BLOCO REDES

HARDWARE – Componentes físicos de uma máquina

Software – Sequência de algoritmos compilados. Também é a parte técnica de um hardware.  
“Software é a parte que você xinga, e o Hardware é a parte que a gente chuta.”

FIRMWARE- Como se fosse um software, porém dentro de um hardware, também se trata de um programa, mas que está embutido no hardware, sendo responsável por realizar tarefas básicas de entrada e de saída de dados e não pode ser removido, normalmente armazenado em memórias não voláteis.

Memória RAM – componentes responsáveis por armazenar dados temporariamente no computador. A RAM é um dos principais fatores que influenciam o desempenho e a velocidade de processamento dos dados.

Memoria ROM – A memória ROM (read only memory) é um tipo de memoria que armazena dados e instruções de forma permanente e não volátil

O que é um SO?  
O SO é um software é um software essencial que atua como intermediário entre o hardware (parte física do computador) e o usuário

Ele funciona com uma camada de abstração para que seja possível interagir com o computador sem entre a complexidade do hardware ou linguagem da máquina.

Sem o sistema operacional teríamos que controlar manualmente todos os aspectos do hardware  
Alocação de memória  
Controle de processador

Entre muitos outros processos.

TIPOS DE SO

-Monousuários

Apenas um usuário pode utilizar o sistema por vez

Mesmo que múltiplas contas estejam cadastradas apenas um usuário pode estar ativo em determinado momento

-Multiusuário

Permite múltiplos usuários utilizem o sistema simultaneamente

Cada usuário pode ter suas próprias permissões, processos e sessões independentes

-Monotarefa

Um sistema monotarefa são consegue executar uma única tarefa/ processo por vez

Enquanto esse processo estiver rodando o sistema não pode iniciar outro até que o primeiro termine

-Multitarefa

Em um sistema multitarefa vários programas podem ser executados do mesmo tempo

O sistema operacional gerencia os processos e aloca recursos de CPU, memória e disco para que eles rodem simultaneamente

Funções principais de um SO

Gerenciamento de processos

O SO controla a execução de programas garantindo que cada tarefa receba tempo de processador adequado

Gerenciamento de memória

O SO aloca e libera memória ram para os programas de execução

Evita que um programa use memória indevidamente o que poderia travar o sistema

Gerenciamentos de arquivos

O SO organiza e controla o armazenamento de dados em discos rígidos, SSDs ou pen drives

Gerenciamento de Dispositivos

O SO controla a comunicação entre o computador e dispositivos externos como impressoras scanners e mouses.

Para isso ela usa drivers que são programas específicos para cada dispositivo

Interface com o usuário

O SO oferece uma interface para interação que pode ser gráfica ou textual

Características de um SO

BIOS e UEFI

O que podemos fazer com a BIOS

Escolher o dispositivo de Boot definir se o sistema iniciará via HD SSD, pendrive ou DVD

O boot é esse processo de preparação ele é responsável por acordar o computador, verificar se tudo está funcionando direito e finalmente carregar o sistema operacional.

Habilitar ou desabilitar recursos de hardware ativar. desativar portas USB placas de rede áudio etc.

Configurar overclocking e gerenciamento de energia ajustar frequência da CPU e RAM para melhor desempenho

Alterar configurações de segurança confiar secur boot e TPM para segurança adicional

Restaurar configurações de fabricar resetar a BOIS UEFI caso haja problemas de inicialização

Criar e gerenciar senhas de inicialização acompanhar uma senha antes da inicialização do sistema operacional

Interface gráfica x CLI

Ambas são utilizadas para interagir com o sistema operacional sendo que a GUI é mais intuitiva, possuindo botões ícones janelas e outros facilitadores

Já o CLI a interação é feita por comandos onde acaba sendo mais pratico e eficiente para que já está habituado.

Utilizando o GUI

Modo gráfico os sistemas operacionais modernos oferecem uma interface gráfica que permite aos usuários interagirem de maneira intuitiva com o computador. Essa interface inclui elementos a como ícones janelas e menus para facilitar a navegação e execução de tarefas.

Ativos e Passivos de uma rede de computador

Equipamentos de rede

-Equipamentos ativos

-Equipamentos passivos

Equipamento de rede

Os equipamentos de rede são responsáveis pela interligação, Comunicação e segurança em redes de computadores. Eles garantem que os pacotes de dados sejam transmitidos corretamente entre dispositivos dentre uma LAN ou entre redes diferentes.

