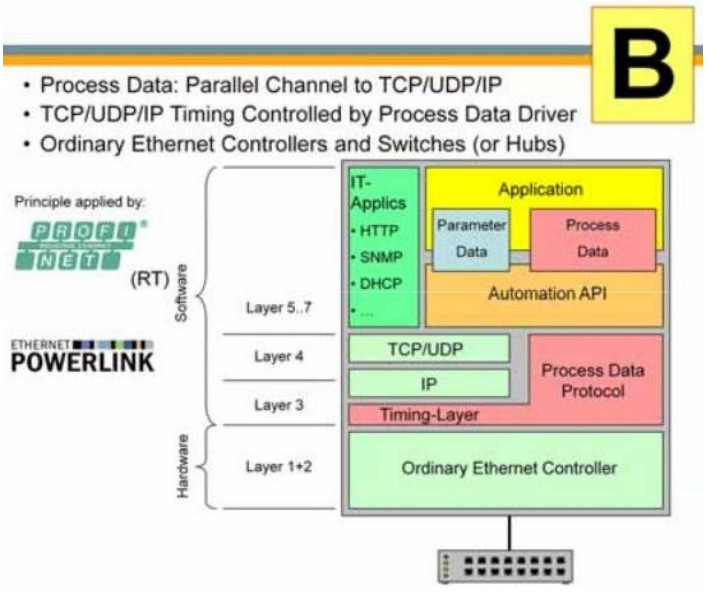


Figura 1.75- Arquitetura Profinet RT (fonte: www.ethercat.org)

- Versão 3 (Classe C): **Tempo Real Isócrono (IRT)**

O seu tempo de ciclo típico é de 1ms. A diferença em relação à comunicação em tempo real é essencialmente o elevado grau de determinismo, para que o início de um ciclo de rede seja mantido com alta precisão.

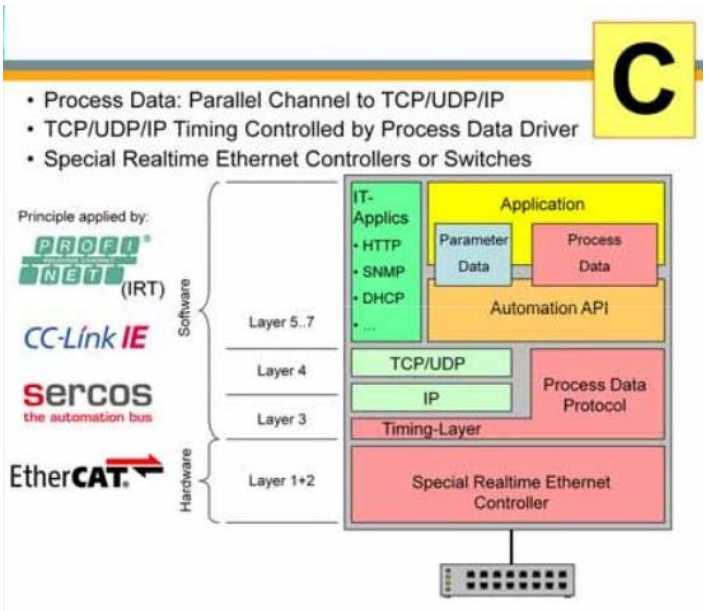


Figura 1.76- Arquitetura Profinet IRT (fonte: www.ethercat.org)

2. Protocolo OPC

OPC (Open Platform Communications) é o padrão de interoperabilidade para a troca segura e confiável de dados na automação industrial. É independente da plataforma e garante o fluxo contínuo de informações entre dispositivos de vários fornecedores.

Essas especificações definem a interface entre **clientes e servidores**, bem como servidores e servidores, incluindo acesso a dados em tempo real, monitorização de alarmes e eventos, acesso a dados históricos e outras aplicações.

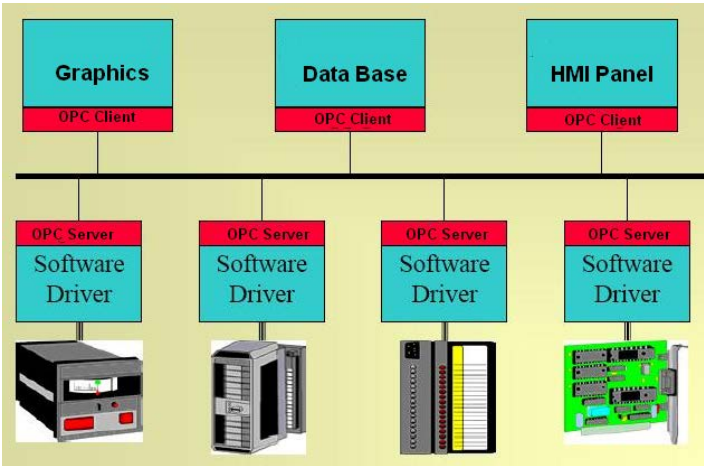


Figura 1.77- Arquitetura OPC server/client (fonte: Wikipedia)

O OPC foi projetado para fornecer uma ponte comum para aplicações de software e hardware de controlo de processos para aceder a dados de campo de dispositivos a partir do piso da fábrica (Figura 1.78).

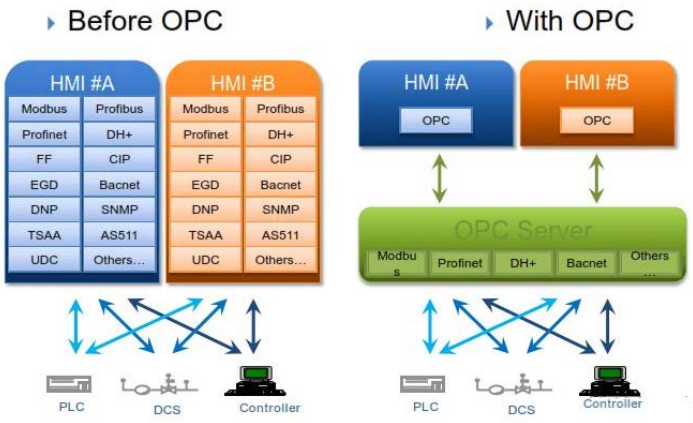


Figura 1.78- Arquitetura OPC (fonte: www.theautomization.com)

Um servidor OPC para um dispositivo de hardware fornece os mesmos métodos para um Cliente OPC aceder aos seus dados. Assim que um fabricante de hardware desenvolve o seu **Servidor OPC** para o novo dispositivo de hardware, o seu trabalho vai permitir que qualquer "superior" aceda ao seu dispositivo, e assim que o produtor SCADA desenvolve o seu **Cliente OPC**, o seu trabalho vai permitir o acesso a qualquer hardware com um servidor compatível com OPC.

A **Arquitetura OPC Unificada (UA)** é uma arquitetura orientada a serviços, independente da plataforma que integra toda a funcionalidade das especificações individuais do OPC Clássico, numa estrutura extensível única.

Tecnologias e metodologias inovadoras, como novos protocolos de transporte, algoritmos de segurança, padrões de codificação ou serviços de aplicações, podem ser incorporadas na OPC UA, mantendo a compatibilidade com versões anteriores.

Tarefa 1. Configurações do computador

Nesta primeira tarefa, vai aprender como configurar a rede do seu computador.

Abra uma janela da interface de comando (Iniciar> comando). A seguinte janela será aberta:

Lembre-se de como a abrir, pois pode precisar de repetir o procedimento posteriormente.

Digite “ipconfig” (sem as aspas) e pressione o botão Enter. O comando retornará os dados de configuração de rede do seu computador. Preencha a tabela que se segue com a resposta:

Endereço IP	
Máscara de sub-rede	
Gateway padrão (router)	

Digite "ipconfig /?" para ver as opções de comando.

Digite “ipconfig / all” e será devolvida a informação de configurações avançadas. Esta informação também pode ser vista iniciando o winipcfg (Início / launch / winipcfg). Preencha a tabela.

Configurações de IP do Windows	
Nome do host	
Sufixo DNS principal	
Router ativado	
Adaptador Ethernet	
Endereço físico	
DHCP ativado	

Preencha a tabela com os dados referentes aos seus colegas que se encontram do lado esquerdo e aos que se encontram do lado direito (se for o último da fila, pergunte a outro colega). Compare valores semelhantes e diferentes.

Colega à esquerda

Configurações de IP do Windows	
Nome do host	
Sufixo DNS principal	
Router ativado	
Adaptador Ethernet	
Endereço físico	
DHCP ativado	
Endereço IP	
Máscara de sub-rede	
Gateway padrão (router)	
Servidor DNS	

Colega à direita

Configurações de IP do Windows	
Nome do host	
Sufixo DNS principal	
Router ativado	
Adaptador Ethernet	
Endereço físico	
DHCP ativado	
Endereço IP	
Máscara de sub-rede	
Gateway padrão (router)	
Servidor DNS	

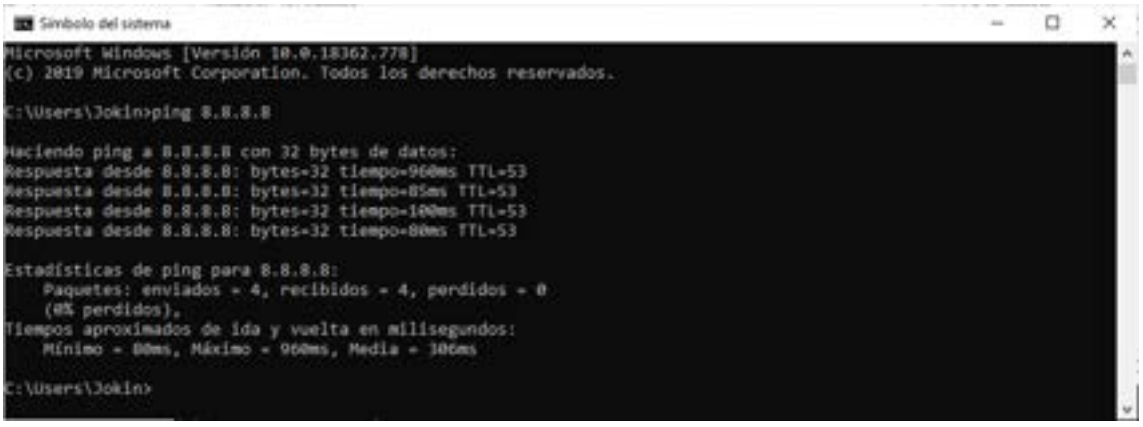
Tarefa 2. Endereço IP

Na Internet, os computadores são identificados pelo endereço IP (Protocolo da Internet). O IP é composto por 4 números, separados por 3 pontos. Cada um dos 4 números tem um valor entre 0 e 255 (ou seja, 192.168.2.3 ou 158.42.4.2).

Existe também outro tipo de identificação, usando nomes de domínio (por exemplo, www.google.com). Devido a um protocolo denominado DNS, o computador sabe qual é o endereço IP que corresponde a esse nome, nesse caso, o endereço IP 216.58.201.164.

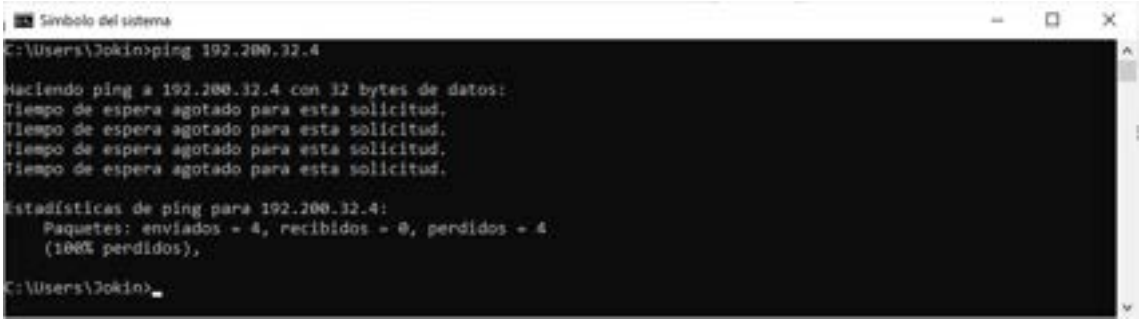
Abra uma janela da interface de comando (Iniciar> comando). A seguinte janela será aberta:

Inicie o comando “ping 8.8.8.8” e veja se o resultado é semelhante a este:

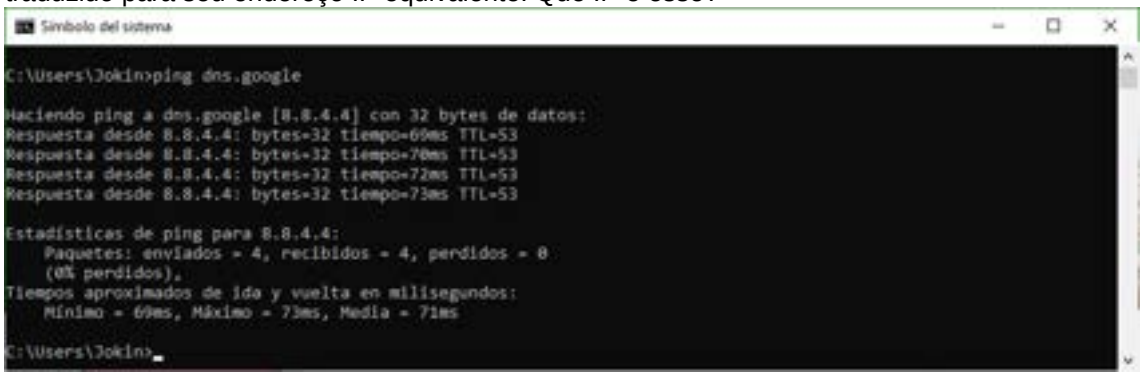


O parâmetro de resposta "Tempo" mostra a quantidade de tempo (geralmente milissegundos) de que um pacote ICMP precisa (isso corresponde ao comando *ping*) para alcançar o destino (nesse caso, o computador com o endereço IP 8.8.8.8) e retornar ao remetente (nosso computador).

Se não houver ligação entre o remetente e o destino, a mensagem de erro será semelhante a esta:



Veja o que acontece ao iniciar o comando "ping dns.google". *O DNS* do Google deve ser traduzido para seu endereço IP equivalente. Que IP é esse?



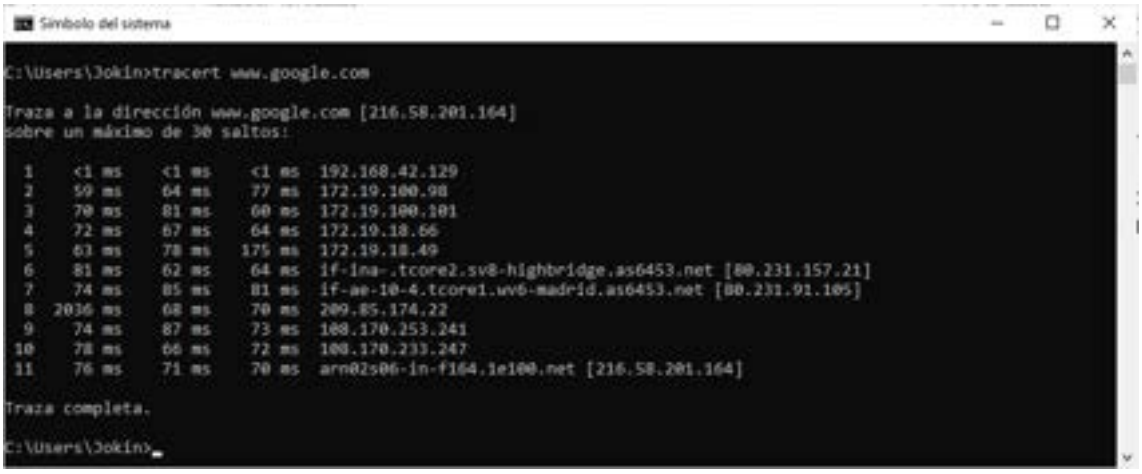
Agora inicie "ping www.google.com ". Qual é o IP?

Tarefa 3. Comando Tracert

A Internet é composta por muitas redes, ligadas entre si por dispositivos de comunicação denominados routers. Quando as informações são enviadas pela Internet, os dados passam por todos os roteadores até chegar ao destino. Sempre que uma rede é alterada através de um router, dizemos que os dados saltaram.

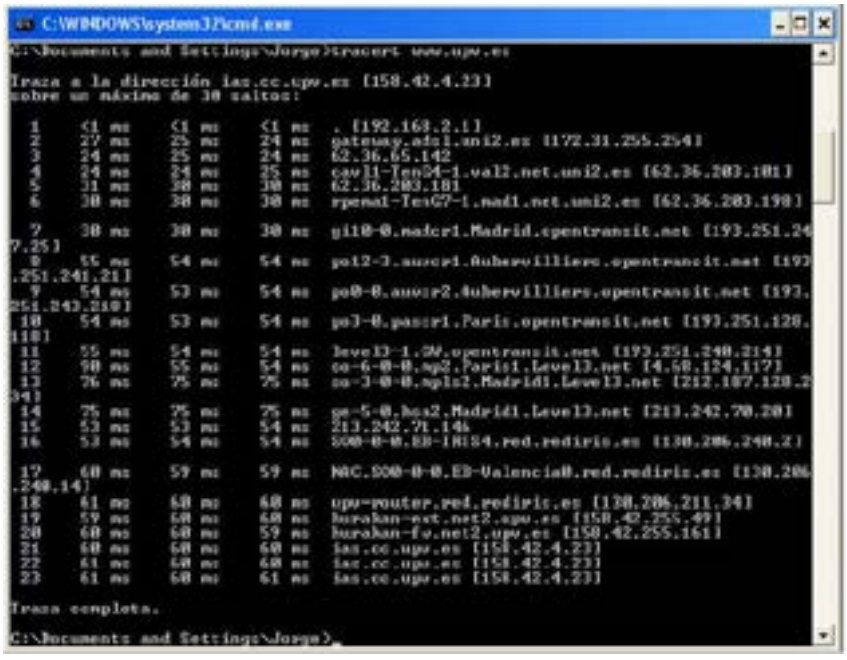
O comando tracert (proveniente da *rota de rastreamento*) pode ser usado para saber que dados dos dispositivos passaram para alcançarem o destino. Este comando funciona como o comando ping. Numa janela da interface de comando, precisamos de iniciar o tracert seguido do endereço IP ou do nome de domínio a partir do qual precisamos de obter das informações. Se pedirmos um domínio, também fornecerá as informações do endereço IP.

Por exemplo, se precisarmos de saber como aceder ao servidor da web do Google, precisamos de lançar “tracert www.google.com”:



A resposta mostra os endereços IP dos routers pelos quais a solicitação de resposta passou até atingir o destino e também o tempo de resposta.

Usando o comando tracert, podemos encontrar algumas curiosidades, como o facto de o pedido nem sempre seguir o caminho mais curto para chegar ao destino. No exemplo a seguir, pode ver que, para aceder ao servidor UPV (localizado em Valência) de Bilbao, o pedido passou por vários routers em Paris.



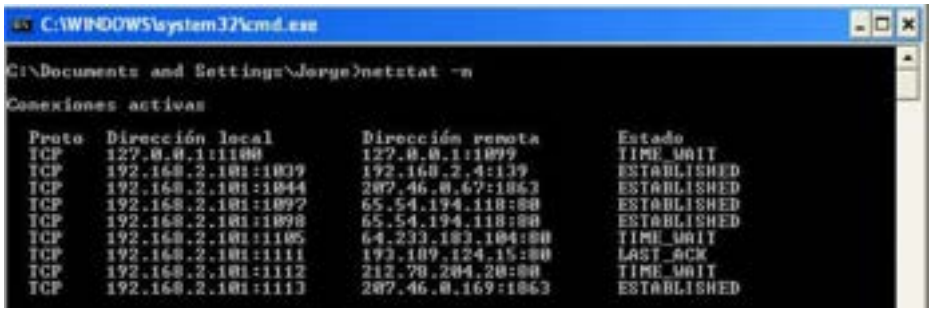
Preencha a tabela a seguir com os resultados do uso do comando tracert com os seguintes domínios:

Nome	**Número de "saltos"**
www.elpais.com	
www.upv.es	
www.marca.com	
Smtp.correo.yahoo.es	
www.google.com	

Tarefa 4. Comando Netstat

O comando netstat revela as ligações abertas entre vários computadores, por exemplo, quando se liga a um site ou descarrega o email.

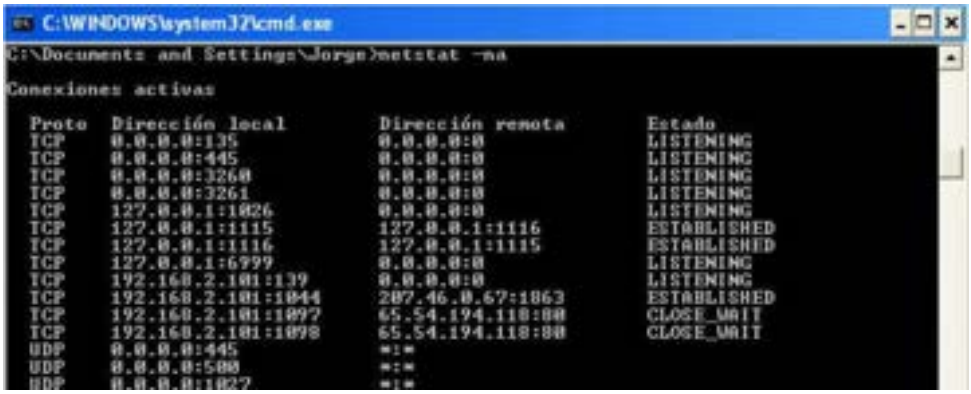
Inicie o comando “netstat –n” e veja que ligações estão abertas nesse momento no seu computador:



Na resposta do comando Netstat, os endereços local e remoto são indicados pelo nome do IP ou do computador, seguidos por dois pontos e o número da porta. A porta é um número que indica a aplicação ou protocolo que está a ser utilizado.

Por exemplo, a porta 80 é do protocolo http para sites; ou 1863 é a porta do Messenger (aplicação de mensagens em desuso).

Outra opção para o comando netstat é -a. Isso mostra que portas abriu nesse momento no seu computador. Estas são aplicações que funcionam como servidores no seu computador e que permitiriam que outras pessoas se ligassem ao seu computador (por exemplo, se tiver uma pasta compartilhada). Podem ser identificadas porque o estado mostra *escutando*.



Inicie o netstat -na na sua linha de comandos. Quantas ligações existem? Quais são os seus endereços IP e as portas?

Tarefa 5. Como se ligar através de SSH / Telnet a um router para configurações avançadas com o PuTTY

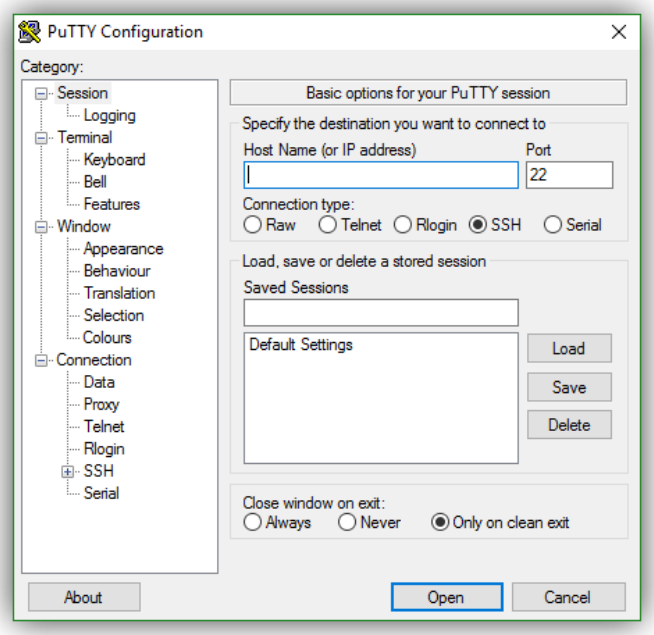
Atualmente, praticamente todos os routers do mercado têm uma interface da web a partir da qual podemos fazer todos os tipos de configurações: alterar nome de utilizador/senha, configurações de Wi-Fi, portas abertas, entre outros. Essa interface foi criada principalmente para utilizadores domésticos que têm um conhecimento avançado e, além de fácil de usar, mostra apenas as opções principais e mais utilizdas por routers; portanto, a maioria das funções fica oculta e sem acesso, pelo menos através dessa interface.

Praticamente todos os routers possuem um servidor Telnet que nos permite comunicar com o router a partir da linha de comando, o que é ideal para utilizadores experientes com conhecimento avançado. Permite-nos controlar quase todas as configurações internas possíveis do router, caso precisemos de aceder. Os routers mais avançados suportem o protocolo SSH, o que permite ligar-se de maneira semelhante à do Telnet, mas codificando todas as ligações.

Embora o Windows possa ativar um cliente Telnet e SSH no sistema, existem algumas aplicações de terceiros mais fáceis de utilizar, como o PuTTY, que nos permitem gerir todas essas ligações da maneira correta.

PuTTY é um aplicativo gratuito, portátil e com código aberto, desenvolvido para facilitar as conexões através dos protocolos SSH/Telnet do Windows. Vamos ver como nos podemos ligar remotamente a um router usando estes protocolos.

Primeiro, precisamos de fazer o download da versão mais recente do PuTTY do website principal. É portátil e não precisa de instalação, portanto, após o download, só é necessário executá-lo. Uma janela semelhante a esta será aberta:

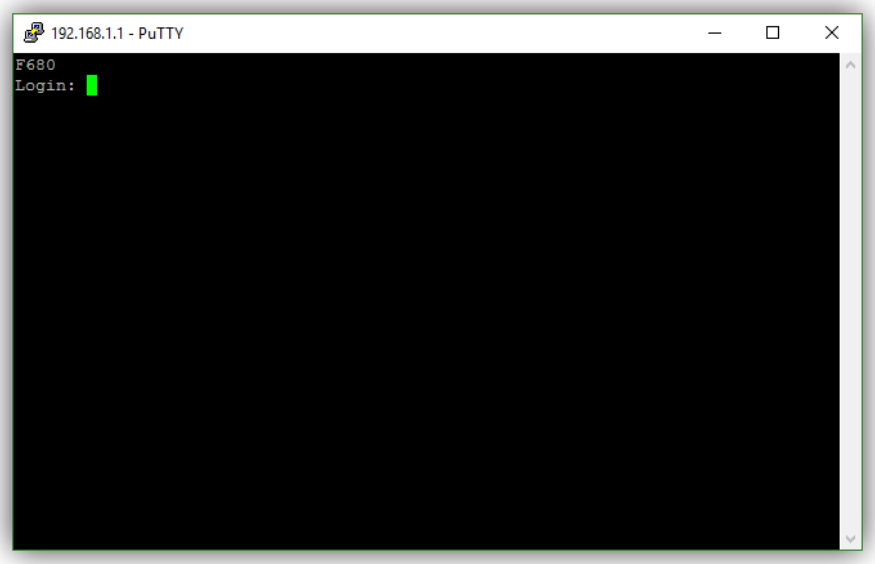


Primeiro, temos de introduzir o endereço IP do nosso router. Geralmente é 192.168.1.1 ou 192.168.0.1, dependendo do modelo e das configurações.

Logo abaixo do espaço em branco para introduzir o IP, encontramos “**Tipo de ligação**”, no qual precisamos de especificar o protocolo que vamos utilizar. Os mais comuns, como dissemos, são SSH e Telnet. Se o nosso router se ligar através da porta de série, o PuTTY também nos permitirá estabelecer uma ligação com a porta de série para a configurar através dos comandos.

Após introduzir o IP e selecionar o protocolo de ligação, pressione “Abrir” e o programa ligar-se-á ao router.

Se a ligação for permitida e tiver sido configurada, o PuTTY mostrará a seguinte janela:



Por fim, é necessário fazer login com o nosso nome de utilizador e palavra passe para começar a controlar o dispositivo.

O nome de utilizador e a palavra passe do Telnet/SSH podem não corresponder aos da interface da web, especialmente nos routers dos operadores.

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 2

Conceitos de segurança em ambientes industriais, Integração de IT/OT

2.1 Segurança em Infraestruturas Críticas

Description

Segurança em Infraestruturas Críticas

Table of contents

1. Segurança das instalações da fábrica

2. Segurança das instalações da fábrica (continuação))

3. Segurança da rede e sistemas

1. Segurança das instalações da fábrica

A segurança da fábrica garante que os edifícios envolvidos na produção estejam bem protegidos contra acesso interdito. Algumas medidas de prevenção podem consistir em:

Ø Vedações

É comum as instalações da fábrica estarem fechadas com uma vedação (Figura 2.1).

Figura 2.1 Área industrial vedada fonte

Normalmente, uma vedação em torno das instalações estabelece os limites da propriedade da fábrica, mas a sua principal utilização é funcionar como uma primeira medida de segurança contra possíveis intrusos. Embora uma vedação por si só não impeça um invasor, se usada em conjunto com outras medidas de segurança, pode ser uma boa solução. Atualmente, as vedações estão a ficar 'inteligentes'. Isto significa que os sensores espalhados ao longo da vedação podem identificar a entrada de um invasor na área. Esta nova geração de vedações pode ser ligada a uma rede.

G

G Seguranças.

A presença de seguranças depende principalmente do tipo e do tamanho das instalações. Dependendo da lei, os seguranças também podem estar armados. Geralmente, há um posto de vigia no portão principal do recinto da fábrica e os guardas permitem ou não a entrada do pessoal e também dos visitantes. Parte das suas funções poderia ser patrulhar as instalações, especialmente quando a fábrica está fechada.

Torniquetes.

Pode ser colocado um torniquete (Figura 2.2) no portão principal da fábrica. Impede os visitantes da fábrica de entrarem na instalação sem controle e também atrasa os invasores. As implementações mais recentes fornecem recursos de rede para torniquetes.

Figura 2.2: Um torniquete - por Fabtron - trabalho próprio, CC BY-SA 4.0 fonte

2. Segurança das instalações da fábrica (continuação))

Câmeras CCTV

CCTV significa televisão de circuito fechado. As câmaras de segurança (Figura 2.3) são colocadas à volta do perímetro externo da fábrica - geralmente em abóbadas na vedação externa - para registar qualquer atividade 24/7. Câmaras de segurança também são colocadas no prédio, na entrada principal e, frequentemente, também nas áreas de trabalho. Em grandes instalações (com um grande número de câmaras de segurança) existe uma sala de controlo, onde o pessoal autorizado e treinado monitoriza as câmaras para detetar comportamentos anómalos. Todos os dados captados pelas câmaras são guardados em discos rígidos num gravador de vídeo digital (DVR) ou num gravador de vídeo em rede (NVR). Neste último caso, os técnicos de instalação e o pessoal de monitorização devem ter muito cuidado, pois o NVR pode ser facilmente alvo de um ataque cibernético.

Figura 2.3 Cameras de Security

Leitores Biométricos

Colocam-se no exterior das portas, portões principais, etc.. Os dados biométricos tipicamente utilizados para identificar uma pessoa incluem: as impressões digitais, a íris e o formato do rosto. Como todas as características biométricas mencionadas são únicas para cada pessoa, é suposto os leitores biométricos fornecerem um nível de segurança muito bom. No entanto, existe o risco de os leitores biométricos também serem comprometidos, especialmente se estiverem ligados a uma rede. Os leitores biométricos também podem ser usados em conjunto com um cartão RFID ou uma palavra passe para melhor segurança (Figura 2.4). Os leitores biométricos mais recentes têm recursos de rede, portanto, o risco de se tornarem alvo de um ataque cibernético é relativamente alto.

Ø

Figure 2.4 Leitor biométrico - Fonte

Ø

Controlos de Acesso

Estes sistemas de segurança são usados para fornecer acesso a pessoal ou a visitantes autorizados. São programáveis e podem definir diferentes direitos de acesso, de acordo com o plano de segurança do sector. Diferentes funcionários podem ter direitos de acesso diferentes em relação às áreas onde podem circular, horários de utilização, etc.. Como todos os métodos mencionados, os controlos de acesso também possuem recursos de rede. Podem ser usados leitores de RFID, cartões magnéticos inteligentes, ou mesmo leitores biométricos.

3. Segurança da rede e sistemas

Segurança de rede

- Refere-se a hardware e a *software*
- Concentra-se numa variedade de ameaças
- Impede o acesso não autorizado a redes
- Supervisiona o acesso à rede

Tipos comuns de segurança de rede são:

- Software de segurança na Internet (antivírus, anti-malware, proteção contra *ransomware*, etc.)
- Segurança da aplicação
- Prevenção contra perda de dados
- Segurança do e-mail
- *Firewalls*
- Segmentação de rede
- Segurança na Web
- Rede virtual privada (VPN)
- Segurança sem fio
- Controle de acesso

A integridade do sistema refere-se a todas as medidas/políticas adotadas para proteger sistemas e componentes de automação contra acesso não autorizado (físico ou remoto). Algumas das medidas podem ser:

- Software antivírus e lista branca
- Processos de manutenção e de atualização
- Autenticação de utilizador para operadores de instalações ou máquinas
- Mecanismos integrados de proteção de acesso em componentes de automação

2.2 Integração OT/IT

Description

Integração OT/IT

Table of contents

1. Integração OT/IT

2. Vantagens

3. Desvantagens

4. Política de atualização de segurança do computador

5. Política de atualização de segurança dos PLCs

1. Integração OT/IT

Tecnologia Operacional (OT) em qualquer ambiente industrial define-se como o hardware e o software que deteta ou provoca uma mudança através da monitorização direta e/ou controlo de dispositivos físicos, processos e eventos na empresa.

Basicamente, OT consiste na utilização de PCs para monitorizar ou alterar a condição física de um sistema. Exemplos de tecnologia operacional:
PLCs SCADA
Equipamento científico DCS

Tecnologia da Informação (IT) menciona qualquer aspeto identificado com o registo de inovação em tecnologia de computadores, equipamentos de PC, programação de software, administração de hardware e sistemas. A programação de software incorpora todos os programas de PC - códigos e diretrizes - dentro de um PC. PCs não funcionam sem programação. O hardware do computador, mencionado nesta situação, faz alusão aos segmentos físicos de um PC. O ecrã, o rato e a placa-mãe e existem outros dispositivos em que eles são dispositivos de hardware.

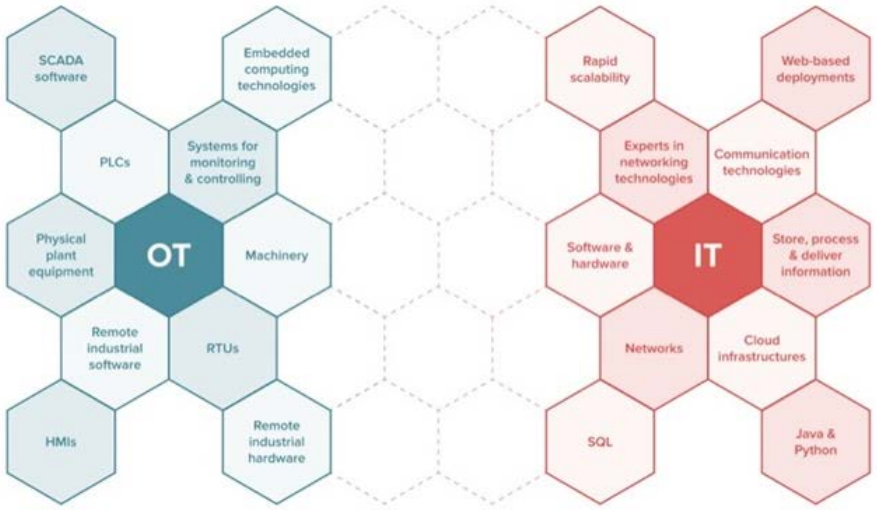


Figura 2.5 Tecnologia operacional (OT) e tecnologia da informação (IT) fonte

Pode pensar que a IT é a comunicação, o hardware, o software do sistema que armazena, processa e transmite dados para todas as partes de uma organização. Os especialistas em IT são íntimos e passam um tempo significativo no processo. por exemplo, fundações em nuvem, aplicações Web e tecnologias de programação (Python, SQL, java, c ++), etc..

OT inclui dispositivos, equipamentos físicos, hardware e software industrial remoto. Os especialistas em OT concentram-se nos sistemas utilizados para monitorização e controlo. São utilizados em PLCs, interfaces homem-máquina (HMIs), tecnologias de computação incorporadas, unidades terminais remotas (UTRs), estruturas de Controlo de Supervisão e Aquisição de Dados (SCADA).

Os sistemas SCADA recolhem informações de vários procedimentos no terreno da fábrica. Os indivíduos que trabalham em OT têm de dar sentido à incorporação de cada um dos sistemas para cooperarem. Como a maioria das inovações e OT é propriedade, é difícil integrar vários arranjos do SCADA.

PROFINET (rede OT) e Ethernet (rede de IT) são dois protocolos comuns que podem ser interligados (mais informações podem ser encontradas no Módulo 1). O único problema quando estes dois protocolos são interligados é a possibilidade de diminuição da disponibilidade.

Para obter mais informações sobre medidas preventivas de segurança, visite: https://www.iso.org/isoiec-27001- information-security.html

2. Vantagens

A integração OT/IT tem várias vantagens:

Aumenta a Produção e Economiza Tempo

A tecnologia da informação ajudou a que os processos de negócios se tornassem máquinas de fazer dinheiro incrivelmente económicas. Dessa forma, expande a eficiência que finalmente oferece lucros que implicam melhores salários e condições de trabalho menos cansativas.

Melhora a Comunicação

As ferramentas de Tecnologias da Comunicação da Informação (TCI), como e-mail, videoconferência, telefones celulares, laptops e assim por diante, permitem a comunicação direta dentro da empresa. Isto possibilita uma maior interligação através de estruturas internas e externas.

Melhora o Armazenamento de Dados, a Gestão de Arquivos e os Relatórios/Análises de Dados

As empresas utilizam serviços em nuvem, o que facilita o armazenamento e backup de dados, reforçando as informações comerciais. Além disso, permite economizar tempo e facilita quer a transferência quer o acesso remoto aos dados guardados, a partir de qualquer lugar, em qualquer momento. Através de serviços como a Dropbox, os empreendedores podem obter as suas informações em qualquer momento. Atualmente, os bancos de dados têm ainda em consideração uma melhor análise de muitos dados, o que permite que as tomadas de decisão ocorram de forma mais informada e com mais eficiência, com impacto direto no desenvolvimento.

Reduzir Custos de Operação

A tecnologia de comunicação e a tecnologia social tornaram o avanço dos negócios e o lançamento de produtos mais acessíveis. Inúmeras empresas independentes descobriram abordagens para a utilização da tecnologia social com o fito de aumentar o reconhecimento da marca e obter mais clientes a um custo reduzido. Elementos como o "custo" desempenham um papel decisivo no avanço e desenvolvimento de um negócio. Nesse sentido, a utilização de inovação de dados de tecnologia da informação para reduzir custos operacionais terá um impacto positivo no desenvolvimento de negócios.

Melhora o Caráter Competitivo dos Negócios

Uma utilização comercial da tecnologia será para a obtenção de vantagens competitivas. Empresas que avançam e adotam a inovação para permanecerem produtivas e melhorarem o seu processo. Geralmente, confiam plenamente na taxa de clientes, pois podem ir encontro, com confiança, dos desejos dos seus clientes.

3. Desvantagens

No entanto, a integração OT/IT também tem desvantagens:

Custos de Implementação

Por vezes, as pequenas empresas têm tecnologia básica e ao manterem esta tecnologia com baixa precisão, perdem os seus clientes, ao competir com outras empresas do setor que dispõem de fundos e de recursos.

Trabalho de Remoção

O crescimento das tecnologias substituiu as posições humanas em vários empregos.

Violações de segurança

Como as empresas armazenam a sua informação em servidores remotos, na nuvem, que podem ser acedidos on-line com um nome de utilizador e uma palavra passe, existe a possibilidade de as perder para *bugs* ou *hackers* de vulnerabilidade.

4. Política de atualização de segurança do computador

Para garantir segurança e fiabilidade, é importante ter práticas bem documentadas para a instalação e atualizações de software. A tabela que se segue oferece regras para backups, processos de atualização de administrador e um planeamento dos períodos de atualizações.

Da política: Manter um cronograma padrão de atualizações - a aplicação de correções básicas, sempre que forem encontradas vulnerabilidades, é vital para manter a integridade da segurança corporativa. Com o aparecimento de ameaças como o *ransomware*, a execução de atualizações regulares de segurança às plataformas e a criação de backups é importante para garantir que os processos de negócios são conduzidos sem problemas.

Tabela 1: Política de Segurança de Computadores

Atualizações Semanais	
Carga Útil:	*Patches* de segurança e atualizações às aplicações padrão instaladas no computador.
Plano:	Todas as quintas-feiras (ou outro dia) a partir das 20h.
Estado da Alimentação de Energia:	O computador deve estar ligado para receber atualizações.
Estado de Login:	O computador tentará instalar atualizações, independentemente de alguém estar a utilizar o computador ou não. GUARDE O SEU TRABALHO - O COMPUTADOR IRÁ INICIALIZAR INDEPENDENTEMENTE DE ESTAREM EM ABERTO APLICAÇÕES E/OU O TRABALHO NÃO TER SIDO GUARDADO.
Failover (falha):	Se o computador não for ligado durante a atualização agendada, as atualizações terão efeito na vez seguinte em que o computador for ligado.
Backup:	Faça *backup* de arquivos importantes duas vezes por mês
No caso de um utilizador estar a utilizar o computador (logged in)	
Visão geral:	O computador tentará instalar atualizações, solicitando ao utilizador opções flexíveis de instalação e de reinício para se adaptar ao horário de trabalho do utilizador. As atualizações serão aplicadas e o computador será reiniciado no caso de não existir resposta às solicitações.
Tempo limite de adiamento:	Se a atualização não for adiada em 30 minutos, as atualizações serão iniciadas automaticamente.
Reiniciar o sistema:	Se for aplicada uma atualização que exija um reinício, o utilizador poderá adiar esse reinício até sete (7) vezes antes que o computador reinicie automaticamente para concluir a instalação. O estado de suspensão/espera dura 30 minutos. De seguida, o utilizador é notificado novamente.
Tempo limite de reinício:	Se o reinício não for adiado 30 minutos, o computador emite nova notificação em 120 minutos (ou seja, outro adiamento). Após os sete (7) adiamentos possíveis mencionados, o utilizador terá mesmo de reiniciar o computador.
Frequência de reinício:	Se for aplicada uma atualização que exija reiniciar o computador, ele reinicia uma vez.
Impacto no desempenho:	As atualizações das aplicações variam em número e em tamanho a qualquer momento. O impacto no desempenho do computador geralmente é insignificante, com um possível reinício após a instalação.
No caso de ninguém estar a utilizar o computador	
Visão geral:	O computador instala as atualizações e reinicia-se automaticamente, se necessário.
Frequência de reinício:	Se for aplicada uma atualização que exija reiniciar o computador, ele reinicia uma vez.

5. Política de atualização de segurança dos PLCs

Os PLCs são tão importantes nas redes dos sistemas de controle como em qualquer outro ambiente de rede. É essencial que sejam geridos com prioridade. Qualquer acesso, manutenção, atualização, teste, modificação e tempo de inatividade dos PLCs tem de ser considerado e estas políticas têm de ser aplicadas.

Princípios básicos da política

- **Corrigir as palavras passe padrão**

Altere todas as palavras passe padrão. A não alteração das palavras passe padrão que vêm definidas de origem é um dos erros mais comuns cometidos pelas organizações.

- **Garantir que somente indivíduos certificados têm acesso ao ambiente de sistema do controlo**

Por questões de segurança, apenas as pessoas afetas ao sistema de controlo de segurança da empresa devem ter acesso a esse sistema.

- **Limitar o acesso às movimentações e manter o acesso seguro.**

Os utilizadores devem frequentemente ser informados sobre a utilização dos dispositivos e das tecnologias novas, ou de qualquer alteração futura.

- **Fazer upgrade do *firmware* para a sua última versão**

A atualização regular do sistema operativo/atualização de *firmware* consiste numa atualização de segurança emitida para proteger o seu computador/sistema contra as vulnerabilidades que podem ser exploradas por hackers e vírus.

Figura 2.6 PLC fonte

Figura 2.7 PLC fonte

2.3 Ataques em Sistemas Industriais

Description

Ataques em Sistemas Industriais

Table of contents

1. Ataques DoS/DDos
1.1. Tipos de ataques DDoS
1.2. Ataques Baseados em Volume
1.3. Ataques de Protocolo
1.4. Ataques na Camada da Aplicação
1.5. Exemplo de ataque de inundação SYN
1.6. Exemplo de ataque de inundação HTTP
1.7. Exemplo de amplificação de ataque DNS
1.8. Prevenção DDoS
1.9. Atividade DoS
1.10. Resumo DoS

2. Ataque Man-in-the-Middle (MitM)
2.1. Simplificação do protocolo ARP
2.2. Tráfego da rede ARP
2.3. ARP Spoofing
2.4. Exemplo de cenário
2.5. HTTPS para o resgate... ?
2.6. Forçar a comunicação HTTP

3. Ataques de dicionário e phishing

4. Ataque de injeção SQL
4.1. Como funcionam os ataques de injeção SQL?
4.2. Como podem ser evitados os ataques de injeção SQL?