Equipamentos Passivos

Tomada de Superfície

O que são?

As tomadas de superfície são pontos de conexão para cabos de rede, geralmente instaladas em paredes, pisos ou mobiliários, permitindo a conexão de dispositivos à infraestrutura cabeada

Características

Possuem conectores RJ45 fêmea

Podem ser de embutir ou sobrepor

Categorias variadas (Cat5e, Cat6, Cat6A, Cat7)  
Proporcionam organização e flexibilidade na rede

Patch Cord

O que é?

O patch cord é um cabo de conexão com conectores RJ45 em ambas as extremidades, usado para interligar dispositivos de rede como computadores, switches e patch panels

Características

Disponível em varias categorias (Cat5e, Cat6, Cat6A, Cat7)

Comprimentos variados (geralmente de 0,5m a 10m)

Pode ser blindado (STP) ou não blindado (UTP)

Padrões de cabeamento: T568A e T568B

Patch Panel

O que é?

O patch panel é um painel de conexões usado para organizar e distribuir os cabos de rede dentro de um rack. Ele facilita a gestão e manutenção da infraestrutura.

Características

Disponível em 12,24, 48 ou mais portas RJ45

Possui estrutura modular para instalação em racks

Pode ser não gerenciado (passivo) ou gerenciado (ativo, com monitoramento)

Facilita a reorganização e manutenção de rede.

Rack de rede

O que é?

O Rack de rede (Rack de comunicações) é um armário metálico utilizado para acomodar equipamentos de rede como switches, servidores, patch panels e roteadores.

Características

Tamanho padronizado em U(altura), como 12U, 24U, 42U

Pode ser aberto (estrutura vazada) ou fechado (com portas e ventilação)

Inclui bandejas, organizadores de cabos e unidades de ventilação

Geralmente tem padrão de 19 polegadas garantindo compatibilidade com equipamentos

Equipamentos Ativos

Equipamentos

Roteador

Switch

AcessPoint

Gateway

Firewall

Tranceiver

Roteador

O roteador é um dispositivo de camada 3 no modelo OSI que tem a função de encaminhar pacotes entre diferentes redes. Ele utiliza tabelas de roteamento para determinar o melhor caminho para o tráfego de dados

Funções principais

Encaminhamento de Pacotes

NAT (Network Adress Translation)

DHCP (Dynamics Host Configuration Protocol)

Firewall e segurança

Conexão de redes distintas

Switch

O Switch é um equipamento de camada 2 do modelo OSI que conecta dispositivos dentro de uma mesma rede local. Ele gerencia o tráfego internamente usando endereços MAC

Funções principais

Encaminhamento baseado em MAC

Criação de VLANs

Full Duplex

Segurança

AcessPoint

O AcessPoint permite a conexão de dispositivos sem fio à rede cabeada (nem sempre, pode ser sem cabo também), funcionando como um “extensor” do sinal

Funções Principais

Ampliação da cobertura Wi-fi

Autenticação e controle de acesso

Suporte a múltiplas SSIDs e VLANs

SSIDs

SSID é uma abreviação para Service Set Identifier (Identificador de Conjunto de Serviços), que é um importante identificador de redes sem fio. Exemplos de SSID podem incluir "O Lar dos Smiths" ou "Prêmios da Cafeteria".

Gateway

O Gateway é u dispositivo(hardware ou software) que interliga redes diferentes, permitindo a comunicação entre sistemas que usam o protocolo

Funções principais

Conversão de endereços e protocolos

Encaminhamento de tráfegos entre redes

Implementação de regras de segurança

AULA 03

-Firewall

-Tranciever

-Camadas

Camadas

-Camada02

-Pra que é usada?

-Onde é usada?

-Qual a diferença entre a camada 02 e a 03?

-Camada03

-Pra que é usada?

-Onde é usada?

-Qual a diferença entre a camada 02 e a 03?

Firewall

O firewall protege a rede bloqueando ou permitindo tráfego com base em regras de segurança

Funções principais

Filtração de pacotes

Bloqueios de acesso não autorizados

Monitoramento de tráfego em logs

Tipos de Firewall

Firewall de software - Instalado em sistemas operacionais (Windows Defender, IPTables no Linux).