5. Ataque Modbus
5.1. Medidas de prevenção

1. Ataques DoS/DDos

DOS é o acrónimo **D**enial **o**f **S**ervice. É um tipo de ataque que ocorre num computador ou rede, impedindo que os recursos do sistema sejam acessíveis aos utilizadores. Desativa o site (servidor da web) a que o utilizador pretende aceder. Para atingir esse objetivo, cria muitas solicitações de serviço em simultâneo que o servidor que hospeda o site não pode satisfazer, levando à falha da resposta do servidor a todas as solicitações. Portanto, enquanto houver um ataque DoS, o tráfego habitual do site será lento ou inativo.

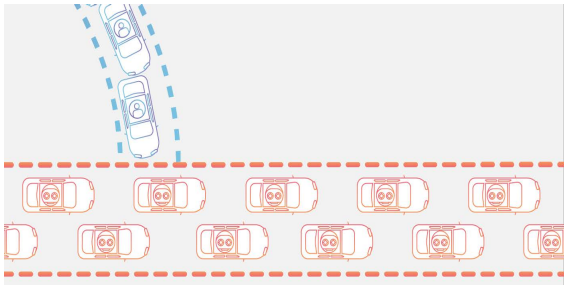


Figura 2.9 Tráfego do ataque DoS fonte

Eliminar alguns negócios da Web pode Conduzir a uma enorme perda de negócios ou dinheiro. A Web, a Internet e as redes de computadores alimentam muitas organizações. Algumas organizações, por exemplo, de comércio eletrónico, serviços de pagamento, dependem totalmente da Internet para funcionarem, em conjunto, como empresa.

Existem dois tipos de ataques:

DoS- este tipo de ataque é realizado por um único host.

DoS distribuído (DDoS)- realiza-se ao enviar um grande número de pedidos desnecessárias ao sistema ou ao recurso de rede, de muitas fontes diferentes.

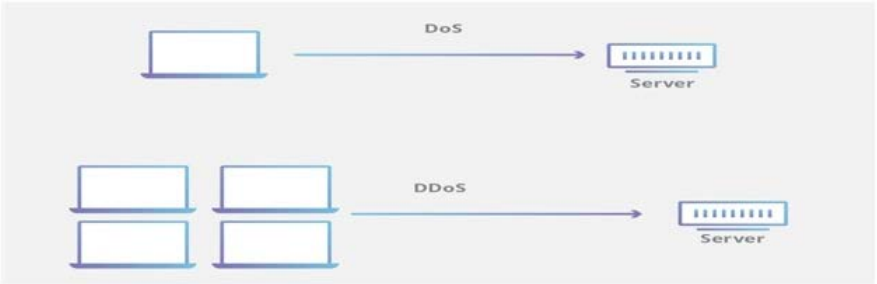


Figura 2.9 Tipos de ataques DoS fonte

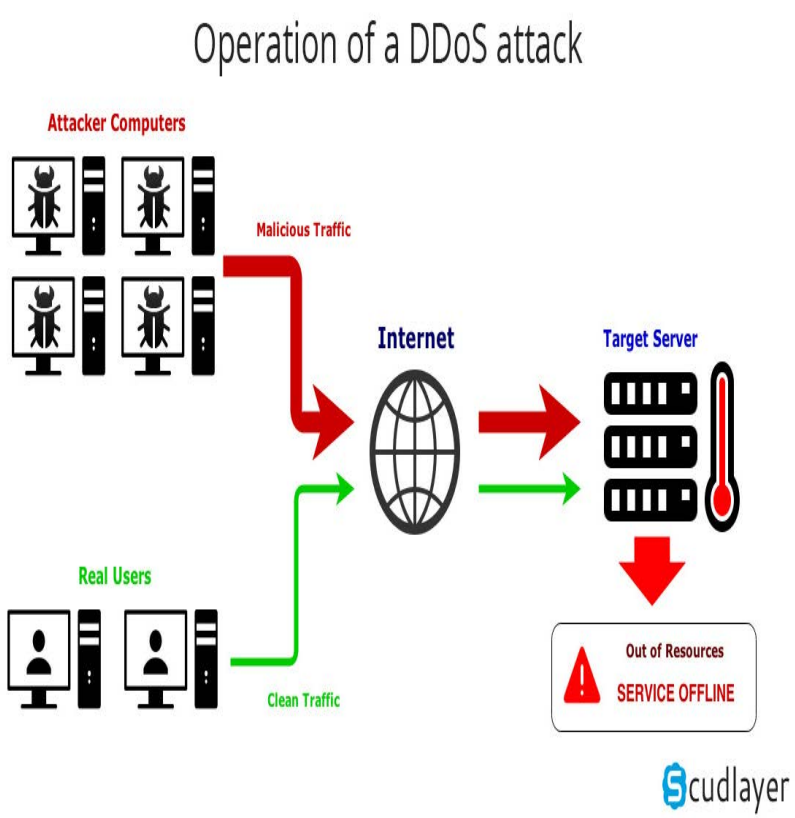


Figura 2.10 Compreender os ataques DDoS fonte

1.1. Tipos de ataques DDoS

Existem três tipos de ataques DDoS:

- Protocolo de ataques com base em volume
- Ataques de protocolo
- Ataques na camada de aplicações

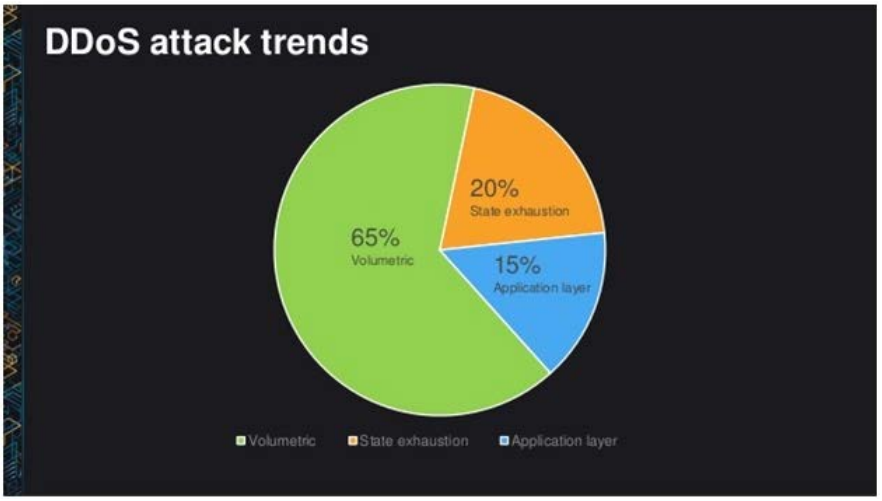


Figura 2.11 Tendências de ataques DDoS fonte

1.2. Ataques Baseados em Volume

Ataques baseados em volume como o próprio nome indica, estes ataques baseiam-se no volume. Também se denominam de **Ataques de Camadas 3 e 4.**O atacante utiliza táticas muito básicas, obtendo a maioria dos recursos disponíveis neste "jogo". Se conseguirem sobrecarregar e exceder os recursos disponíveis, vencem. Para a maioria dos proprietários de sites, facilmente ficam sem recursos. A magnitude do ataque é medida em **bits por segundo (bps)**.

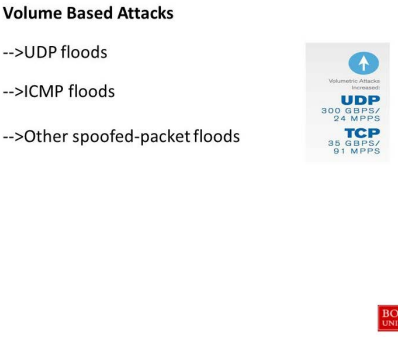


Figura 2.12 Ataques baseados em volume fonte

Abordagens para este tipo de ataque:

- **Inundação de UDP** - Um ataque de inundação de UDP envolve o envio de um número muito grande de pacotes UDP para portas aleatórias de um computador, mais especificamente para a porta número 53. O computador atacante primeiro terá de determinar se algum dos seus serviços está em escuta nessa porta e se não está a responder, devendo responder com um pacote de Destino Inacessível ICMP. Portanto, o influxo de um grande número de pacotes UDP no computador atacante obriga-o a responder com um número igualmente grande de pacotes ICMP, o que, em última instância, impede que outros utilizadores comuns usem os serviços do seu PC. Firewalls especializadas podem ser utilizadas para filtrar ou bloquear pacotes UDP maliciosos.

- **Inundação de ICMP** - O invasor envia pacotes de inundação de Pedido Eco ICMP para um host/utilizador remoto. Para que esse ataque seja bem-sucedido, o invasor tem de ter mais largura de banda do que a vítima. Se a vítima responder com um pacote de Resposta Eco ICMP a cada pacote de ping (pedido Eco ICMP), consumirá toda a sua largura de banda e, consequentemente, os serviços oferecidos não estarão mais disponíveis para os seus utilizadores. A tática para lidar com essa situação consiste em: Em vez de rejeitar todos os pacotes de ping, o número de pacotes que a firewall recebe é registado e, se esse número exceder um limite predefinido, a firewall começa a rejeitá-los.

- **Flood HTTP** - O ataque de flood HTTP é um tipo de ataque de negação de serviço no qual o invasor manipula os protocolos HTTP e POST para atacar um servidor da Web ou aplicação.

1.3. Ataques de Protocolo

Ataques de protocolo Este tipo de ataque é direcionado ao nível do protocolo. Esta categoria inclui Synflood, Ping of Death, inundação de DNS e muito mais. A magnitude do ataque é medida em **Pacotes por Segundo**.

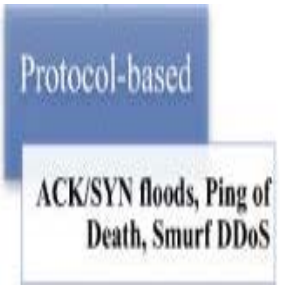


Figura 2.13 Ataques basaedos em protocolo

- **Inundação de DNS** - O invasor organiza o envio de um grande número de solicitações de DNS ao destino, que aparentemente é um servidor DNS. A vítima recebe tantos pedidos DNS ao mesmo tempo que não consegue lidar com eles, acabando, portanto, por falhar devido a sobrecargas, principalmente na memória e na CPU.

- **SYN Flood** -O atacante envia várias solicitações de SYN para uma vítima. O computador da vítima aloca um lugar nas suas tabelas para cada pedido que chega e envia um pacote de resposta SYN + ACK. Se o atacante não responder, ou se ele ocultou o seu endereço IP real, a posição na tabela permanecerá reservada até o tempo de espera expirar. Se o invasor enviar milhares de pedidos SYN, as posições da tabela do computador da vítima serão preenchidas e as ligações legítimas não poderão passar.

  A maneira mais eficaz de lidar com esse risco é registar o número de ligações que cada cliente iniciou e proibir a criação de novas ligações quando esse número exceder um limite predefinido. No entanto, se o invasor em cada novo pedido SYN fornecer um endereço IP de remetente diferente, o método acima não funcionará.

- **Ping of Death** -Um pacote de ping normalmente tem 64 bytes (ou 84 bytes se o cabeçalho que adiciona o protocolo IP for incluído). Muitos tipos de computadores não podem manipular pacotes de ping maiores do que 65535 bytes, que é o máximo permitido pelo protocolo IP. Como resultado, o ataque Ping Of Death envolve o envio contínuo de grandes pacotes de ping para um computador até ocorrer a falha do sistema.

Para combater esse ataque, é importante verificar se os pacotes são válidos ao montar os pacotes IP. Dessa forma, é possível rejeitar pacotes IP maiores que o permitido e, assim, evitar o risco desse tipo de ataque.

1.4. Ataques na Camada da Aplicação

Ataques na camada de aplicação esse tipo de ataque tem como alvo vulnerabilidades em software como Windows, Apache, OpenBSD, etc., para executar o ataque e travar o servidor. A magnitude do ataque é medida em **Pedidos por Segundo**.

- **Application Attack** - também chamado de Layer 7 Attack, é um dos tipos mais populares de ataques direcionados a vulnerabilidades específicas a nível da aplicação. Tudo o que é necessário é uma pequena modificação no código e um pequeno ajuste para começar a enviar informações aos hackers. É extremamente difícil reconhecer os ataques da Camada 7, uma vez que seguem o tráfego original do site.

- **Slowloris** - é usado para iniciar o servidor e executar um ataque DDoS. Envia um grande número de pedidos HTTP ao destino (servidor da web). O destino mantém todas as ligações abertas havendo, portanto, um excesso de ligações simultâneas.

- **Ataques DDoS dia-zero** - são novos tipos de ataques que exploram vulnerabilidades para as quais ainda não foi lançado nenhum patch. O exemplo mais comum é (explorar vulnerabilidades) nas máquinas linux

1.5. Exemplo de ataque de inundação SYN

Ataque SYN Flood no qual o atacante envia múltiplos pedidos SYN (Sincronização) à vítima com um endereço IP fictício. O protocolo TCP exige as seguintes três etapas para estabelecer a ligação entre dois computadores:

- Remetente envia pacote SYN (Sincronizar)
- O destinatário responde com um pacote SYN-ACK (Confirmação de Sincronização)
- O remetente envia um pacote ACK recente e a ligação é considerada bem-sucedida.

O invasor envia várias solicitações de SYN e não envia ACK para que o processo continue, com o objetivo de desperdiçar recursos de computação significativos e impedir o sistema de atender outros utilizadores.

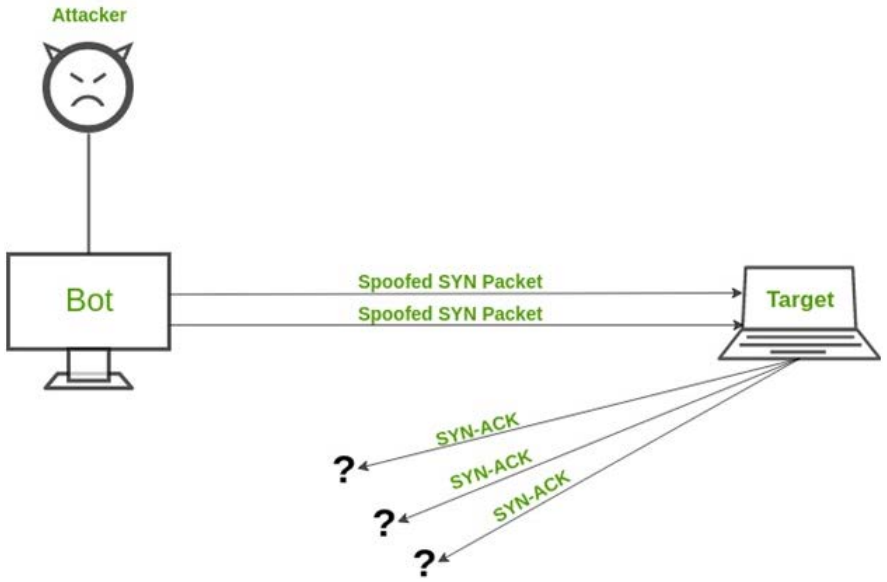


Figura 2.14 Ataque do tipo Syn flood fonte

1.6. Exemplo de ataque de inundação HTTP

Um **HTTP Flood attack** envia vários pedidos HTTP GET ou POST para atacar um servidor web ou aplicação. O ataque força o servidor ou aplicação a dedicar o máximo de recursos possíveis na resposta a cada pedido.

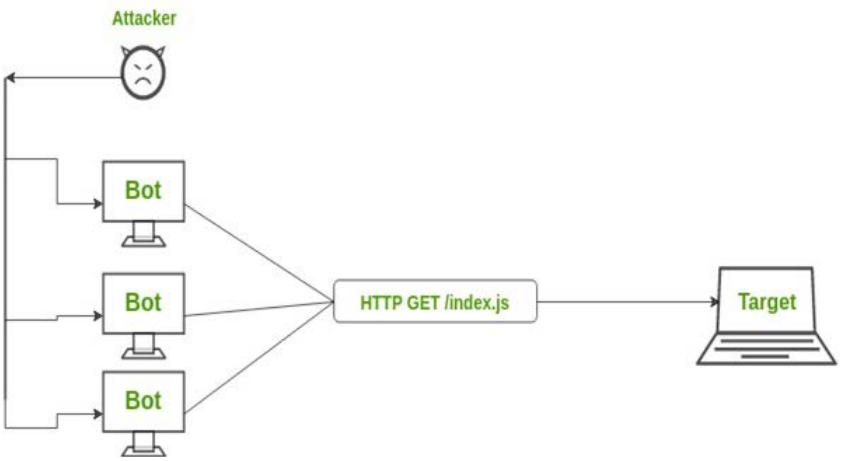


Figura 2.15 Ataque do tipo Http flood fonte

1.7. Exemplo de amplificação de ataque DNS

Estes ataques são muito populares atualmente e são observados na camada 3/4. Usam servidores DNS amplamente disponíveis de diferentes partes do Globo para inundar o seu servidor com tráfego de respostas DNS. Sobrecarregado com uma confusão de respostas, o servidor tem dificuldade em funcionar, à medida que os seus recursos vão sendo reduzidos, resultando em falha total na capacidade para responder adequadamente ao tráfego normal de DNS.

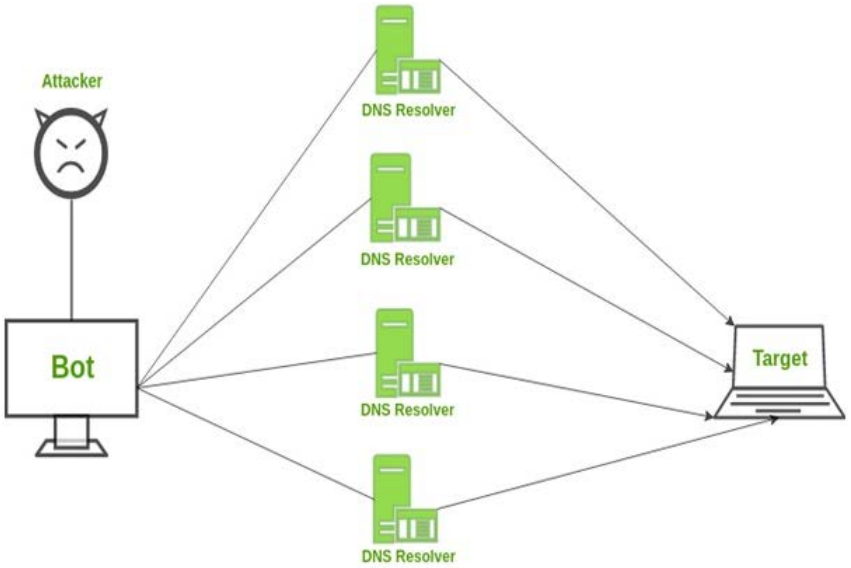


Figura 2.16 Ataque do tipo DNS flood fonte

1.8. Prevenção DDoS

Prevenir ataques DDoS é **mais difícil do que prevenir DoS ataques** , devido à origem dispersa, por vários endereços IP (fontes), do tráfego. Algumas dos medidas de prevenção que podem ser utilizadas são:

Algumas técnicas que podem ser usadas são:

1. **Encaminhamento de buraco negro**

No encaminhamento de buraco negro, o tráfego da rede é direcionado para um 'buraco negro'. Nesta estratégia, quer o tráfego de vírus quer o tráfego não malicioso se perdem no buraco negro. Essa medida de prevenção é útil quando o servidor está perante um ataque DDoS e todo o tráfego é desviado para a manutenção da rede.

2. **Limitação de tráfego**

A limitação de volume de tráfego envolve o controle do volume de tráfego que é enviado ou recebido por uma interface de rede. É eficiente na redução do ritmo dos invasores da Web, assim como a reduzir as tentativas de login forçado. No entanto, é improvável que apenas a limitação da taxa de tráfego impeça ataques DDoS compostos.

3. **Lista negra / lista de permissões**

A Lista Negra consiste num mecanismo de bloqueio de endereços IP, URLs, nomes de domínios, etc. mencionados na lista e permite o tráfego de todas as outras fontes. Por outro lado, a lista de permissões refere-se ao mecanismo que permite o acesso a todos os endereços IP, URLs, nomes de domínio, etc. mencionados na lista e nega acesso aos recursos da rede a todas as outras fontes.

Uma organização pode adotar a estratégia de acompanhamento para se prevenir contra os ataques de Denial of Service.

- Os ataques SYN flooding exploram bugs no sistema operativo (Windows, Linux, etc.). **A instalação de patches de segurança** pode ajudar a diminuir a possibilidade desses ataques.
- **Os sistemas de deteção de intrusões (IDS)** podem ser utilizados para monitorizar atividades ilegais.
- **Os routers** podem ser configurados através da Lista de Controlo de Acesso para restringir novamente o acesso à rede e eliminar o tráfego ilegal.
- **As firewalls** podem ser utilizadas para interromper um ataque de DoS, impedindo todo o tráfego advindo de um ataque, ao reconhecer o seu IP.

Figura 2.17 Mitigação de ataques Dos fonte

1.9. Atividade DoS

Atividade:

Imagine que utilizamos janelas e que temos dois computadores na mesma rede. Os ataques do DOS são ilegais em sistemas/redes em que não tem autorização de acesso. Este é o motivo pelo qual deve organizar o seu próprio sistema.

Basta abrir o prompt de comando do Windows (cmd)

Temos uma vítima e estamos a inundar este endereço IP com 65000 pacotes.

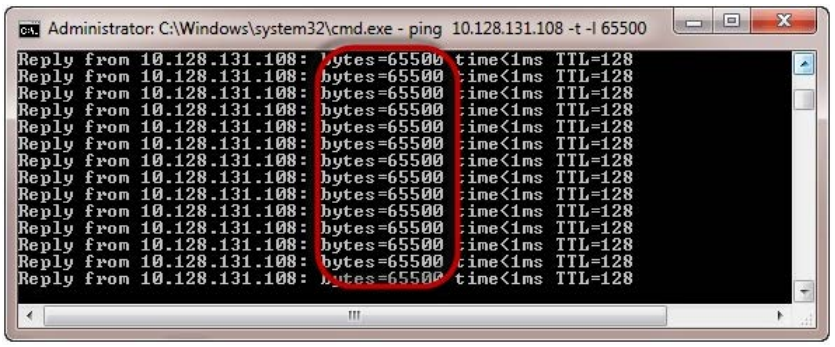


Figura 2.18 Ataque Dos flooding

Atacar um único host tem pouco efeito no alvo. Para ser mais eficaz, são necessários mais computadores (ataque DDoS).

O ataque é frequentemente usado em servidores web, routers, etc..

Pode verificar se esse ataque afeta a vítima. Basta abrir o gestor de tarefas e clicar na tab Rede.

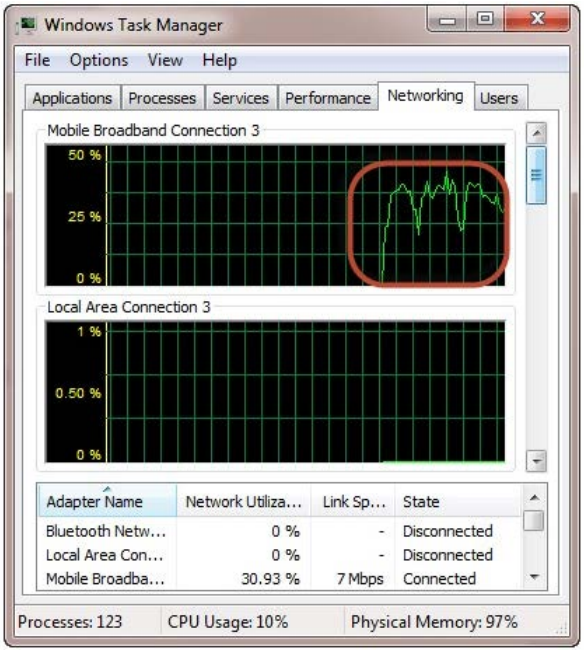


Figura 2.19 Verificar a rede

Como é possível observar, a atividade da rede aumentou quando o ataque foi bem-sucedido

1.10. Resumo DoS

- O objetivo de um ataque DOS é impedir o acesso de clientes reais a um recurso, por exemplo, num sistema, ou servidor.
- Existem dois tipos de ataques, **DoS** e **DDOS**.
- Pode realizar-se um ataque do DoS usando flood HTTP, flood DNS, flood SYN, ataque à aplicação, sobrecarga de buffer, etc..
- As atualizações para sistemas operativos, firewalls, sistemas de monitorização, como IDS (Sistema de deteção de intrusão) e configurações de router/switch, podem ser usadas para proteger de ataques DOS.

2. Ataque Man-in-the-Middle (MitM)

Um ataque **Man-in-the-Middle (MITM)** ocorre quando uma comunicação entre dois sistemas é interceptada por uma entidade externa. Isso pode acontecer com qualquer rede ou qualquer forma de comunicação on-line, como o email, as redes sociais, navegação na web, serviços bancários on-line, etc..

O objetivo comum de um ataque é roubar informações pessoais, obter credenciais de login, detalhes da conta e números de cartão de crédito ou recursos digitais.

O protocolo ARP

A forma como o protocolo ARP funciona é a razão da sua vulnerabilidade a um ataque MiTM. Portanto, para entender o ataque, é necessário um entendimento básico deste protocolo.

ARP significa **Address Resolution Protocol**, ajuda um host de rede a converter o endereço IP para o endereço MAC. Este auxílio é necessário para que os dados passem da Camada de Rede do modelo OSI (camada 3) para a Camada de Vínculo de Dados (camada 2).

Suponha que a Máquina A precise de transferir dados para a Máquina B. Ao aumentar o zoom para os níveis mais baixos do modelo OSI, seria necessário passar pela Camada Rede, pela Camada de Vínculos de Dados e pela Camada Física (camada 1). Para que a Máquina A possa ligar-se à Máquina B, a Máquina A precisaria de saber o endereço IP da Máquina B? Informações conhecidas na camada de rede.

A camada de Vínculo de Dados comunica usando endereços MAC. Portanto, é necessário converter o endereço IP para o endereço MAC da Máquina B (e vice-versa na máquina destinatária). A Figura 2.20 ilustra este aspeto:

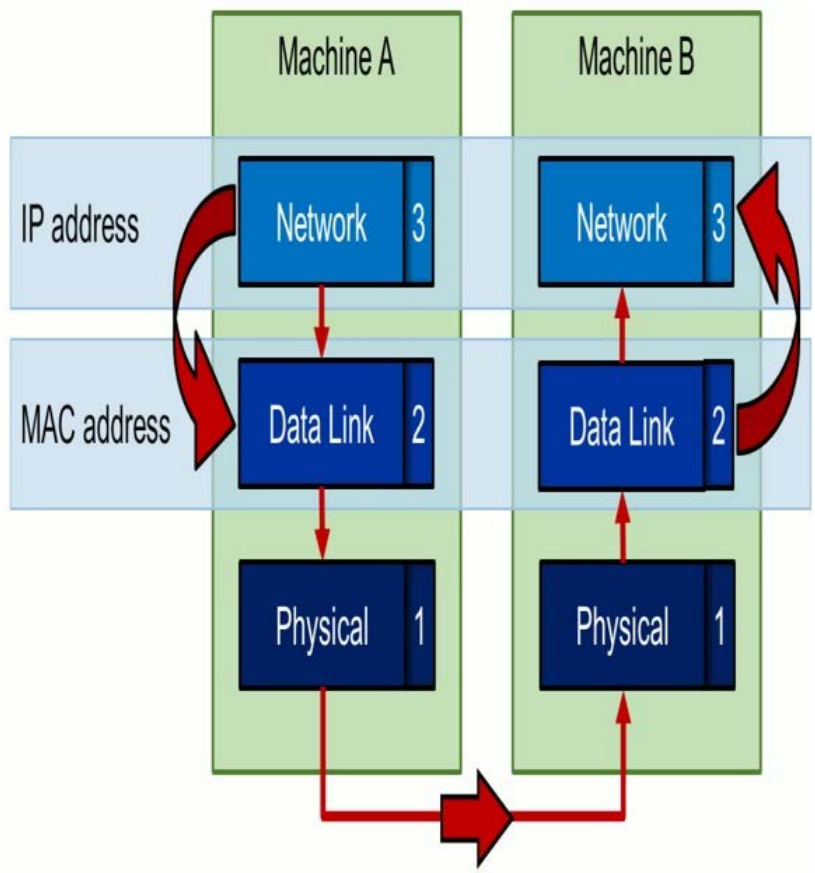


Figura 2.20 Camadas do modelo OSI 1-3 fonte

Camadas do modelo OSI 1-3

A conversão, ou melhor, a resolução do endereço IP em endereço MAC (e vice-versa) é onde o protocolo ARP entra em ação. Ambas as máquinas terão uma tabela **ARP** onde os endereços IP e MAC correspondentes de todas as máquinas conhecidas são armazenados. Então, como obtém a Máquina A o endereço MAC correspondente ao Endereço IP da Máquina B?

A máquina A apenas o solicita.

2.1. Simplificação do protocolo ARP

A Figura 2.21 representa de forma simplificada o protocolo ARP:

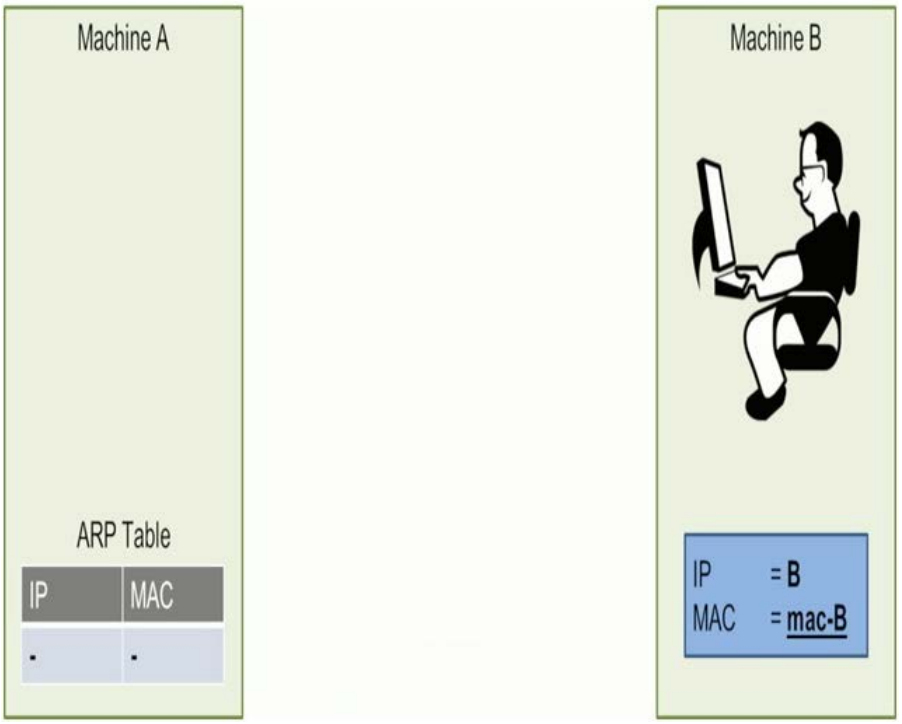


Figura 2.21 Protocolo ARP fonte

As três etapas no resumo

1. Na primeira etapa do protocolo ARP, a máquina A envia um pedido **ARP**. Esta é uma transmissão para a rede com a pergunta "Quem possui o endereço MAC para o endereço IP da Máquina B?".

2. As máquinas B têm essa informação e enviam um **ARP re-testando** "O endereço MAC B é o endereço MAC da máquina B".

3. A máquina A recebe a resposta do ARP e grava (ou atualiza) a entrada na sua tabela **ARP**.

É no último passo que reside o problema com este protocolo. No entanto, antes de abordarmos esses problemas, veremos os pacotes ARP a serem transmitidos pela rede.

2.2. Tráfego da rede ARP

A imagem abaixo mostra uma parte de uma captura de rede feita com Wireshark.

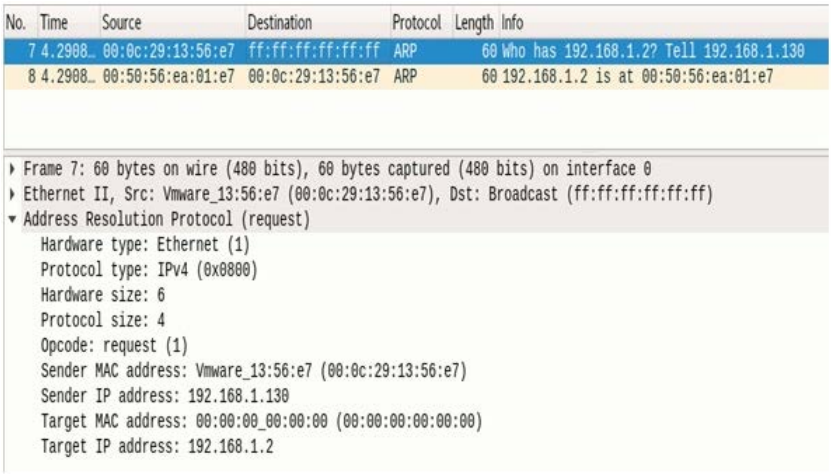


Figura 2.22 Tráfego capturado na rede ARP fonte

Podemos observar com clareza dois pacotes com os números 7 e 8.

- O primeiro Pacote (7) contém o pedido **ARP** de um computador com endereço MAC de origem 00:0c:29:13:56:e7 e com o endereço MAC de destino ff:ff:ff:ff:ff:ff, o que significa uma mensagem de difusão. Então, o lógico é "Quem tem 192.168.1.2? Diga 192.168.1.130".
- O segundo pacote (8) é a resposta **ARP** de um computador com endereço MAC 00:50:56:ea:01:e7 e com o endereço MAC de destino do pacote 7 original. O Wireshark sabe que o ip "192.168.1.2 tem endereço mac 00:50:56:ea:01:e7", que é realmente o mesmo endereço MAC da fonte desta mensagem.

2.3. ARP Spoofing

O facto de a Máquina A atualizar a sua tabela ARP com as informações de uma resposta ARP **sem nenhuma dúvida sobre a validade dessas informações**, abre a porta para a falsificação de ARP (também conhecida como **envenenamento por ARP**).

Um invasor pode enviar uma resposta ARP mal-intencionada, sem nenhum pedido anterior, contendo o seu próprio endereço MAC e o endereço IP de outra máquina. A máquina para a qual a resposta foi direcionada atualizará a sua tabela ARP sem questionar.

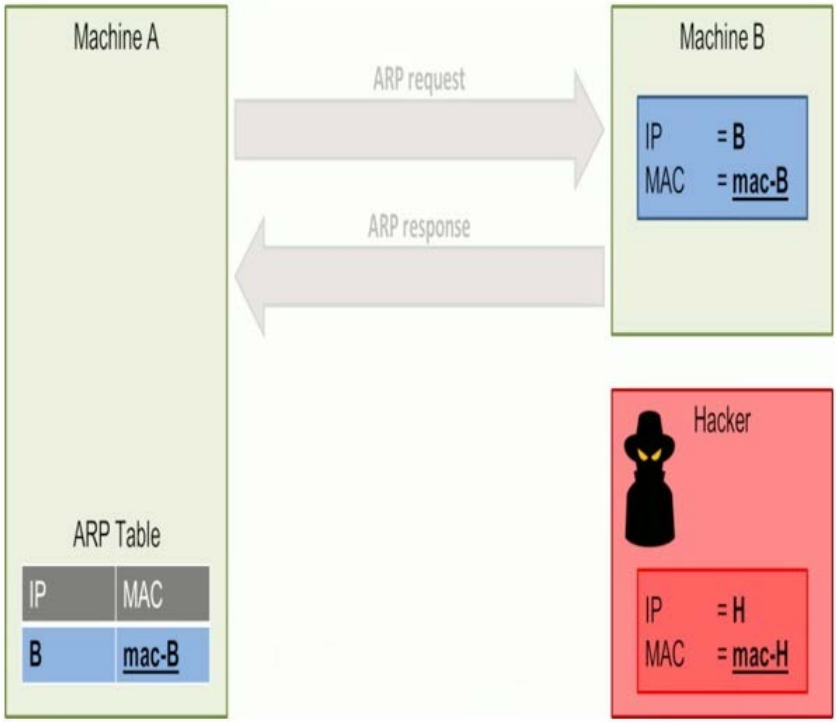


Figura 2.23 ARP spoofing fonte

A imagem acima mostra o mesmo cenário anterior. No entanto, um hacker acaba de se juntar às Máquinas A e B na rede. O hacker fez o seu trabalho nas fases de reconhecimento e scanning, sabe que as máquinas A e B existem na rede e quais os seus endereços IP.

Neste exemplo, o próprio hacker possui o endereço IPHe o endereço MAC mac-H. Envia a sua resposta ARP maliciosa à Máquina A, com a mensagem "mac-H é o endereço MAC do endereço IP B". A máquina A atualiza sua tabela ARP e o endereço IP B agora está vinculado ao endereço MAC H.

A partir de agora, sempre que a Máquina A quiser enviar uma mensagem para a Máquina B, ele converterá o endereço IP da Máquina B no endereço MAC H que será enviado ao hacker em vez de à Máquina B.

Homem-do-meio

Vimos como um invasor pode fazer uma máquina enviar os seus dados para ele, em vez de enviá-los para o destino pretendido, enviando um ARP malicioso.

2.4. Exemplo de cenário

Suponha que temos o seguinte cenário:

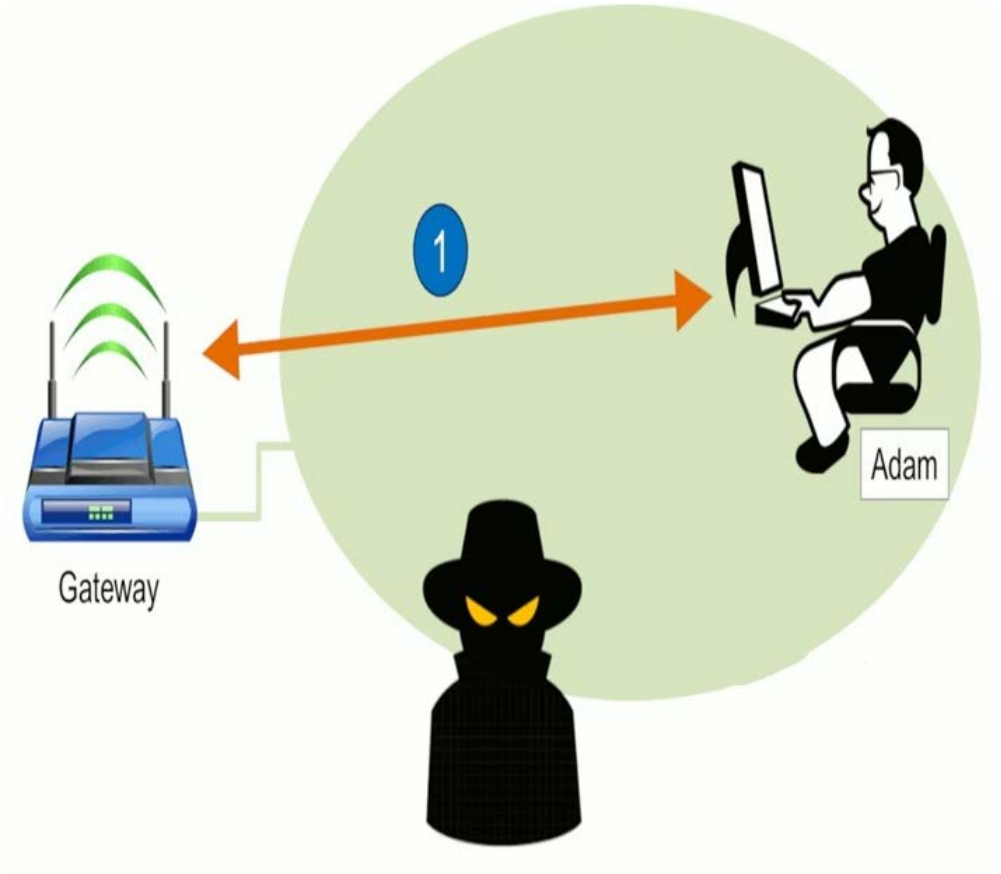


Figura 2.24 Cenário de falsificação de ARP fonte

Temos Gateway A, um hacker e Adam.

1. Na primeira etapa, Adam ligou-se à rede. Nesta progressão, o invasor fará um scan da rede para descobrir quem mais está disponível e que endereços IP e MAC ele possui.
2. Em seguida, o hacker envia uma resposta ARP maliciosa para ambos (Gateway e Adam). Basicamente, o hacker diz ao Gateway que ele é o Adam e simultaneamente diz ao Adam que ele é o Gateway.
3. Gateway e Adam atualizarão as suas tabelas ARP com as novas informações. A partir de então, esses nós começarão a enviar os seus dados ao hacker em vez de os enviar ao outro. Paródia ARP concluída!

O invasor precisará de tomar algumas medidas antes de começar a interceptar dados corretamente.

2.5. HTTPS para o resgate... ?

Considere o cenário do subcapítulo anterior em que o hacker está entre o Gateway e o Adam. O hacker seria capaz de ver todo o tráfego de ambas as partes. Por exemplo, se o Adam navega num site, o hacker pode ver todos os dados enviados e recebidos dos sites que ele está a aceder.

E quanto ao **HTTPS**? Isto é HTTP sobre **TLS** (ou HTTP sobre SSL). Isto significaria que todos os dados na linha seriam encriptados, certo? A descriptação verdadeira e em tempo real ainda não é remotamente viável. Portanto, o hacker não conseguiria ver o conteúdo encriptado do tráfego HTTPS.

A solução: **força a vítima a comunicar via HTTP** que é um texto sem encriptação, em vez de HTTPS.

Antes de explicar como isto pode ser feito, vamos ver como uma sessão de HTTPS é configurada quando navega em www.google.com (por exemplo):

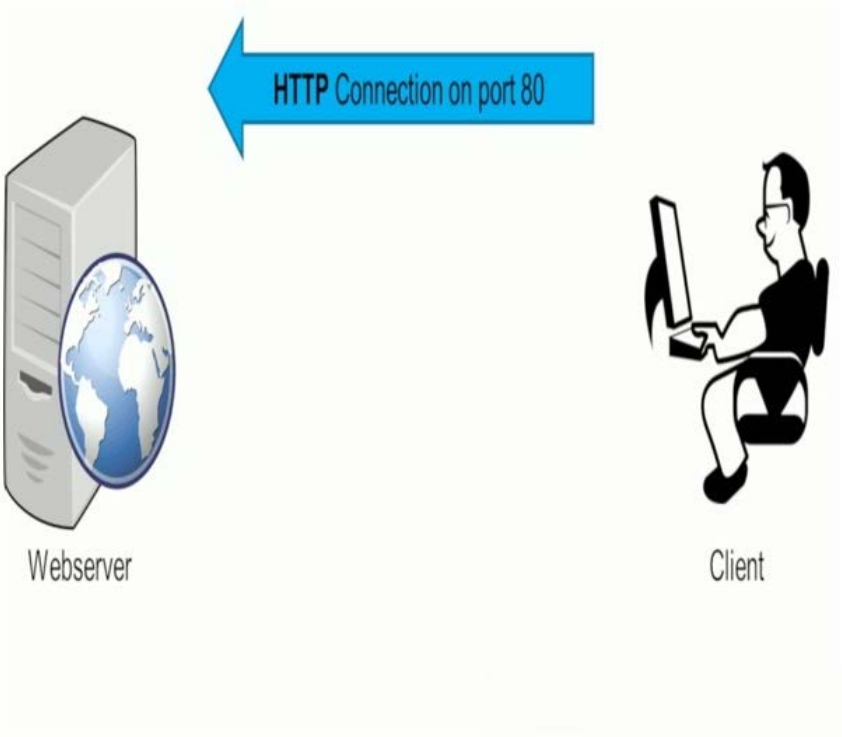


Figura 2.25 Sessão HTTPS fonte

Se digitar www.google.com na barra de endereços de um navegador da Web, o navegador fará uma ligação HTTP (na porta 80) com www.google.com. Como o google.com apenas permitirá ligações HTTPS, o site solicitará que o utilizador faça uma ligação HTTPS. Em vez disso, o cliente que usa HTTPS na porta 443 religa-se novamente. Na última etapa, o Google envia o certificado.

2.6. Forçar a comunicação HTTP

Considere o cenário em que um hacker está algures entre a comunicação do servidor da web e o cliente. O hacker poderá ler o conteúdo do tráfego da Web até o momento em que o cliente configurar a ligação HTTPS. Depois disso, todos os dados serão encriptados e não serão mais legíveis pelo hacker. Anteriormente, afirmamos que isto pode ser contornado, forçando o cliente a continuar a comunicar via HTTP. SSLStrip é a ferramenta que usamos para conseguir isso.

SSLStrip, criado por Moxie Marlinspike, irá transparentemente roubar o tráfego HTTP numa rede, observará os links e redirecionamentos HTTPS e mapeará esses links em links HTTP parecidos ou em links HTTPS homograficamente semelhantes. Vamos ver a configuração da sessão HTTPS quando o hacker utiliza SSLStrip entre o cliente e o servidor da web.