Firewall de hardware - Equipamentos dedicados que protegem redes corporativas

Transceiver

Os Transcievers são dispositivos responsáveis pela conversão e transmissão de sinais ópticos ou elétricos em redes de comunicação. Eles são usados para conectar switches, roteadores e outros equipamentos de rede a diferentes tipos de mídia (Fibra óptica ou cobre).

MODELOS E PROTOCOLOS DE REDES

O que são modelos de redes?

-Modelos de redes escrevem como uma estrutura conceitual para descrever como a comunicação ocorre entre dispositivos.

-Dois modelos principais - Modelo OSI e modelo TCP/IP

-Definem regras e padrões de comunicação

OSI - 7 Camadas

1-Física

2-Enlace

3-Rede

4-Transporte

5-Sessão

6-Apresentação

7-Aplicação

Importância dos protocolos de redes

-Protocolos garantem que dispositivos diferentes possam se comunicar

-Definem regras como endereçamento formatação de dados e controle de erros.

-Exemplos - HTTPS, FTP, SMTP, TCP, UDP, IP.

Arquitetura TCP/IP

Camadas

aplicação - HTTP, FTP, SMTP

Transporte - TCP, UDP

Internet - IPv4 ou IPv6, IP, TCP

Acesso a Rede - Ethernet, Frame, Relay, Wi-Fi

-Comparativo com o modelo OSI

-TCP/IP foi desenvolvido para a internet e é mais pratico do que o modelo OSI

IPv4 e IPv6

O que é IP?

O IP (Internet Protocol), é um endereço que serve para localizar e diferenciar as máquinas

IPv4

é a quarta versão do protocolo de internet, amplamente utilizado para identificação e localização de dispositivos na rede. Foi desenvolvido nos anos 1980 e se tornou o padrão de comunicações na internet

Importância - IPv4 é a base da maioria das redes atuais, sendo responsável por permitir a comunicação entre dispositivos de forma confiável e eficiente.

IPv6

É a sexta versão do Protocolo de Internet, projetado para substituir o IPv4 devido à exaustão de endereços IP disponíveis no IPv4, o IPv6 foi desenvolvido nos anos 1990 e se tornou o padrão emergente para comunicação na Internet, trazendo várias melhorias em relação ao

Os endereços IPv6 são longos e compostos por 128 bits, geralmente

representados em oito grupos de quatro dígitos hexadecimais, separados por dois

pontos. Para facilitar a leitura e a escrita, IPv6 permite a contração ou abreviação de

endereços, utilizando regras específicas.

Regras de Contração

Omissão de Zeros à Esquerda;

Substituição de Sequências de Grupos de Zeros por "::“

Exemplo 1:

•Endereço Completo: 2001:0db8:0000:0000:0000:ff00:0042:8329

•Passo 1 (Omissão de Zeros à Esquerda): 2001:db8:0:0:0:ff00:42:8329

•Passo 2 (Substituição de Sequência de Zeros): 2001:db8::ff00:42:8329

IPv4

Importância - IPv6 é crucial para o futuro da internet, pois oferece um espaço de endereçamento muito maior. Suporta o crescimento contínuo da internet e a proliferação de dispositivos conectados, como smartphones, IoT e outros.

Estrutura do Endereço

Um endereço Ipv4 é um número de 32 bits dividido em quatro octetos, representado em notação decimal com pontos

Um endereço Ipv6 é um número de 128 bits, dividido em oito grupos de 16 bits chamado de duocteto. Cada grupo é representado por 4 dígitos hexadecimais (O - F)

IPv4

Tabela

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

192 -> 192 > 128 -> 1

(subtrai os valores depois)

64 -> 64 > 64 -> 1

64 - 64 = 0 (O resto fica 0)

10101100, 00010000, 00000000, 11000010

00001010, 01101100, 11001000, 00100001

11000000, 10101001, 11111101, 00101101

00100011, 11011011, 01000110, 01100010

10101101, 11111101, 11100101, 00000100

Classes de endereços

Classe A - Endereços de 0.0.0.0 a 127.255.255.255. Grandes redes, com poucos bits para a rede e muitos para hosts

Classe B - Endereços de 128.0.0.0 a 191.255.255.255. Redes de tamanho médio

Classe C - Endereços de 192.0.0.0 a 223.255.255.255. Redes pequenas, com muitos bits para a rede e pouco para hosts.