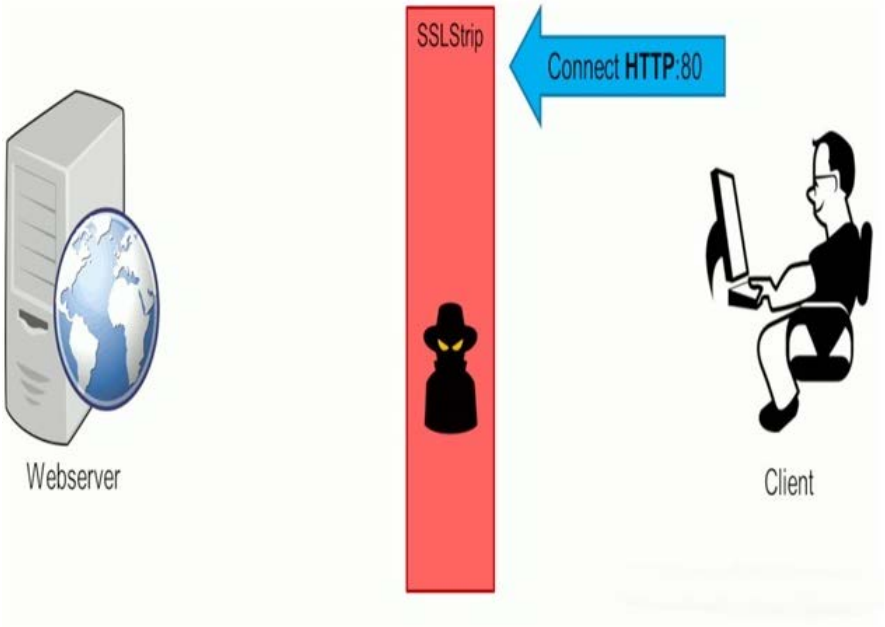


Figura 2.26: SSLStrip fonte

Como antes, o cliente digita www.google.com no navegador da Web, que tentará configurar uma conexão HTTP com o site. Agora, com o SSL Strip no meio, essa ligação é encaminhada para o destino pretendido. No entanto, em vez de todo o processo de redirecionamento HTTPS ser realizado do lado do cliente, o SSL Strip executa-o na máquina do hacker. Após a configuração da conexão HTTPS, o SS LStrip retornará um **HTTP**-OK para o cliente. O navegador do cliente considera isso aceitável, pois nunca viu o redirecionamento HTTPS e continuará a comunicar via HTTP; um formato que o hacker pode ler sem esforço.

Transporte de Segurança estrito HTTP

A ativação da segurança estrita de transporte HTTP (HSTS) para o seu site informará o navegador a comunicar sempre através de HTTPS. Isto é feito por meio de um cabeçalho de resposta HSTS especial. Simplificando, o navegador mantém uma lista de sites dos quais recebeu esse cabeçalho. Para esses sites, o navegador fará imediatamente uma ligação HTTPS, independentemente de como o usutilzar tentou ligar-se. Digitar www.google.com não resultará no processo de redirecionamento HTTP-HTTPS, mas chama imediatamente o www.google.com. Isso impedirá que os utilizadores façam a ligação HTTP em primeiro lugar, evitando que o SSLStrip execute esse truque. Ou seja, se o seu navegador suportar.

A primeira visita de um cliente a um site ainda pode ser feita via HTTP e um invasor pode retirar o cabeçalho do HSTS da resposta. É por isso que a maioria dos browsers modernos tem uma lista pré-carregada de sites HSTS. Mais sobre prevenção no capítulo final.

3. Ataques de dicionário e phishing

Um **ataque de dicionário** é um ataque à palavra passe que tenta determinar uma senha tentando palavras de uma lista predefinida, ou dicionário, de senhas possíveis.

Um ataque de dicionário é o ataque mais simples e rápido de descodificar uma senha. Use um arquivo que contenha palavras, frases ou senhas comuns que possam ter sido usadas por alguém como senha. Os hackers têm acesso a bancos de dados com 100.000 (ou mais) senhas principais ou podem criar e encontrar arquivos maiores. O ataque faz hash nessas senhas e compara o hash com a senha que ele deseja decifrar. Este é um método mais rápido que outros.

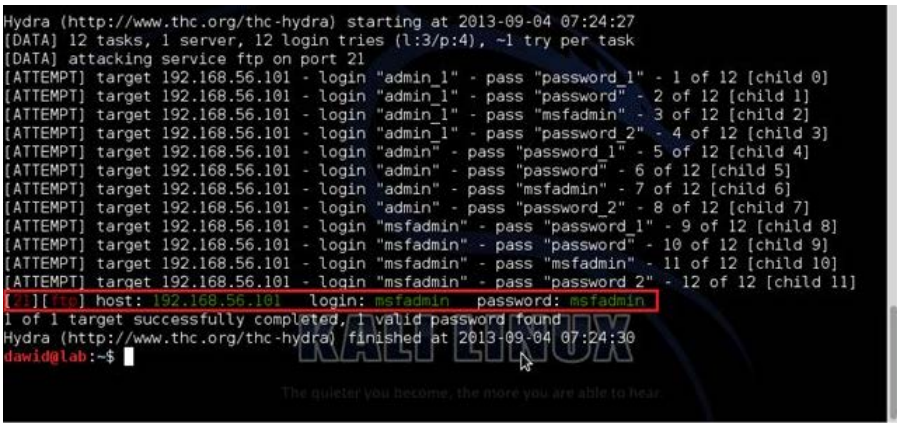


Figura 2.27: Um ataque do tipo dicionário

Phishing

Phishing é um exemplo de abordagem de engenharia social usada para obter informações confidenciais do utilizador (dados de identificação pessoal), normalmente nomes de utilizador, palavras passe, números de cartão de crédito, informações de contas bancárias, ou outros dados importantes para utilizar ou vender as informações roubadas, que serão usadas para enganar os sistemas. As tentativas de phishing geralmente começam com um e-mail na tentativa de obter informações confidenciais por meio de alguma interação do utilizador, como clicar num link malicioso ou fazer o download de um anexo infectado.

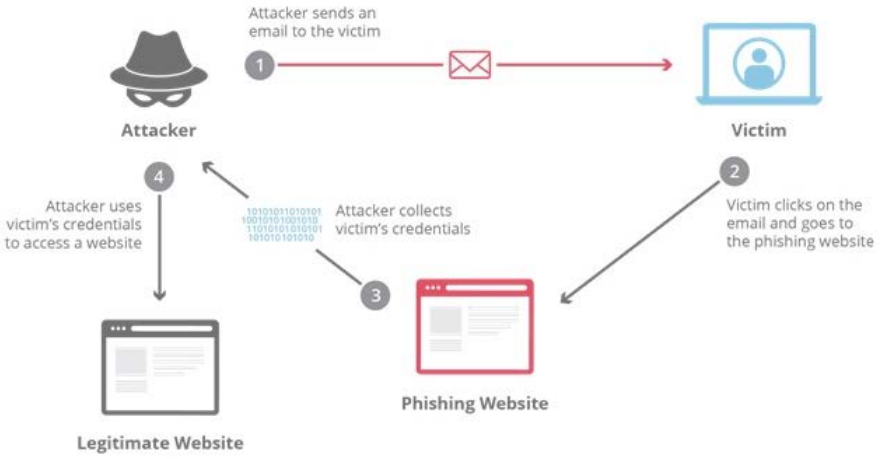


Figura 2.28 Ataque do tipo phishing fonte

Para combater ataques de phishing, as organizações e empresas devem fornecer aos seus funcionários maneiras de os identificar e de os combater. Os ataques de phishing mais comuns são e-mails, arquivos de anexos de vírus e links de vírus que propagam o vírus e diminuem a largura de banda da ligação. Os invasores são atualizados constantemente sobre novos ataques; portanto, tem de fornecer aos funcionários informações sobre estas questões para evitar esses ataques.

4. Ataque de injeção SQL

Injeção SQL (SQLi) é um tipo de ataque de injeção que possibilita a execução de instruções SQL mal-intencionadas. Essas instruções controlam um servidor de banco de dados atrás de uma aplicação da web. Os invasores podem usar vulnerabilidades de injeção SQL para ignorar as medidas de segurança da aplicação. Podem executar a autenticação e a autorização de uma página da Web ou aplicação Web e recuperar o conteúdo de todo o banco de dados SQL. Também podem usar o SQL Injection para adicionar, modificar e excluir registos no banco de dados.

Uma vulnerabilidade de injeção de SQL pode afetar qualquer site ou aplicação da Web que utilize um banco de dados SQL como **MySQL, Oracle, SQL Server ou outros**. Os criminosos podem usá-lo para obter acesso não autorizado aos seus dados confidenciais: informações do cliente, dados pessoais, segredos comerciais, propriedade intelectual e muito mais. Os ataques de injeção de SQL são uma das mais antigas, prevalentes e mais perigosas vulnerabilidades de aplicativos da web. Geralmente, permite que um invasor visualize dados que normalmente não seria capaz de recuperar. Podem ser dados pertencentes a outros utilizadores ou quaisquer outros dados que a própria aplicação possa aceder. Em muitos casos, um invasor pode **modificar** ou **excluir** esses dados, causando alterações persistentes no conteúdo, ou no comportamento da aplicação.

Em algumas situações, um invasor pode escalar um ataque de injeção SQL para comprometer o servidor subjacente ou outra infraestrutura de back-end ou executar um ataque de recusa de serviço.

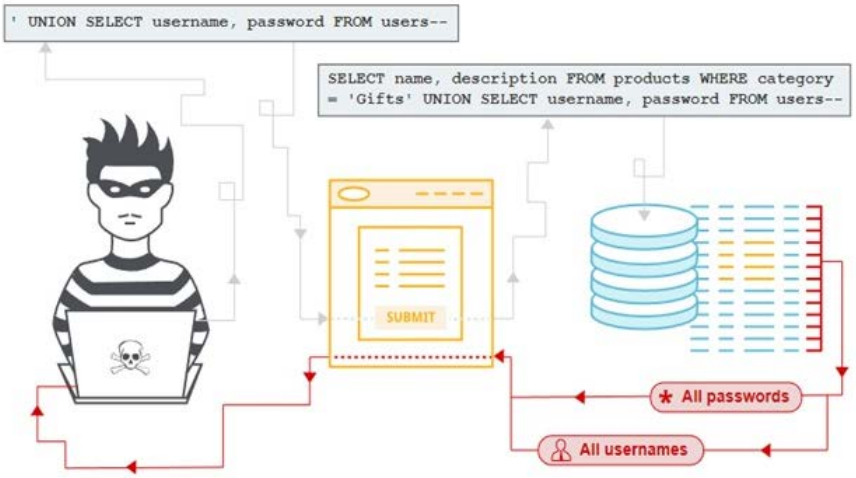


Figura 2.29 SQL injection fonte

4.1. Como funcionam os ataques de injeção SQL?

Fatores específicos de bases de dados

Alguns recursos principais da linguagem SQL são implementados da mesma maneira em plataformas populares de bases de dados, sendo que muitas estratégias de detectar e explorar vulnerabilidades de injeção SQL funcionam de maneira idêntica em diferentes tipos de bases de dados.

No entanto, também existem muitas diferenças entre bases de dados comuns. Isto significa que algumas técnicas para detectar e explorar a injeção de SQL funcionam de maneira diferente em plataformas diferentes.

O que podem fazer os ataques de injeção SQL?

Há muitas coisas que um invasor pode fazer ao explorar uma injeção de SQL num website vulnerável. Ao alavancar uma vulnerabilidade de injeção de SQL, nas circunstâncias corretas, um invasor pode fazer o seguinte:

- Ignorar os mecanismos de autorização de uma aplicação Web e extrair informações confidenciais
- Controlar facilmente o comportamento da aplicação com base na informação da base de dados
- Inserir outro código malicioso a ser executado quando os utilizadores acederem à aplicação
- Adicionar, modificar e excluir dados, corrompendo a base de dados e tornando a aplicação inacessível ou inutilizável
- Enumerar os detalhes de autenticação de um utilizador registado num site e utilizar os dados em ataques noutros sites

Figura 2.30 Ataque do tipo SQL injection fonte

O seguinte pode resultar da injeção de SQL:

- Piratear a conta de outra pessoa.
- Roubar e copiar dados confidenciais do site ou sistema.
- Alterar os dados confidenciais do sistema.

- Excluir dados confidenciais do sistema.
- O utilizador pode efetuar login na aplicação como outro utilizador, até mesmo como administrador.
- O utilizador pode visualizar informações privadas pertencentes a outros utilizadores, por exemplo, detalhes dos perfis de outros utilizadores, detalhes das suas transações, etc..
- O utilizador pode alterar as informações de configuração da aplicação e os dados dos outros utilizadores.
- O utilizador pode modificar a estrutura do banco de dados; até excluir tabelas no banco de dados da aplicação.
- O utilizador pode assumir o controlo do servidor do banco de dados e executar comandos à vontade.

4.2. Como podem ser evitados os ataques de injeção SQL?

Figura 2.31 Prevenção SQL fonte

Existem várias maneiras de lidar com ataques de injeção de SQL, para que esteja preparado e evite possíveis danos. Algumas formas são:

- Descobrir as vulnerabilidades de injeção SQL com as várias técnicas disponíveis para este ataque
- Reparar vulnerabilidades de injeção SQL, utilizando consultas parametrizadas. O banco de dados tratá-los-á sempre como dados, e não como parte de um comando SQL.
- Corrigir as vulnerabilidades de injeção SQL usando caracteres de escape para que os caracteres especiais sejam ignorados.
- Reduzir o impacto das vulnerabilidades de injeção SQL, aplicando o mínimo de privilégios no banco de dados, desta forma cada componente de software de uma aplicação pode aceder e afetar apenas os recursos necessários.
- Usar um WAF (Web Application Firewall) para aplicativos da Web que acedam a bancos de dados. Isso pode ajudar a identificar tentativas de injeção de SQL e, às vezes, impedir que as tentativas de injeção de SQL atinjam a aplicação.

5. Ataque Modbus

O Modbus é um protocolo de comunicação industrial muito difundido, com uma especificação disponível ao público, com base numa arquitetura master/slave. Atualmente, não há restrições extensivas no momento em que os blocos de dados podem ser geridos num sistema industrial; implementar isso seria simples e exigiria pouco desenvolvimento. Atualmente, existem duas implementações: Série Modbus (com modos de operação ASCII e RTU) e Modbus / TCP.

Fraquezas do protocolo

No Modbus, o modo de operação dos elementos slave consiste em responder sempre aos pacotes que recebem. A ferramenta Modscan aproveita este recurso, dirigindo solicitações TCP (portanto, disponíveis apenas para implementações Modbus/TCP) para a porta Modbus padrão 502 e, assim, descobrindo os slave ligados à rede, como exemplificado na imagem na Figura 2.32.

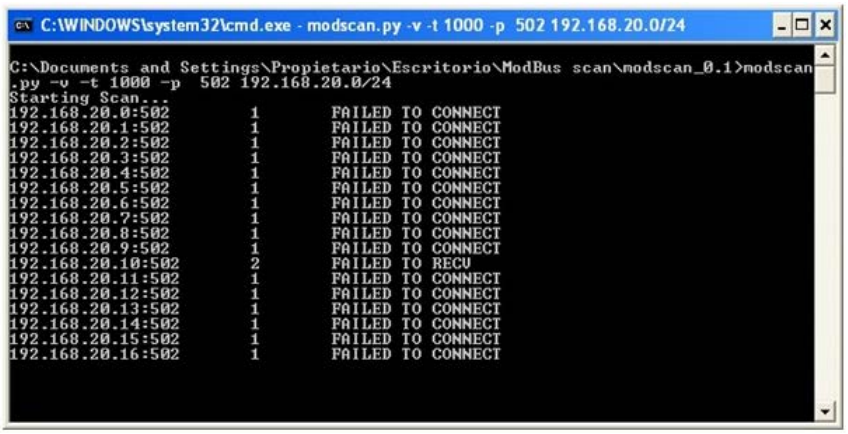


Figura 2.32 Descobrindo os IPs dos slaves Modbus com o Modscan

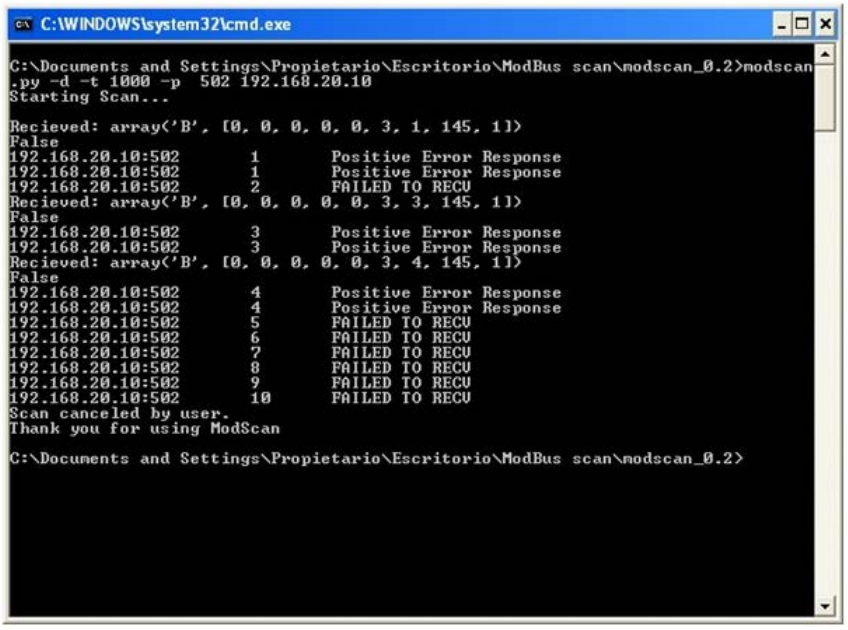


Figura 2.33 Ajustando a busca de slaves e a identificação dos IDs do Modbus

Uma vez identificados os slaves, é fácil capturar o tráfego com qualquer ferramenta desenhada para capturar o tráfego da rede. A análise de captura mostra que as comunicações não são criptografadas, o que significa que é possível identificar e analisar diretamente as informações fornecidas e o modo de operação. A imagem a seguir (Figura 2.34) mostra uma captura de tráfego com uma análise do fluxo.

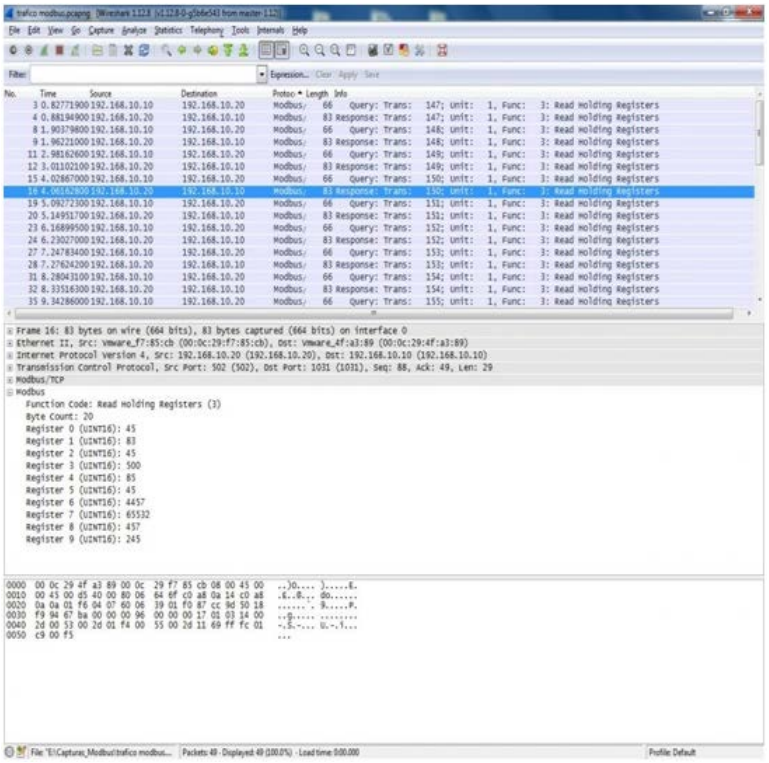


Figura 2.34 Analisar tráfego

5.1. Medidas de prevenção

Os pontos fracos do Modbus estão enraizados na sua especificação, o que significa que são intrínsecos ao protocolo; Como não são previstas alterações na especificação, é necessário introduzir elementos de segurança adicionais para ajudar a atenuar as suas falhas de segurança.

Passando dessa opção, que é a mais simples, a primeira medida a considerar é a adoção de uma estratégia de encriptação para comunicações. A encriptação de comunicações impedirá que as informações sejam analisadas em trânsito, caso o tráfego seja capturado.

Os dispositivos que implementam esse protocolo geralmente não são capazes de encriptar as comunicações e, portanto, devem usar ferramentas externas, que podem encriptar e desencriptar as informações executadas pelo cabo Ethernet.

Embora essa solução seja eficaz, na prática é difícil, pois o uso de ferramentas de encriptação traz problemas de gestão e de distribuição de palavras passe; além disso, a encriptação e a desencriptação de informações devem ser permitidas por todos os equipamentos industriais a serem usados pelo protocolo Modbus.

Portanto, para controlar o tráfego entre slaves e o master, os firewalls são a solução mais popular. Os firewalls convencionais permitem o controlo de tráfego no nível da rede, o que significa que os endereços do master e dos slaves podem ser estabelecidos como autoridades, evitando assim certos tipos de ataques de representação. Os firewalls de aplicações permitem a inspeção, inclusive para a secção de dados do fluxo.

Há Modbusfw , um módulo para iptables que filtra o tráfego no nível da camada da aplicação para proteger redes, usando o protocolo Modbus/TCP. Permite a filtragem de pacotes de tráfego Modbus, identificando-os, usando o ID do slave, o código da função, o tamanho do pacote ou o número de referência. Desta forma, é possível evitar registar em equipamentos que devem receber apenas leituras ou vice-versa e filtrar o uso de códigos de função de diagnóstico (como aqueles usados em certas ferramentas de varredura da rede Modbus), etc..

Os firewalls permitem o controlo de tráfego em redes diferentes, mas é útil usá-los em conjunto com os sistemas de detecção e de prevenção de intrusões (IDS/IPS), para detectar outros tipos de ações.

Para o Snort IDS e para todos os que estão nele, há uma extensão para interpretar o protocolo Modbus. É possível definir regulamentos de controlo de tráfego para o Modbus com base em valores que devem conter diferentes bytes de dados num fluxo Modbus/TCP.

O uso de sistemas IDS/IPS para supervisionar o protocolo Modbus permite o reconhecimento de funções não permitidas e o reconhecimento de quando pacotes de dados são enviados de endereços IP não controlados, ajudando, por exemplo, a detetar possíveis ataques de DoS.

2.4 Lei dos Serviços da Sociedade da Informação e do Comércio Eletrónico

Description

Lei dos Serviços da Sociedade da Informação e do Comércio Eletrónico

Table of contents

1. Lei dos Serviços da Sociedade da Informação e do Comércio Eletrónico

1. Lei dos Serviços da Sociedade da Informação e do Comércio Eletrónico

Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno ("Directiva sobre comércio electrónico").

Alguns parágrafos da lei:

- · Com o propósito de garantir a segurança jurídica e a confiança do consumidor, é essencial que a presente directiva estabeleça um quadro geral claro, que abranja certos aspectos legais do comércio electrónico no mercado interno.
- · (9) A livre circulação dos serviços da sociedade da informação pode, em muitos casos, constituir um reflexo específico no direito comunitário de um princípio mais geral, designadamente o da liberdade de expressão, consagrado no n.o 1 do artigo 10.o da Convenção para a protecção dos Direitos da Humanidade e das liberdades fundamentais, ratificada por todos os Estados-Membros. Por esta razão, as directivas que cobrem a prestação de serviços da sociedade da informação devem assegurar que essa actividade possa ser empreendida livremente, à luz daquele preceito, apenas se subordinando às restrições fixadas no n.o 2 daquele artigo e no n.o 1 do artigo 46.o do Tratado. A presente directiva não tem por objectivo afectar as normas e princípios nacionais fundamentais respeitantes à liberdade de expressão.

Objetivo da Lei Serviços da Sociedade da Informação

(1) Esta Lei fornece os requisitos para os prestadores de serviços da sociedade da informação, a organização da supervisão e a responsabilidade por violação desta Lei.

mais informações sobre a lei http://unpan1.un.org/intradoc/groups/public/documents/un-kmb/unpan041622~1.htm

Comércio eletrónico - regras padrão da UE

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=LEGISSUM%3Al24204

A Diretiva Comércio Eletrónico (Diretiva Comércio Eletrônico 2000/31 / CE), adotada em 2000, estabelece uma estrutura de mercado interno para o comércio eletrónico que fornece segurança jurídica para empresas e consumidores.

Objetivo da Diretiva Comércio Eletrónico

A diretiva foi introduzida para esclarecer e harmonizar as regras dos negócios on-line em toda a Europa. O objetivo da Diretiva é, em última análise, incentivar a maior utilização do comércio eletrónico, derrubando barreiras existentes na Europa, e aumentar a confiança do consumidor, esclarecendo os direitos e obrigações dos consumidores e das empresas.

Âmbito dos Regulamentos de Comércio Eletrónico (Diretiva CE) 2002

Os Regulamentos do Comércio Eletrónico (Diretiva da CE) de 2002, que entraram em vigor em 21 de agosto de 2002, transpõem os principais requisitos da Diretiva de Comércio Eletrónico para a lei do Reino Unido.

O regulamento aplica-se aos "serviços da sociedade da informação". "São definidos como qualquer serviço normalmente prestado mediante remuneração à distância, por meio de equipamentos eletrónicos para processamento (incluindo compressão digital) e armazenamento de dados, mediante solicitação individual de um destinatário de um serviço."

Isto inclui a maioria dos tipos de serviços on-line e de informações, como:

- Publicidade de bens ou serviços on-line (por exemplo, via internet, e-mail, televisão interativa ou telemóvel);
- Venda de bens ou serviços na Internet ou por e-mail, independentemente de os bens ou serviços serem entregues eletronicamente;
- Transmissão ou armazenamento de conteúdo eletrónico ou fornecimento do acesso a uma rede de comunicações.

A lei oficial e completa:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Recomendações da União Europeia para combater ataques cibernautas. Aplicam-se as seguintes diretrizes:

- **Estudo da ENISA sobre "CIBERSEGURANÇA DA INDÚSTRIA 4.0: DESAFIOS & RECOMENDAÇÕES, maio 2019":**

https://www.enisa.europa.eu/publications/industry- 4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

A apropriação das propostas de nível significativo propostas pela ENISA visam o aprimoramento da cibersegurança da Indústria 4.0 sobre a União Europeia e o alicerce do trabalho futuro relevante, além de servir de base para desenvolvimentos futuros. Neste breve artigo, a ENISA busca uma maneira holística e abrangente de lidar com os problemas identificados a nível da cibersegurança no setor 4.0, na qual dificuldades e propostas estão relacionadas com uma das classes a seguir: Pessoas, processos e tecnologias.

- **Este documento tem como objetivo "Diretrizes e melhores práticas de segurança cibernauta para serviços de emergência, junho de 2018"**: https://eena.org/wp-content/uploads/2018/11/Cybersecurity-Guidelines-and-Best-Practices-for-Emergency-Services.pdf

  Este documento da EENA (Associação Europeia de Números de Emergência) espera expandir a consciencialização entre as associações de Segurança Pública sobre os efeitos identificados nas vulnerabilidades, riscos e ameaças cibernautas e oferece algumas sugestões para a sua mitigação. A segurança cibernauta, para o propósito deste documento, refere-se às tecnologias, processos e práticas projetadas para proteger utilizadores, redes, computadores, programas e dados contra ataques, danos ou acesso não autorizado.

- **ISACA, "Auditoria de segurança cibernauta"**: https://m.isaca.org/About-ISACA/advocacy

/Documents/CyberSecurityAudit_mis_Eng_1017.pdf

  Este guia concentra-se em três partes: análise de gestão, avaliações de risco e auditorias dos controlos de segurança cibernauta. Além disso, inclui questões base de segurança e controlo para segurança cibernauta, controlos e ameaças para segurança cibernauta.

- **Este estudo da ENISA tem como objetivo as "Boas Práticas de Segurança da Internet das Coisas no contexto da Manufatura Inteligente, novembro de 2018":** https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

  Este estudo da ENISA visa abordar os desafios de segurança e privacidade relacionados com a evolução de sistemas e serviços industriais despoletados pela introdução de inovações de IoT. Os principais objetivos consistiram em recolher boas práticas para garantir a segurança da IoT no contexto da Indústria 4.0/Smart Manufacturing, mapeando os desafios relevantes de segurança e privacidade, ameaças, riscos e cenários de ataque.

- **Relatório Interno do NIST 8228 (Rascunho) "Considerações para gerenciar riscos de cibersegurança e privacidade na Internet das Coisas (IoT) em, setembro 2019"**: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

  O objetivo deste artigo é ajudar as empresas a apreender e manipular melhor os perigos de segurança cibernética e privacidade associados aos dispositivos da Internet das Coisas (IoT) durante os seus ciclos de vida. Além disso, o texto versa sobre Considerações Sobre Riscos de Segurança e Privacidade Cibernauta e sobre desafios da Mitigação de Riscos em Segurança e Privacidade para Dispositivos IoT.

- **"Código de Práticas de Segurança da Internet das Coisas do Consumidor, outubro de 2018" do Departamento para o Digital, Cultura, Média e Desporto**: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867

/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

  O Código de Práticas do Governo para a Segurança da Internet das Coisas (IoT) para manufatura, com orientação para consumidores de dispositivos inteligentes em casa.

Exemplos Práticos

Inserção de SQL

Existem ferramentas automatizadas para verificar se um website é vulnerável.

Essas ferramentas incluem:

- **SQLMap**
- **Havij**

Um link de demonstração para praticar.

http://testphp.vulnweb.com/artists.php?artist=1

A primeira coisa que fazemos é colocar uma citação simples no final do url.

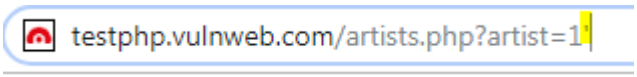


Figura 1 Verificando a inserção de SQL

e obtemos o erro.

Portanto, percebemos que o website é vulnerável a ataques de inserção de SQL.

Demonstração detalhada para entender melhor o ataque.

Demonstração SQL

Um ataque de dicionário

Um ataque de dicionário é o ataque mais simples e rápido para descodificar uma palavra passe.

Os atacantes podem criar os seus próprios dicionários feitos com passwords ou podem fazer download de palavras passe existentes.

Criar a lista de palavras com Crunch - Kali linux

```
root@kali:~# crunch 6 8 1234567890 -o /root/numericwordlist.lst
Crunch will now generate the following amount of data: 987000000 bytes
941 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 111000000
```

Figura 2 Exemplo

Onde o primeiro número (6) é o menor comprimento da palavra e o segundo (8) é o comprimento da palavra mais longa e os caracteres são de 0 a 9.

Que comando precisamos para caracteres minúsculos a-z?

RESPOSTA: crunch68abcdefghiklmnopqrstuvwxyz-o/root/loweralpha.lst

Um exemplo de serviço de cracking (porta 22)

```
C:\hydra>hydra -l root -P sshcrack.txt 192.168.1.31 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-09 14:12:
18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:0), ~7 tr
y per task
[DATA] attacking ssh://192.168.1.31:22/
[22][ssh] host: 192.168.1.31   login: root   password: toor
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-09 14:12:
20
```

Figura 3 SSH cracking do Windows

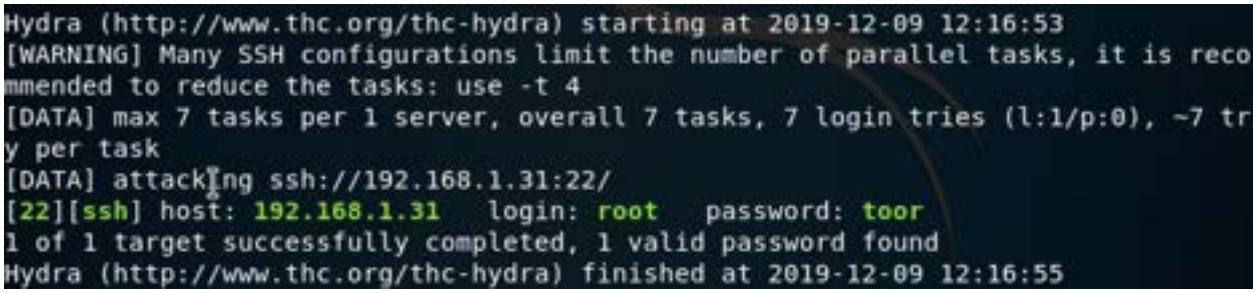


Figura 4 SSH cracking do Linux

Tente fazer o mesmo usando uma lista de palavras pronta chamada "rockyou"! (Rock you download link)

Lembretes!

1) Palavras passe fortes
A palavra passe deve ter pelo menos 12 caracteres (no mínimo), com a combinação de letras, números e símbolos especiais. Algumas letras devem ser maiúsculas e outras minúsculas.

2) Palavra passe única
Deve ter-se uma palavra passe única para diferentes contas. Nunca use a mesma palavra passe para todas as suas contas.

3) Password caleidoscópica
A sua password deve ser atualizada pelo menos de três em três meses. Nunca reutilize as suas passwords antigas.

Ataque de DOS

Ataque dos DOS: Um ataque Denial-of-Service (DoS) é um ataque que tem por objetivo desligar uma máquina ou rede, tornando-a inacessível aos seus utilizadores.

O hping3 é uma ferramenta de rede capaz de enviar pacotes TCP/IP personalizados e exibir respostas de destino, como o programa ping faz com respostas de ICMP. O hping3 lida com fragmentação, com o conjunto e tamanho de pacotes arbitrários e pode ser utilizado para transferir arquivos codificados sob protocolos suportados.

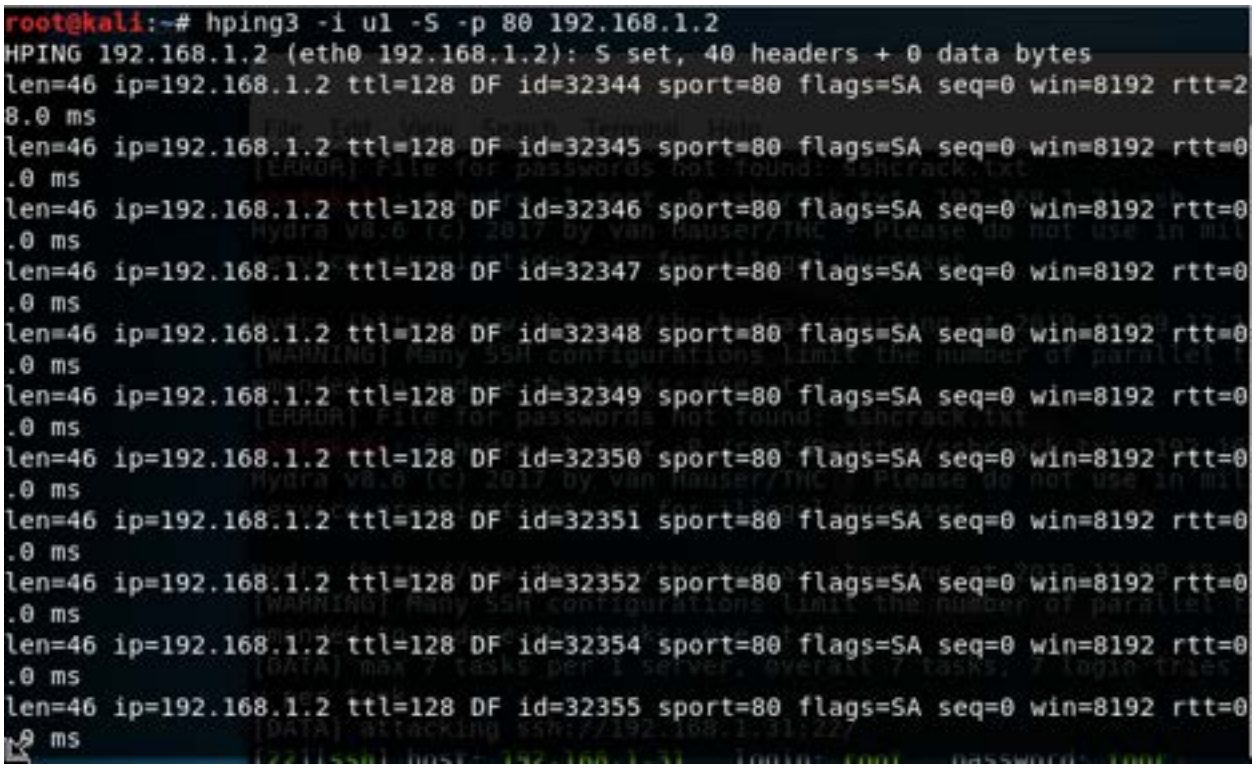


Figura 5 hping3 em ação

em que:i - espera por intervalo, - u1- 1 microssegundo -S - Pacote Syn -p - número da porta

Atacamos a nossa rede local

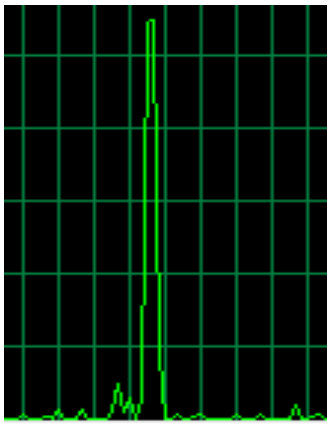


Figura 6 Ataque à rede na prática, após 15 a 20 segundos

Figura 7 Após 1-2 minutos

Como é possível observar, a atividade da rede aumentou significativamente quando o ataque foi bem-sucedido.

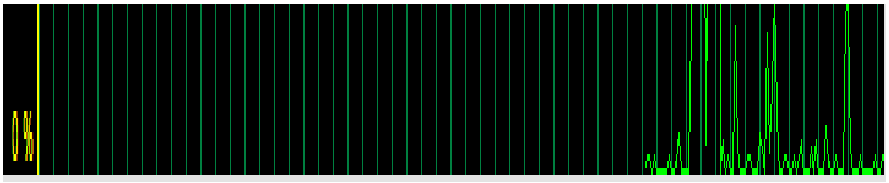


Figura 8 Fluxo normal da rede

No.	Time	Source	Destination	Protocol	Length	Info
3635…	10.305082	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5758 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305087	192.168.1.2	192.168.1.31	TCP	58	80 → 5758 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305119	192.168.1.31	192.168.1.2	TCP	60	5758 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305147	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5759 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305152	192.168.1.2	192.168.1.31	TCP	58	80 → 5759 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305184	192.168.1.31	192.168.1.2	TCP	60	5759 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305223	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5760 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305229	192.168.1.2	192.168.1.31	TCP	58	80 → 5760 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305261	192.168.1.31	192.168.1.2	TCP	60	5760 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305289	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5761 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305294	192.168.1.2	192.168.1.31	TCP	58	80 → 5761 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305326	192.168.1.31	192.168.1.2	TCP	60	5761 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305354	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5762 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305360	192.168.1.2	192.168.1.31	TCP	58	80 → 5762 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305390	192.168.1.31	192.168.1.2	TCP	60	5762 → 80 [RST] Seq=1 Win=0 Len=0

Figura 9 O Wireshark capturou os pacotes atacados

Pode ver-se claramente que a nossa máquina está a enviar pacotes SYN (ataque DoS) continuamente para a máquina de destino.

E-mail de phishing

Em geral, phishing é quando alguém tenta roubar informações pessoais on-line de várias maneiras. Geralmente, ocorre por e-mail e o remetente real não é quem parece.

Vejamos um exemplo real

E-mail de phishing clássico

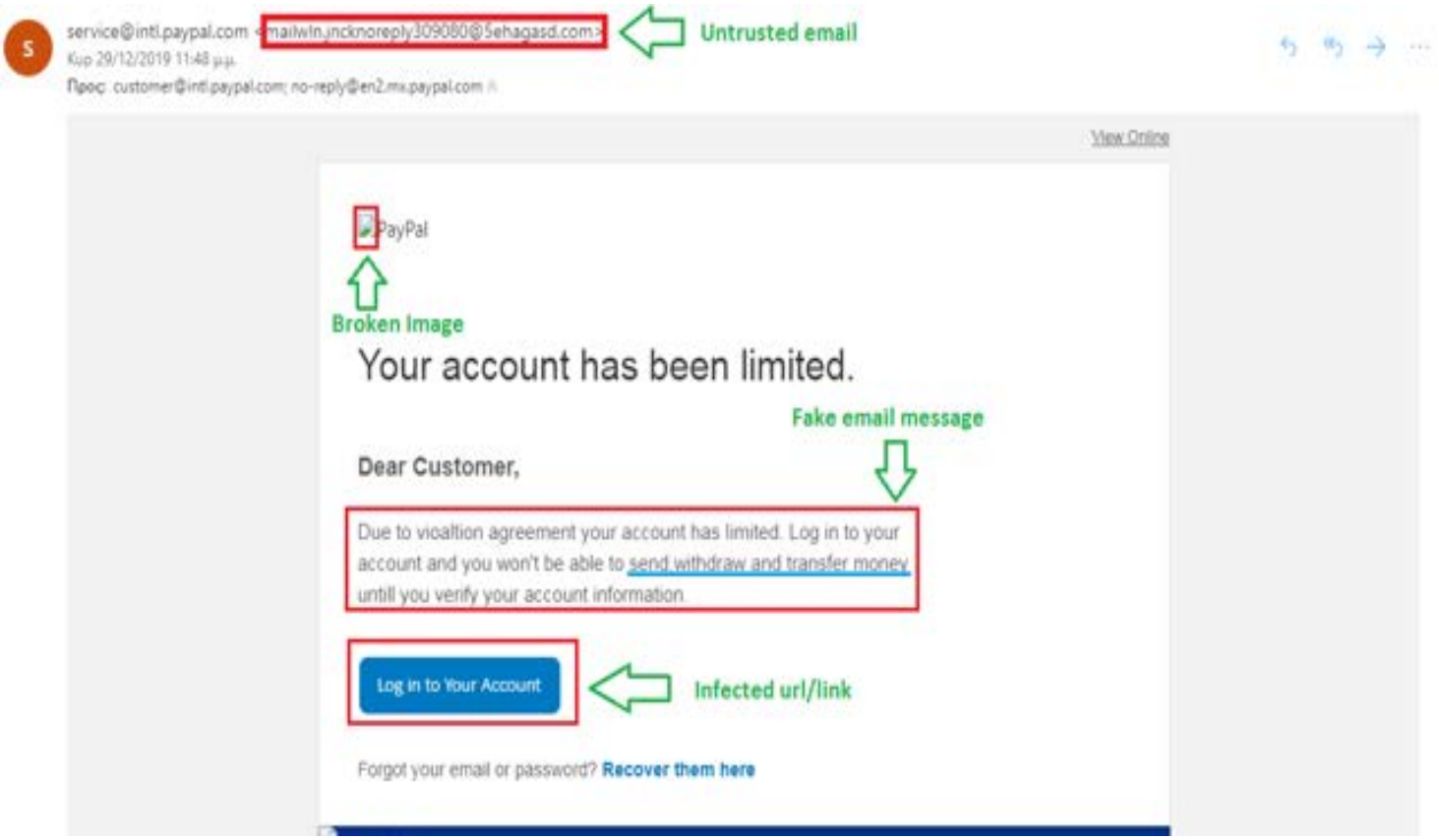


Figura 10 Exemplo de email de phishing do Fakepaypal

Existem também outras categorias de phishing por email.

Os básicos são:

- Anexos infetados (extensões de arquivo .JS, .DOC, .HTML).
- Macros com Payloads em documentos do Word.
- Exploits nos Media Sociais com o propósito de instalar extensões maliciosas do navegador.
- Ataques de phishing do LinkedIn (para roubar credenciais do utilizador).

Uma boa demonstração online, para distinguir se um email é real ou não (phishing) é a seguinte:

Demonstração de phishing

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 3

Confidencialidade, integridade, disponibilidade em ambientes industriais

3.1 Disponibilidade

Description

Disponibilidade

Table of contents

1. Continuidade de Negócio

2. Grau de disponibilidade

3. Tolerância a falhas

4. Prevenção de Falhas

5. Deteção de Falhas

6. Plano de Continuidade de Negócios

7. Avaliação de Risco

8. Recuperação de Desastre

9. Plano de Contingência

10. Política de Segurança

1. Continuidade de Negócio

A continuidade dos negócios depende de muitos fatores. No campo da administração de sistemas, é imperativo preocupar-se com o impacto que a infraestrutura da tecnologia tem nos negócios.