Classe D - Endereços de 224.0.0.0 a 239.255.255.255. Usados para Multicasts

Classe E - Endereços de 240.0.0.0 a 255.255.255.255. Reservados para pesquisas e testes

Endereços especiais

Redes Locais - Faixas de endereço como

10.0.0.0 - 10.255.255.255

172.168.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

São reservadas para uso em redes privadas e não podem ser roteadas na internet pública

Multicast - Endereços multicast são usados para enviar um único pacote de dados para um grupo de destinos simultâneos

Endereço de Loopback - 127.0.0.1. Usado para testar a pilha de rede local.

Máscaras de Sub-rede

Uma máscara de sub-rede é usada para dividir uma rede IP em sub-redes

menores, o que facilita a organização e o gerenciamento da rede. Ela define qual

parte do endereço IP é a parte da rede e qual parte é a parte do host. A notação

CIDR (Classless Inter-Domain Routing) é uma maneira de representar a máscara de

sub-rede, como /24, que indica que os primeiros 24 bits do endereço IP são usados

para a rede.

Rede Original: 192.168.1.0/24

•Endereço IP: 192.168.1.0

•Máscara de sub-rede: 255.255.255.0 (ou /24)

•Número de endereços na rede: 2^(32-24) = 2^8 = 256

•Endereços disponíveis para hosts: 256 - 2 (rede e broadcast) = 254

NAT (Network Address Translation)

Técnica que permite a um conjunto de endereços IP privados serem

mapeados para um endereço IP público, ajudando a economizar endereços IPv4.

NAT Estático, NAT Dinâmico e PAT (Port Address Translation)

NAT Estático é um tipo de tradução de endereços de rede onde um endereço

IP privado é mapeado para um endereço IP público de forma fixa e permanente.

Esse mapeamento é configurado manualmente pelo administrador da rede.

NAT Dinâmico, também conhecido como NAT Overload, é um tipo de

tradução de endereços de rede onde múltiplos endereços IP privados são mapeados

para um conjunto de endereços IP públicos de forma dinâmica.

PAT, também conhecido como NAT Overloading, é um tipo de tradução de

endereços de rede onde múltiplos endereços IP privados compartilham um único

endereço IP público, utilizando diferentes números de portas TCP ou UDP.

CGNAT (Carrier-Grade Network Address Translation)4

CGNAT (Carrier-Grade Network Address Translation) é uma técnica utilizada

por provedores de serviços de Internet (ISPs) para gerenciar a escassez de endereços

IPv4 públicos. CGNAT permite que múltiplos clientes compartilhem um único

endereço IPv4 público, utilizando NAT (Network Address Translation) em uma escala

muito maior do que a tradicionalmente utilizada em redes domésticas ou

corporativas.

Calcular Endereço Broadcast

192.168.16.10/24

11000000, 10101000, 0001000, 01000111

11111111, 11111111, 1111111, 11000000,

11000000, 10101000, 0001000, 01100000,

192. 168 16. 92

/27

/28

/25

/25

Endereço de rede

Primeiro IP válido para host

O último IP válido para host

O endereço de Broadcast

10.0.5.200/8

0 – 255

Endereço de rede – 10.0.0.0/8

Primeiro IP host – 10.0.0.1/8

Último IP host – 10 .255.255.254/8

Broadcast – 10.255.255.255/8

172.20.35.180/16

Rede- 172.20.0.0/16

Primeiro IP – 172.20.1.0/16

Ultimo IP – 172.20.255.254/16

BroadCast – 172.20.255.255/16

192.168.15.240

Rede- 192.168.15.0/24

Primeiro IP – 192.168.15.1/24

Ultimo IP – 192.168.15.254/24

BroadCast – 192.168.15.255/24

10.10.8.145/8

Rede - 10.0.0.0/8

Primeiro IP – 10.0.0.1/8

Ultimo IP – 10.255.255.254/8

BroadCast – 10.255.255.255/8

R-172.16.0.0

F1- 172.16.0.1  
L1-172.16.255.254

Br-172.16.255.255

R -192.168.10.0/24

F1-192.168.10.1/24

L1-192.168.10.254/24

Br-192.168.10.255/24

R-10.0.0.0/8

F1-10.0.0.1/8

L1-10.255.255.254/8

Br-10.255.255.255/8

R-172.31.0.0/16

F1-172.31.0.1/16

L1-172.31.255.254/16

Br-172.31.255.255/16

r- 192.168.100.0/24

F1-192.168.100.1/24

L1-192.168.100.254/24

Br-192.168.100.255/24