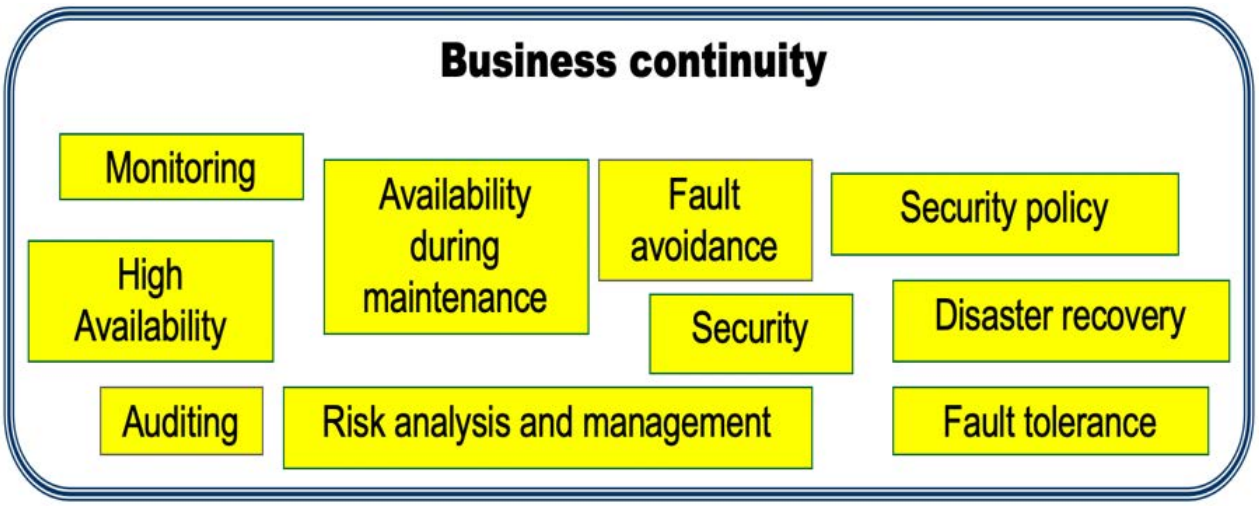


Figura 3.1. Continuidade de negócio

A infraestrutura tecnológica deve garantir a continuidade dos negócios em execução sem interrupção, dentro dos **parâmetros** previstos para os negócios suportados por essa infraestrutura.

É considerado um **sistema seguro (infraestrutura tecnológica segura)**, que é mantido em funcionamento dentro dos parâmetros qualitativos e quantitativos esperados (**SLA** - Contrato de nível de serviço). Qualquer desvio nesses parâmetros é considerado uma falha.

Esses parâmetros envolvem a tríade de segurança do computador: **Confidencialidade**, **Integridade** e **Disponibilidade**.

Planear um sistema seguro que garanta a continuidade dos negócios envolve a ponderação dos **custos** e **benefícios**, para se **obter uma probabilidade aceitável de falhas.**

Não há sistemas totalmente seguros até o ponto em que haja garantias totais de que uma falha nunca ocorra (probabilidade de falha de 0%).

Embora a probabilidade de falha seja um dado útil, o MTBF - Tempo Médio Entre Falhas é comumente usado, o que indica o tempo médio decorrido entre falhas, geralmente expresso em horas.

2. Grau de disponibilidade

A disponibilidade de um sistema é a razão entre a soma dos períodos em que o sistema opera sem falhas e o tempo total considerado (geralmente um ano ou um mês).

$$Availability = \frac{Operation\ time\ without\ failures}{Total\ time}$$

Figura 3.2. Disponibilidade

Exemplo: Se um servidor falhar 18 dias num ano (mais ou menos 5%) do tempo de funcionamento (um ano é igual a 365 dias), Disponibilidade = (365-18)/365 = 0,95

A sua disponibilidade pode ser definida como 95%.

3. Tolerância a falhas

A Tolerância Total a Falhas garante que uma falha no componente não tenha impacto nos parâmetros funcionais.

Exemplo:RAID1.

Matriz redundante de discos independentes (RAID) é um exemplo comum de tolerância a falhas baseada em redundância. RAID 1 (Efeito Espelho), que usa uma matriz de N discos idênticos (pelo menos 2), todos contendo as mesmas informações. É capaz de suportar falhas simultâneas de discos N -1.

A tolerância a falhas geralmente é alcançada através da redundância de componentes. A substituição perfeita e instantânea do componente com falha nem sempre é possível.

Nesse caso, há uma degradação temporária dos parâmetros operacionais (*Degradação Graciosa*). Se essa degradação for significativa ou prolongada, o sistema será renomeado *Fail soft*, não *Tolerante a Falhas*.

Um sistema é chamado *Fail safe* se a falha causar indisponibilidade, mas não comprometer a sua integridade.

Exemplo: UPS sem gerador.

4. Prevenção de Falhas

A prevenção de falhas destina-se a impedir a ocorrência de falhas. Baseia-se em várias medidas de bom senso:

- Uso de componentes de qualidade comprovada

- Controle ambiental (temperatura, humidade, poeira)

- Controle de potência (estabilidade e filtragem)

- Controle de acesso físico, incluindo linhas de comunicação

- Controle de acesso remoto (firewall, autenticação)

- Prevenção e combate a incêndio

- Execução de testes antes de colocar os componentes em funcionamento

- Simplificar a administração do sistema, por exemplo, com acesso virtual

- Controlar permissões e privilégios de administração

- Divulgação da Política de Segurança e treino de utilizadores e funcionários

- Aplicação de todas as atualizações de software

- Garantias de autenticidade (mecanismos sólidos de autenticação)

- Monitorização (permite a deteção de possíveis pontos de falha)

- Controle de utilização de recursos (limitação/reserva). Ex.: CPU; RAM; DISCO; REDE

5. Deteção de Falhas

Não importa o quão cuidadosas sejam as medidas tomadas nas áreas de **prevenção de falhas** e de **tolerância a falhas**, elas não podem ser totalmente eliminadas, portanto, o último recurso é a **redução do impacto das falhas.**

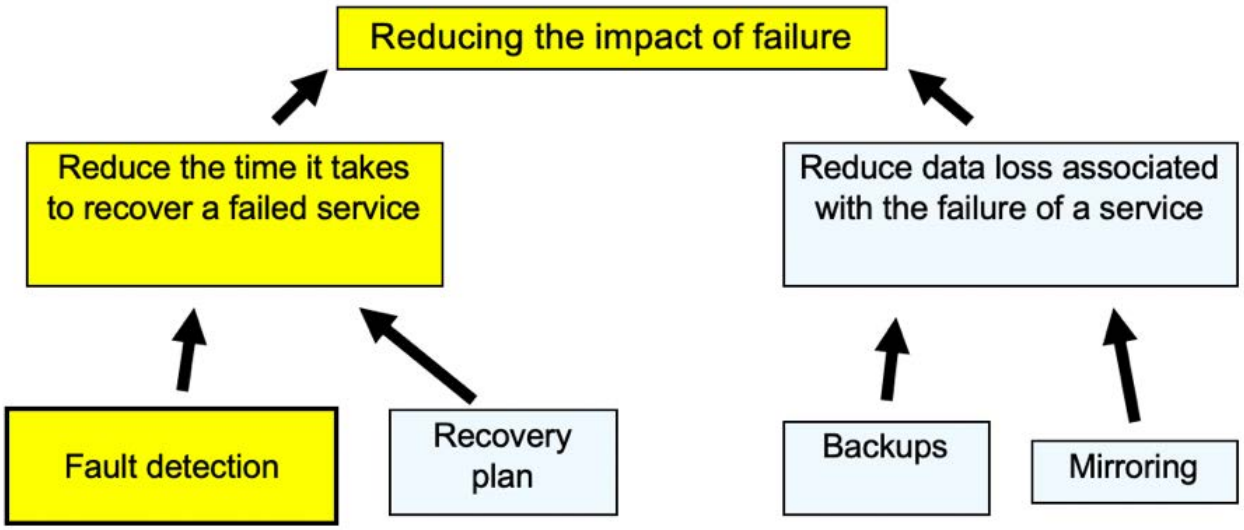


Figura 3.3. Reduzindo o impacto da falha

Para obter mais detalhes sobre o efeito espelho, consulte Secção 1.2 Tolerância a falhas.

Por várias razões, a deteção de falhas está diretamente envolvida nas três vertentes complementares de falha, como pode ser visto na Figura 3.4.

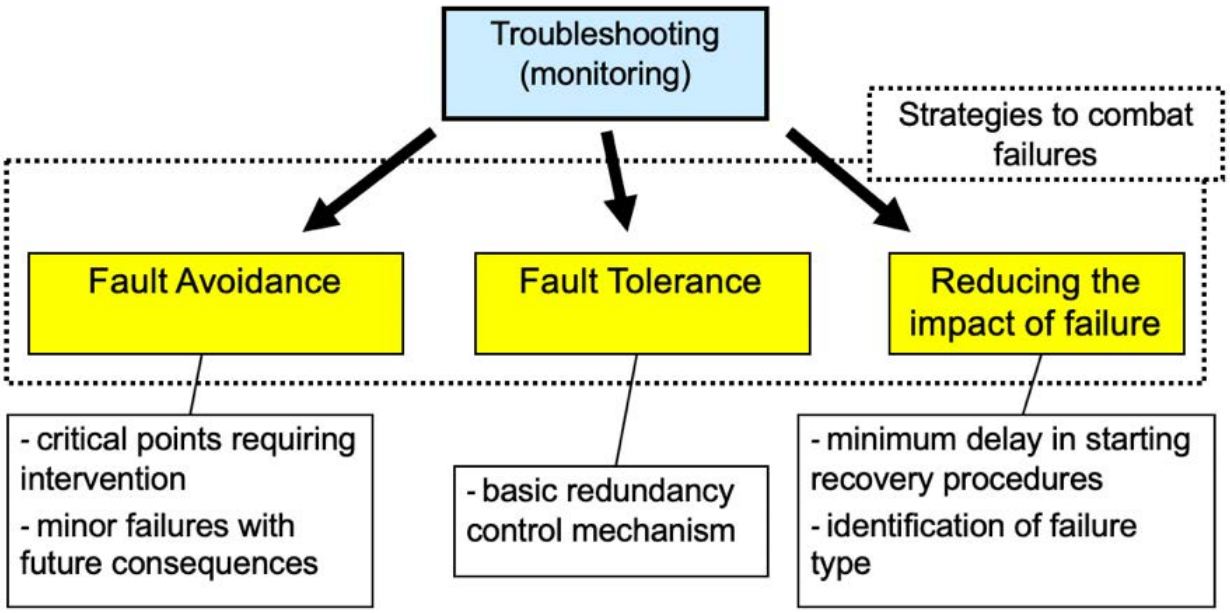


Figura 3.4. Resolução de problemas

Monitorização

A deteção de falhas deve ser automatizada 24/7. Este processo consiste na execução periódica de testes nos componentes da infraestrutura de computadores:

- Tempos de resposta do serviço

- Estado de dispositivos internos

- Medições (temperaturas, etc.)

- Anomalias nos logs de atividades

- Volumes e tipos de tráfego de rede

- Deteção de anomalias e intrusos

Depois que uma anomalia ser detetada, o sistema de monitorização deve notificar os administradores o mais rápido possível, para que o processo de recuperação possa ser acionado. Normalmente, o e-mail é usado, mas é preferível suplementar essa opção com uma forma de mensagem instantânea.

Em alguns sistemas, pode ser possível definir mecanismos de recuperação automática para algumas anomalias.

6. Plano de Continuidade de Negócios

O objetivo do Plano de Continuidade de Negócios (BCP) é definir um conjunto de condições e procedimentos destinados a garantir a continuidade dos negócios.

O Plano de Recuperação de Desastres (DRP) é um dos elementos mais importantes do BCP (às vezes confuso), mas o BCP é mais abrangente.

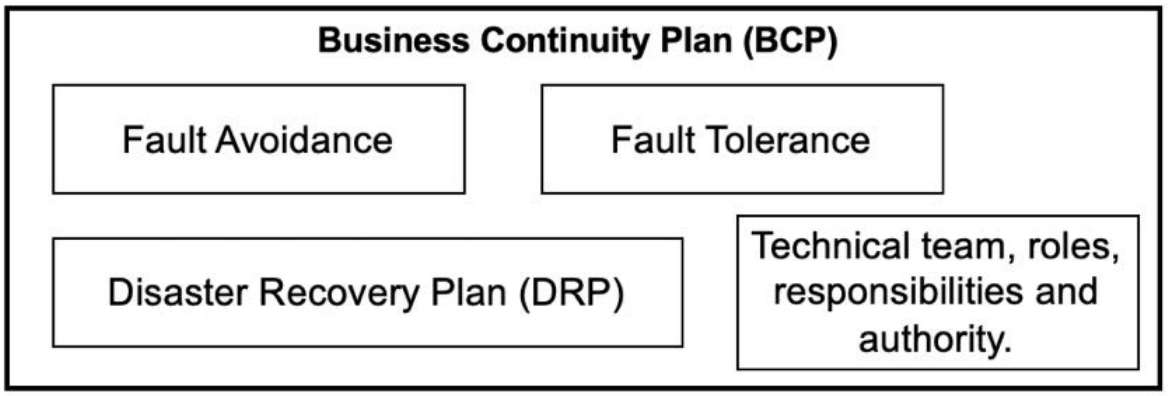


Figura 3.5. Plano de Continuidade de Negócios

Um plano de continuidade de negócios deve ser composto por:

- Prioridades e Responsabilidades
- Principais riscos e medidas de minimização
- Estratégias sugeridas
- *Backup* (cópia de segurança)
- Funções e Responsabilidades
- Condições de ativação do Plano de Continuidade de Negócios
- Processos de recuperação de emergência

7. Avaliação de Risco

A Avaliação de Risco pode ser feita usando formulários / pesquisas que, ao quantificar um conjunto de parâmetros, permitem uma quantificação abstrata do risco no domínio em análise.

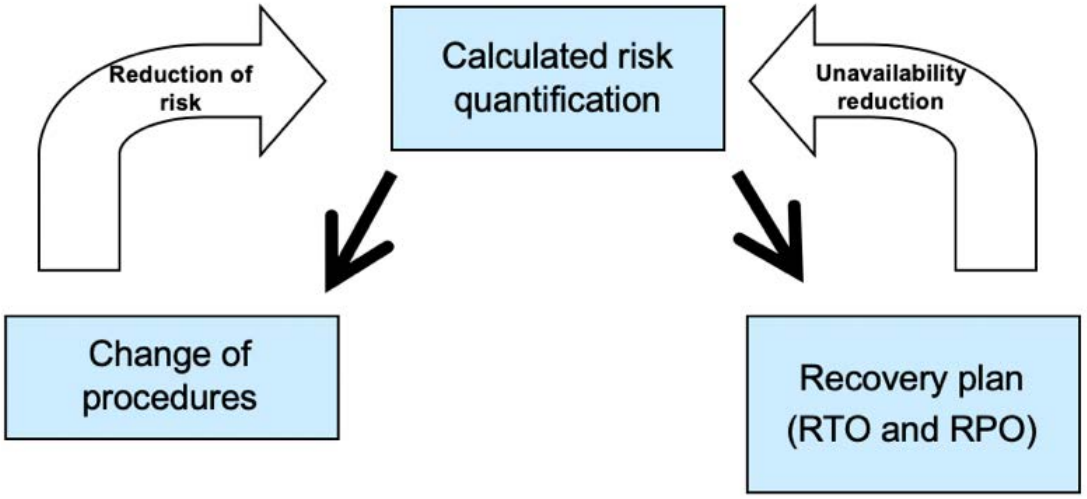


Figura 3.6. Avaliação de Risco

Objetivo do Ponto de Recuperação

Para serviços em que a perda de dados de desastre é permitida, o RPO (*Recovery Point Objective*) especifica a quantidade máxima de dados que podem ser perdidos. O RPO especifica um tempo de funcionamento pré-desastre no qual todas as alterações feitas serão perdidas.

O tempo entre os *backups* nunca pode ser maior que o RPO. Se o espelhamento for usado, o RPO será nulo ou muito próximo de zero (se o espelhamento for síncrono, o RPO será nulo).

Objetivo do Tempo de Recuperação

O objetivo do tempo de recuperação (RTO) é, portanto, o tempo máximo em que se supõe que o sistema está inoperante.

8. Recuperação de Desastre

No caso de uma falha, deve iniciar-se um processo de recuperação (mesmo que seja um componente de um sistema redundante).

O termo **recuperação de desastre** direciona-se mais para eventos de alto impacto que incluem desastres naturais catastróficos com destruição física quase total.

A recuperação de desastres é essencial para a continuidade dos negócios, o objetivo é minimizar o tempo de inatividade e a possível perda de dados.

A recuperação de desastres tem tudo a ver com preparação e planeamento:

- Efeito espelho para localização remota

- Backups regulares armazenados em local remoto

- Reserve o hardware armazenado num local remoto

- Cenários de desastre e os seus planos de recuperação.

1.7.1. Plano de recuperação de desastre

O objetivo do DRP é minimizar o tempo de inatividade e a perda de dados no caso de um desastre.

O DRP define cenários de desastre e procedimentos de recuperação para cada um deles. Isto também deve ter um tempo máximo, considerando que o sistema está inoperante.

1.7.2. Backup/Recuperação

O backup permite que, após um desastre com perda de configurações de dados ou software, seja possível recriar um sistema **com o mesmo estado de dados em que a última cópia foi feita.**

A frequência de execução dos backups deve depender da frequência das alterações nos dados e, portanto, deve ser ajustada adequadamente a cada elemento da infraestrutura.

O horário exato do backup deve ser ajustado para o horário comercial. Para cópias diárias, geralmente o horário fora do horário habitual de trabalho é o mais apropriado.

Atualmente, os discos de alta capacidade estão disponíveis a baixo custo, sempre que possível, essa solução deve ser preferida às soluções de fita magnética mais tradicionais (acesso muito lento).

Estes meios mais lentos são mais adequados para cópias de arquivo morto do que para cópias de backup.

Os meios lentos também causam problemas durante a execução das cópias, tornando a operação demorada. As operações de backup podem afetar a disponibilidade do sistema. Geralmente, os objetos como arquivos precisam de ser bloqueados para impedir que sejam feitas alterações durante a cópia.

1.7.3. Plano de backup/ Recuperação

Uma maneira de reduzir o comprimento das operações de cópia é usar **cópias incrementais** ou **cópias diferenciais. De qualquer forma, o ponto de partida é sempre uma cópia completa**.

Uma cópia incremental contém os dados que foram alterados desde a cópia incremental anterior (ou cópia completa, se for a primeira).

Uma cópia diferencial contém dados que foram alterados desde a última cópia completa.

- **Cópias Incrementais**: um grande número de cópias incrementais deve ser mantido; além do espaço ocupado, a operação de substituição torna-se muito demorada.

- Cópias diferenciais: o volume da cópia diferencial aumenta conforme as alterações são acumuladas em relação à cópia integral.

Aqui, novamente, o horário comercial deve ser respeitado, geralmente a opção é fazer uma cópia completa no domingo e cópias incrementais ou diferenciais durante os outros dias da semana (mas depende do tempo de trabalho em questão).

Um backup **nunca deve ser excluído sem que o próximo backup seja concluído com êxito**. É até desejável manter pelo menos uma cópia anterior, geralmente optando por manter várias.

O backup anterior pode ser movido para um meio de arquivo mais económico antes de se fazer uma nova cópia.

Embora o backup possa ser mantido sem manutenção num gabinete à prova de fogo, idealmente, deve estar numa **localização geográfica separada (fora do local)**.

Ainda assim, existem algumas desvantagens.

-Segurança: é necessário garantir autenticação e confidencialidade (por exemplo: VPN).

-Velocidade de acesso: afeta o tempo necessário para a cópia.

-Confiança: a recuperação só é possível se a ligação de rede estiver operacional.

9. Plano de Contingência

O plano de contingência é uma parte importante do BCP e define metodologias alternativas para manter os negócios a funcionar quando os recursos "normais" ficam indisponíveis.

Em organizações altamente dependentes de sistemas informáticos, pode ser difícil de implementar. Deve definir:

- Que tipo de desastre deve despoletar o plano de contingência.

- As etapas exatas a serem seguidas.

- As necessidades em termos de pessoal e materiais ou equipamentos.

- Que procedimentos "normais" estão previstos no plano de contingência e quais estarão indisponíveis (restrições à operação do negócio).

- Como os procedimentos executados durante o plano de contingência serão integrados no sistema após a sua recuperação.

10. Política de Segurança

A Política de Segurança é um documento que estabelece um conjunto de regras obrigatórias com o objetivo de proteger a infraestrutura e os dados.

É um elemento importante para garantir a continuidade dos negócios, especialmente no campo da prevenção de falhas.

A Política de Segurança deve ser mais abstrata do que um manual de utilizador, deve indicar "o que não pode ser feito", "o que pode ser feito", mas não deve incluir "como fazer".

Por razões de segurança e para facilitar sua adaptação à evolução da organização, não deve conter aspectos técnicos da implementação.

A política de segurança deve ser concisa e fácil de ler e interpretar; sugerimos o uso dos 5 Ws do jornalismo: ***Quem, O quê, Onde, Quando, Porquê.***

A natureza mais ou menos restritiva da Política de Segurança deve resultar de uma avaliação prévia do potencial de risco à segurança. É possível quantificar um nível de risco de ataque, por meio de questionários sobre a organização/ negócio e sua infraestrutura.

Características:

- Documento público, facilmente acessível a todos os utilizadores

- Leitura obrigatória para todos os utilizadores

- Identifica os vários atores da organização (utilizadores, administradores, ...)

- Define claramente os objetivos de segurança

- Alerta os utilizadores para as várias ameaças a que o sistema está sujeito

- Salienta a importância de todos, sem exceção, respeitando as regras

- Justifica o motivo das regras impostas (os atores devem concordar)

- Identifica contactos para esclarecimento de dúvidas

- Define o tratamento de situações omissas na "política de segurança"

- Estabelece as consequências da quebra de regras (de maneira abstrata, pois pode entrar em conflito com a legislação e/ou acordos trabalhistas)

- Destaca a manutenção de registos de atividades para auditorias

- É consistente com a profundidade da abordagem de ligações múltiplas

- É possível impor aos atores (é possível monitorizar o cumprimento das regras)

Uma política deve ser explícita em relação ao que é permitido, proibindo tudo o resto. É mais arriscado incluir o que é proibido, permitindo tudo o resto.

Políticas de:

- Autenticação
- Acesso físico
- Acesso lógico
- Uso interno da rede (ligar dispositivos à rede, ...)
- Uso da Internet (acesso a sites, controle de conteúdo, ...)
- Palavras passe (regras na definição, armazenamento e manuseamento)
- Uso de email
- Privacidade (confidencialidade; registos de atividade e acesso)
- Gestão de sistemas de trabalho.

3.2 Confidencialidade de Dados

Description

Confidencialidade

Table of contents

1. Confidencialidade de Dados

2. Armazenamento de Dados
2.1. Armazenamento Externo - PenDrives e Discos Externos
2.2. Cloud Privada
2.3. Network Attached Storage

3. Transporte de Dados

1. Confidencialidade de Dados

A confidencialidade pode ser definida como garantia de que existe um nível apropriado de sigilo em cada nó de processamento e que o vazamento de informações é evitado.

A confidencialidade deve ser implementada em todo o sistema e não apenas em algumas partes. Pode ser obtida através de:

- Encriptação de dados armazenados e transmitidos

- Comunicações 100% seguras

Pode ser substituída por:

- Monitorização da comunicação

- Engenharia social

- Desviando palavras passe

2. Armazenamento de Dados

O armazenamento de dados é uma parte essencial de um computador/sistema industrial em que as necessidades e a importância da informação aumentam diariamente. Atualmente, em muitos casos, a informação é o ativo mais valioso de uma empresa.

Existem vários meios disponíveis para armazenar dados. Esses meios diferem em capacidade, qualidade e preço. Nos sistemas profissionais, é importante escolher meios que garantam que a perda de informações não ocorra.

2.1. Armazenamento Externo - PenDrives e Discos Externos

Pendrives e discos externos são os meios mais baratos presentes no mercado. Têm, no entanto, alguns problemas, resultantes da qualidade da sua produção e porque não são, normalmente, muito bem tratados/utilizados pelos seus utilizadores.

Estes meios podem ser usados para armazenar informações não críticas. No entanto, é aconselhável ter um backup noutro meio.

Este tipo de equipamento normalmente não contempla segurança ou encriptação de dados; portanto, se for perdido ou roubado, dados cruciais poderão ficar disponíveis ao público.

Figura 3.7. PenDrive

2.2. Cloud Privada

"Computação em nuvem é um termo geral para qualquer coisa que envolva o fornecimento de serviços hospedados pela Internet. Esses serviços são amplamente divididos em três categorias: Infraestrutura como serviço (IaaS), Plataforma como serviço (PaaS) e Software como serviço (SaaS). O nome cloud computing foi inspirado no símbolo da nuvem que é frequentemente usado para representar a Internet em fluxogramas e diagramas.

Um serviço de nuvem possui três características distintas que o diferenciam da hospedagem na web tradicional. É vendido sob pedido, geralmente a cada minuto ou hora; é elástico - um utilizador pode ter o serviço tão ou pouco quanto desejar a qualquer momento; e o serviço é totalmente gerido pelo provedor (o consumidor não precisa de nada além de um computador pessoal e acesso à Internet). Inovações significativas na virtualização e na computação distribuída, bem como no acesso melhorado à Internet de alta velocidade, aceleraram o interesse na computação em nuvem.

Uma nuvem pode ser privada ou pública. Uma nuvem pública vende serviços para qualquer pessoa na Internet. (Atualmente, o Amazon Web Services é o maior provedor de nuvem pública.) Uma nuvem privada é uma rede proprietária ou um Centro de Dados que fornece serviços hospedados a um número limitado de pessoas. Privado ou público, o objetivo da computação em nuvem é fornecer acesso fácil e escalável aos recursos de computação e serviços de TI.

Nuvem privada é um tipo de computação em nuvem que oferece vantagens semelhantes às da nuvem pública, incluindo escalabilidade e autoatendimento, mas por meio de uma arquitetura proprietária. Ao contrário das nuvens públicas, que fornecem serviços para várias organizações, uma nuvem privada é dedicada às necessidades e objetivos de uma única organização.

Como resultado, a nuvem privada é melhor para empresas com necessidades de computação dinâmicas ou imprevisíveis que exigem controlo direto sobre os seus ambientes, geralmente para atender aos requisitos de segurança, gestão comercial ou conformidade regulamentar."

[1] Fonte: searchcloudcomputing.techtarget.com

2.3. Network Attached Storage

O Network Attached Storage (NAS) é um tipo de armazenamento habitualmente usado em empresas, porque é uma maneira económica de fornecer um grande espaço de armazenamento para vários utilizadores.

As características mais importantes são:

- Instalação e configuração rápidas.

- Facilidade na garantia de redundância de RAID para vários utilizadores.

- Permite a definição de permissões de acesso a pastas e arquivos aos utilizadores.

- Alta utilização de recursos de armazenamento.

Este tipo de armazenamento também tem algumas desvantagens:

- Usa recursos de rede (possui pelo menos um endereço IP).

- Problemas de latência e potencialmente de transferência de dados.

- Desempenho dependente da disponibilidade da rede.

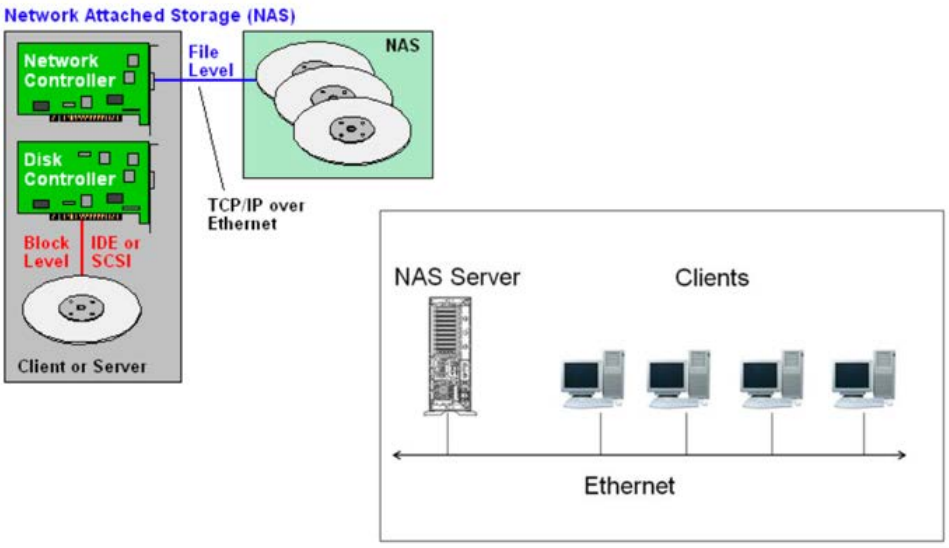


Figura 3.8. Network Attached Storage

3. Transporte de Dados

As redes são, por natureza, um meio privilegiado para conduzir ataques:

- Uma transmissão de informações significa que pode ser usada remotamente para atacar sistemas protegidos contra acesso físico à Content Delivery Network (Rede de Distribuição de Conteúdos).

- Como são extensas, é muito difícil controlar eficientemente o acesso físico, tornando impossível uma missão para as redes sem fio. Embora o controle de acesso físico não ofereça garantias, nunca deve ser esquecido.

Autenticação e encriptação são duas ferramentas essenciais para combater muitos dos ataques, mas podem não ser suficientes. A segmentação de redes em zonas distintas no nível de segurança é essencial, geralmente três zonas podem ser consideradas:

- Rede de Distribuição de Conteúdo (onde estão os servidores)
- Rede interna de utilizadores (intranet)
- Redes externas (Internet)

A separação entre zonas é garantida através da interligação por routers que analisam e filtram as informações designadas por firewalls.

1.5.1. Ligações Wi-Fi

Nas redes sem fio, o controle de acesso físico é totalmente impossível (nesse tipo de rede, o sinal é transmitido pelas ondas de rádio disponíveis no espectro a serem intercetadas). Embora as redes locais com fio atualmente suportem a comutação de pacotes no nível 2 (por exemplo, Ethernet), esses comutadores não separam domínios de broadcast e a sua operação pode ser comprometida. Do ponto de vista da segurança, esse tipo de infraestrutura deve sempre ser considerado equivalente a uma rede de meios de transmissão partilhada: qualquer pacote emitido num determinado nó é entregue em todos os outros nós da rede.

No mercado, estão disponíveis um conjunto de algoritmos que permitem implementar segurança e encriptação nos pacotes que circulam nas redes WIFI.

Os exemplos mais comuns desses algoritmos de segurança são:

WEP - Privacidade equivalente com fio (padrão 1999 - 2004. É possível quebrar. Abandonado) WPA - Acesso protegido por WiFi - Melhoria para WEP. Fácil de quebrar.

WPA2 - Acesso WiFi Protegido versão 2. A Encriptação Avançada AES padrão é a melhoria mais importante feita no WPA2 sobre o WPA.

1.5.2. Transporte Seguro de Dados - Assinaturas Digitais

Uma assinatura digital é uma maneira de garantir autenticação e/ou confidencialidade com base num certificado digital composto por 2 chaves (uma privada que somente o proprietário do certificado deve conhecer e uma chave pública que deve ser conhecida publicamente). Este método denomina-se encriptação assimétrica porque uma mensagem encriptada só pode ser desencriptada com a outra chave par.

PKI (Infraestrutura de Chave Pública)

- Utilizada para encriptar, desencriptar e autenticar (assinatura digital)

- A chave pública é divulgada livremente e pode ser usada para encriptação

- A desencriptação é feita com a chave privada (secreta).

- Não é bidirecional porque um par de chaves permite apenas confidencialidade num sentido.

A separação entre zonas é garantida através da interligação por routers que analisam e filtram as informações designadas por firewalls.

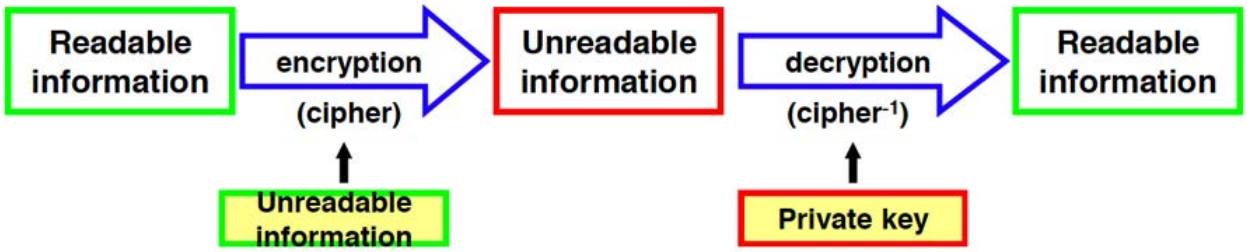


Figura 3.9. Assinatura Digital

Um par chave pública/chave privada garante apenas a confidencialidade unidirecional; para obter a confidencialidade bidirecional, são necessários dois pares de chaves. A aplicação da encriptação assimétrica com a chave privada a um código hash sólido permite implementar de maneira simples todas as funcionalidades de uma assinatura digital, considerando:
- Integridade do conteúdo

- Autenticação do autor

- Não recusa (somente o autor possui a chave privada)

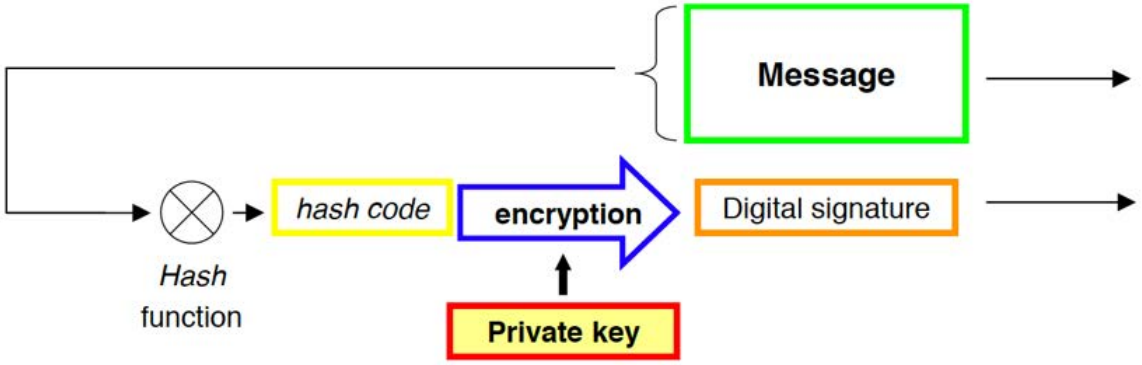


Figura 3.10. Integridade e autenticação

1.5.2.1. Confidencialidade com códigos de chave assimétricas

O uso de uma chave pública de alguém para encriptar uma mensagem permite garantir a confidencialidade, porque a mensagem encriptada será desencriptada apenas com a chave privada do utilizador.

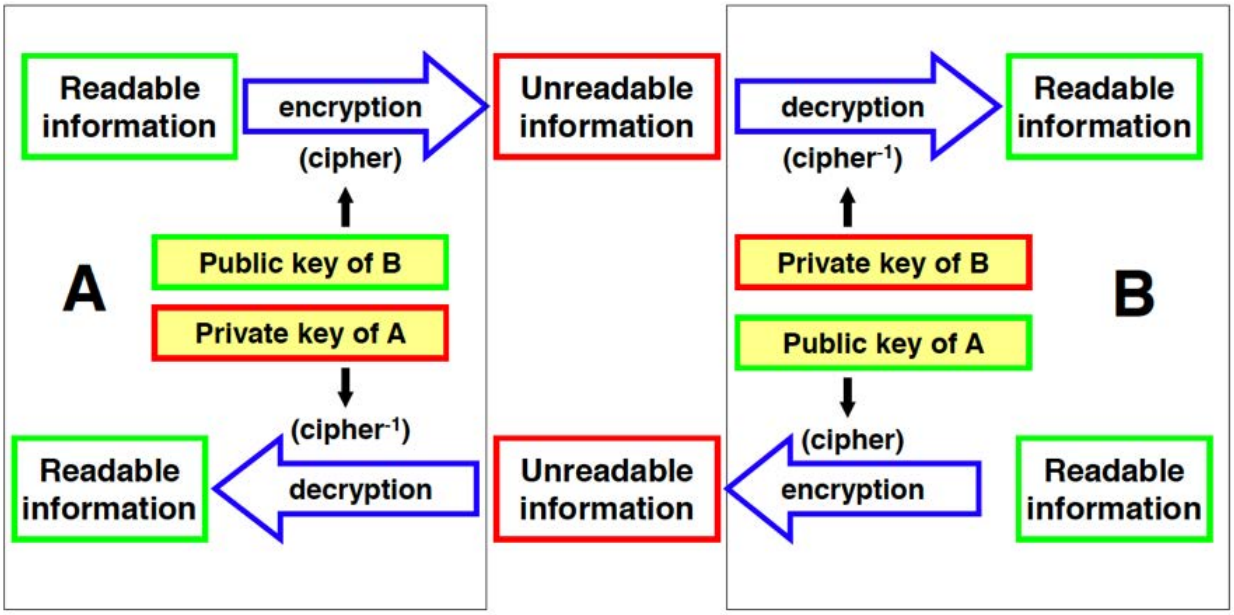


Figura 3.11. Confidencialidade com chaves assimétricas

3.3 Integridade de Dados

Description

Integridade

Table of contents

1. Integridade dos dados
1.1. Armazenamento de dados

1. Integridade dos dados

A integridade pode ser definida como confiança na precisão e fiabilidade do sistema e na prevenção de alterações de dados não autorizadas.

A integridade garante que ataques e erros não comprometam as informações e o sistema pode ser obtido através de:

- boa gestão dos recursos do sistema

- mecanismos de deteção de intrusão

- controlos de acesso apropriados

Sem garantia de integridade, um sistema pode operar com dados incorretos, sem saber.

1.1. Armazenamento de dados

O backup e armazenamento de dados são as medidas mais importantes que uma empresa deve tomar para proteger seus negócios.

É importante:

- Fazer backup dos dados regularmente (essa periodicidade deve ser avaliada em cada situação)
- Criar backups em meios fiáveis ou na nuvem da empresa (essa nuvem deve ter backups redundantes)
- Se usar meios para backup, mantenha-os dispositivos num local seguro e externo.

1.1.1. Lugar seguro de backup correto

O local em que os backups estão localizados é uma parte essencial do processo de backup. Por causa de desastres imprevisíveis, os backups devem ser mantidos em mais de um local. As empresas podem manter um backup local nas suas instalações, mas devem ter outra cópia num local externo (pode ser uma nuvem ou outras instalações da empresa).

1.1.2. Hash dos arquivos de backup

Os arquivos de backup resultantes devem ter um hash para garantir que qualquer modificação foi feita.

Esse processo implica a utilização de um algoritmo de encriptação como o MD5. A aplicação desse tipo de algoritmo a um arquivo retorna um número/código que pode ser considerado como um identificador. Se o arquivo for alterado, o resultado da aplicação do algoritmo será diferente e é possível detetar se foi feita alguma alteração não autorizada.

Quando um backup é feito, um código de hash deve ser gerado com base na aplicação de um algoritmo de encriptação. Posteriormente, esse hash pode ser usado para avaliar se o arquivo foi alterado.

1.1.3. Teste dos backups (2)

"Imagine que vai a conduzir na estrada e, de repente, ouve um som ameaçador vindo da parte de trás do seu automóvel: thumpa-ta, thumpa-ta, thumpa-ta. À medida que o automóvel se torna cada vez mais difícil de controlar, começa a perceber o que aconteceu: Tem um pneu furado.

Não há problema. Basta encontrar um local seguro para parar e retirar a peça de emergência da mala. Uh-oh, o pneu sobresselente também está furado.

Esta é uma situação semelhante à que um número incontável de administradores de armazenamento enfrenta todos os dias. Devido a uma falha na supervisão, erro ou falha no meio de armazenamento, surge uma necessidade repentina de aceder a um conjunto específico de arquivos armazenados no backup. Mas não existem backups, ou estão desatualizados ou com defeito. Como um condutor azarento, o administrador de armazenamento enfrenta agora uma situação que poderia ter sido facilmente evitada tendo havido algum planeamento na forma de testar backups.

Aqui está o que é necessário fazer.

1. Entender a seriedade dos testes de backup regulares. "Assim como é importante testar um pneu sobressalente para garantir que funciona quando for necessário, também precisa de testar os backups," afirmou Girish Dadge, diretora do departamento de gestão de produtos da Sungard Availability Services. "O teste dos seus backups também permite garantir que as suas políticas e agendamentos de backup funcionam corretamente", acrescentou.

2. Criar um plano de teste de backup documentado. "A familiaridade com um plano de teste documentado garante que os funcionários tenham as competências e a experiência necessárias para executar com êxito a recuperação de dados e confere confiança à organização," observou Eamonn Fitzmaurice, líder mundial em proteção de dados na empresa de serviços de TI HPE Pointnext.

3. Fazer dos backups de testes uma rotina. Para garantir a validade e a integridade de qualquer backup, é essencial realizar testes regulares de recuperação. "Não é incomum encontrar organizações que possuem sistemas que inadvertidamente não estão protegidos por meio de um agendamento de backup", explicou Fitzmaurice. Efetuar testes de rotina abrangentes de backup é uma estratégia que permite destacar as anomalias

para que possam ser tomadas ações de correção.

4. Adotar uma abordagem holística. As organizações precisam de entender o seu layout de dados e a razão pela qual fazem backups. Em seguida, precisam de desenvolver um plano de backup de teste para corresponder aos objetivos desejados.

Todas as organizações têm objetivos de backup diferentes. "Por exemplo, o sector bancário precisa de backups para conformidade, auditoria e aspetos legais", afirmou Dadge. "As organizações de assistência médica têm dados pessoais, portanto, precisam de se concentrar em segurança, retenção e requisitos legais." "Todos os testes de reconstrução e recuperação devem incluir dados, aplicações e testes de estado do sistema," recomenda o Dadge.

5. Testar frequentemente, de acordo com os horários regulares. Idealmente, deve ser realizado um teste após a conclusão de cada backup para garantir que os dados possam ser protegidos e recuperados com êxito. No entanto, isso geralmente não é prático devido à falta de recursos disponíveis ou restrições de tempo. "Cada organização deve, no mínimo, comprometer-se com um agendamento regular de recuperações semanais e/ou mensais de sistemas, aplicações e arquivos individuais com verificações para garantir que os dados sejam válidos e acessíveis conforme pretendido", afirmou Marty Puranik, CEO da Atlantic.Net, um provedor de hospedagem em nuvem. "Isso também fornecerá à sua organização um prazo realista para recuperação quando ocorrer um desastre."

Nem todos os dados são criados iguais, facto que deve afetar a frequência dos backups de teste. "Alguns dados são mais importantes do que outros", observou Atif Malik, diretor da unidade de consultoria de CIO da KPMG. Por exemplo, os dados de conformidade e reguladores da Lei Sarbanes-Oxley podem ser considerados mais importantes do que os dados de marketing. "Devem existir controlos para mitigar riscos com base na importância desses dados", recomendou Malik.

6. Aproveitar ao máximo a automação. A automação deve desempenhar um papel fundamental em qualquer estratégia de teste de backup. "As organizações devem esforçar-se para automatizar o máximo possível os seus testes de backup, a fim de garantir a consistência e a validade dos dados e reduzir o ônus da equipa encarregada dos testes de backup", sugeriu Puranik. "Teste de recuperação de sistemas completos em máquinas virtuais, aplicações, bancos de dados e arquivos individuais", acrescentou.

7. Verificar se o teste de backup abrange todas as bases. Se o teste de backup não testar realmente toda a carga de trabalho que está a ser restaurada, não poderá ser considerado um teste real. "Muitas organizações restauram apenas um ou dois ficheiros do arquivo total e consideram um sucesso", observou Chris Wahl, técnico chefe do provedor Rubrik de gestão de dados em nuvem. "Este fluxo de trabalho não tem relação com a realidade da recuperação de aplicações complexas e deve ser evitado quando se considera um teste de backup real."

8. Tornar os backups de teste parte integrante do desenvolvimento e implementação de aplicações internas. O teste de backup deve estar na mente de todos quer no desenvolvimento quer na introdução de novos aplicações na organização. "As estratégias de gestão de dados corporativos mais bem-sucedidas envolvem saber como e quando executar testes de validação de backup, antes de permitir que os dados sejam transferidos para a produção", explicou Wahl.

9. Garantir a precisão do backup. Quando os dados são recuperados, os administradores de armazenamento e do banco de dados podem executar uma "verificação de integridade" inicial nos dados. "No entanto, os utilizadores finais das aplicações de negócios estão, geralmente, melhor posicionados para destacar se os dados restaurados são precisos e consistentes ou não", observou Fitzmaurice.

10. *Possuir backups redundantes. Nunca faça backup apenas numa fita ou conjunto de fitas. "Se utilizar fitas, substitua-as regularmente", recomendou Brian Engert, desenvolvedor sénior de aplicações da Soliant Consulting, desenvolvedora de software para clientes."*

[2] Source: https://searchdatabackup.techtarget.com/tip/Ten-important-steps-for-testing-backups